CA Spectrum®

Virtual Host Manager 解决方案指南

版本 9.4

ca technologies

CA Technologies 产品引用

本文档引用以下 CA Technologies 产品：

- CA Spectrum® (CA Spectrum)
- CA Spectrum® Virtual Host Manager (Virtual Host Manager)
- CA Spectrum® Report Manager (Report Manager)
- CA Spectrum® Active Directory and Exchange Server Manager (ADES Manager)
- CA Spectrum® Cluster Manager (Cluster Manager)
- CA Virtual Assurance for Infrastructure Managers (CA Virtual Assurance for Infrastructure Managers)
- CA SystemEDGE
- CA Mediation Manager (CAMM)

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： Virtual Host Manager

此部分包含以下主题：

关于 Virtual Host Manager

Virtual Host Manager 是随 CA Spectrum 提供的应用程序，用于对虚拟网络环境建模和监控其运行状况。通过此应用程序，可以查看有关虚拟网络组件的详细信息以及物理组件和虚拟组件之间的关联关系。

此全面视图可帮助您更好地监控网络基础架构的运行状况，以防止虚拟组件发生服务中断。通过监控虚拟环境（如监控主机和虚拟设备上的资源利用率），可以帮助您确定可能的性能问题。通过向虚拟环境应用 CA Spectrum 故障隔离技术，Virtual Host Manager 还可以帮助您查明并有效排除整个网络中的问题。

监控虚拟环境时面临的一项主要挑战是使数据保持更新。虚拟环境旨在根据需要优化资源分配，以便快速地更改虚拟网络和物理网络之间的关联关系。Virtual Host Manager 将跟踪这些更改，并持续监控虚拟网络的当前状态，以检测任何更改。

Virtual Host Manager 的预期用户

目前有多个供应商都提供了虚拟技术解决方案。Virtual Host Manager 适用于需要创建和管理虚拟环境的 CA Spectrum 用户。Virtual Host Manager 允许用户监控其物理和虚拟网络实体的故障和性能。

Virtual Host Manager 支持的虚拟技术

Virtual Host Manager 可以建模和管理通过下列虚拟网络技术创建的虚拟网络：

- VMware vCenter Server（VMware 基础架构和 vSphere 的组成部分）
- Solaris Zones
- Microsoft Hyper-V
- IBM 逻辑分区 (LPAR)
- Huawei SingleCLOUD

详细信息：

重叠虚拟技术 (p. 13)

系统要求

Virtual Host Manager 是一个应用程序，在正确配置所有必需组件之后，即可在 CA Spectrum 中运行。根据解决方案，Virtual Host Manager 需要以下组件。

VMware

- CA Spectrum r9.2.3 或更高版本
- VMware vCenter Server
- 带有 vCenter Server AIM 的最新 CA SystemEDGE 代理

Solaris Zones

- CA Spectrum r9.2.3 或更高版本
- 安装在运行 Windows 2003 Server（32 位）的计算机上的带有 Solaris Zones AIM 的 CA SystemEDGE 代理

Hyper-V

- CA Spectrum r9.2.3 或更高版本
- 在每台物理 Microsoft Hyper-V 服务器上安装了带 Hyper-V AIM 的 CA SystemEDGE 代理

IBM LPAR

- CA Spectrum r9.2.3 或更高版本
- 安装在 Windows 服务器（独立于管理 IBM LPAR 的 HMC (请参阅本页中的定义 256)）上的带有 IBM LPAR AIM 的 CA SystemEDGE 代理

Huawei SingleCLOUD

- CA Spectrum r9.2.3 或更高版本
- 带有 Huawei SingleCLOUD 设备包的 CA Mediation Manager

注意：有关 CA SystemEDGE 代理和 AIM 系统要求的详细信息，请参阅《*CA Virtual Assurance for Infrastructure Managers 实施指南*》。有关安装 CA Mediation Manager 的详细信息，请参阅 CA Mediation Manager 文档。

Virtual Host Manager 的工作原理

除 CA Spectrum 中的物理网络实体之外，Virtual Host Manager 还能无缝监控虚拟网络实体。您可以全面了解网络情况，以便于对这两种类型的实体进行故障排除。虽然虚拟网络实体的行为与物理组件的行为类似，但是对这些实体的监控过程不同于一般 CA Spectrum 监控过程。了解此过程的工作原理可帮助您找到并解决与虚拟网络相关的网络问题。

CA Spectrum 通常会联系网络设备上的 SNMP 代理以收集信息。但是，一些网络设备上没有安装 SNMP 代理。如果没有 SNMP 代理，将很难收集监控状态以及使用故障隔离查明问题所需的信息。Virtual Host Manager 扩展了基础 CA Spectrum 功能，可使用代理管理器来收集所需信息，如下图所示：

收集虚拟网络环境信息的过程如下：

1. 代理管理器直接与虚拟环境中的实体进行通信。

   注意：代理管理器驻留在网络中的一个服务器上。该服务器的位置取决于虚拟技术。

2. 通过使用 SNMP，CA Spectrum 可从代理管理器检索此信息，并将其用于建模和监控虚拟实体。

根据具体的解决方案，Virtual Host Manager 将使用下列其中一个代理管理器（将在以下各节中对其进行介绍）：

- 带有 CA Virtual Assurance for Infrastructure Managers AIM 模块的 CA SystemEDGE 代理 (p. 12)
- 带有特定于解决方案的设备包的 CA Mediation Manager (p. 13)

带有 CA Virtual Assurance for Infrastructure Managers AIM 的 CA SystemEDGE 代理

以下 CA Virtual Assurance for Infrastructure Managers AIM 可与 Virtual Host Manager 配合使用：

vCenter Server AIM

提供用于管理和监控受 VMware vCenter Server 控制的系统的功能。AIM 直接与 vCenter Server 软件进行通信，以获取关联的 VMware vCenter Server 管理的所有 ESX 服务器的整个视图。

Solaris Zones AIM

提供用于管理和监控配置为运行容器和区域的 Oracle Solaris 系统的功能。Solaris Zones AIM 需要在 Windows 服务器上运行的 CA SystemEDGE 代理。Solaris Zones AIM 通过 SSH 连接与托管的 Solaris Zones 服务器进行通信。请验证在托管的 Solaris 服务器上和运行 Solaris Zones AIM 的服务器上是否启用了 SSH。在 CA Virtual Assurance for Infrastructure Managers 文档集中验证受支持的平台。

Hyper-V AIM

提供用于监控受 Hyper-V 服务器控制的 VM 的功能。Microsoft Hyper-V AIM 需要 Microsoft Hyper-V 服务器上的 CA SystemEDGE 代理。Microsoft Hyper-V AIM 通过 WMI 与 Microsoft Hyper-V 服务器进行通信。Microsoft Hyper-V AIM 必须驻留在 Microsoft Hyper-V 服务器上才能监控虚拟机。

IBM LPAR AIM

提供用于监控由 HMC (请参阅本页中的定义 256) 管理的 IBM LPAR 的功能。IBM LPAR AIM 需要在 HMC 以外的 Windows 服务器上运行的 CA SystemEDGE 代理。IBM LPAR AIM 使用 SSH 与 HMC 进行通信，从 HMC 收集信息以监控 IBM LPAR 实例。

详细信息：

Virtual Host Manager 如何使用 Solaris 区域 (p. 85)
Virtual Host Manager 如何使用 Hyper-V (p. 131)
Virtual Host Manager 如何使用 IBM LPAR (p. 169)

CA Mediation Manager

以下 CA Mediation Manager 设备包可与 Virtual Host Manager 配合使用：

Huawei SingleCLOUD

提供用于监控 Huawei SingleCLOUD 平台的功能。CA Mediation Manager 直接与 Huawei SingleCLOUD GalaX 进行通信，以获取有关 Huawei HyperVisor 通用虚拟化平台 (UVP) 的信息。

详细信息：

Virtual Host Manager 如何使用 Huawei SingleCLOUD (p. 211)

重叠虚拟技术

当存在下列任一情况时，虚拟环境将具有“重叠”技术：

- 在环境中同时使用两种或更多虚拟技术时
- 相同的虚拟技术嵌套在一起时

Virtual Host Manager *不*支持在单个 SpectroSERVER 内进行建模的重叠技术。下列配置展示了重叠虚拟技术的示例：

- 在同一个 CA SystemEDGE 主机上启用 Solaris Zones AIM 和 vCenter Server AIM
- 在由不同 vCenter Server AIM 管理的 VMware 虚拟机上启用 vCenter Server AIM
- 在 VMware 虚拟机上安装 Solaris Zones AIM
- 在 VMware 虚拟机上安装 Solaris Zones 主机
- 在 Hyper-V 虚拟机上安装 Solaris Zones Manager
- 在 VMware 虚拟机或 Hyper-V 虚拟机上运行 IBM LPAR AIM

当 CA Spectrum 在各虚拟技术中发现不受支持的配置时，会发生下列行为：

- 在虚拟技术管理器的初始建模期间，CA Spectrum 将阻止创建技术文件夹。将生成次要警报，就不支持的配置向您报警。
- 当虚拟技术管理器监控其他管理器当前管理的同一个设备时，CA Spectrum 将为该设备创建重复的模型。

如果在单独的 SpectroSERVER 上为重叠虚拟技术管理器建模，则 Virtual Host Manager *可以*支持重叠技术管理器。

例如，假定在 VMware 虚拟机上承载一个 Solaris 区域实例。您不能在单个 SpectroSERVER 上同时管理这两个虚拟环境， 而必须在单独 SpectroSERVER 上管理每个虚拟环境。

详细信息：

Virtual Host Manager 支持的虚拟技术 (p. 10)

虚拟设备管理和多个 CA Spectrum AIM 解决方案

在通过多个 CA Spectrum AIM 解决方案管理某个设备时，将应用定义的管理排名顺序，如下所示：

1. Virtual Host Manager
2. Cluster Manager
3. 其他技术（如 Active Directory and Exchange Server Manager）

已在 CA Spectrum 中为具有 CA SystemEDGE 代理的主机建模时，Virtual Host Manager 可识别该模型。将不会创建重复模型。相反，Virtual Host Manager 将现有模型置于其自己的管理中，以使用排定的顺序应用每个解决方案的规则。

例如，如果 Virtual Host Manager 和 Cluster Manager 都在管理某个设备，则会使用 Virtual Host Manager 分配的模型参数。这些参数的示例包括模型名称、IP 地址和 MAC 地址。

当解决方案不再管理设备时，将按排定的顺序重新应用剩余解决方案的规则。通常会在下一个轮询周期完成相应的任何更改。

已定义的管理顺序还会影响模型在 Universe 拓扑中的显示方式。由于 Virtual Host Manager 在管理中排名最高，因此所有虚拟设备都自动显示在相应的虚拟主机容器中。

注意：有关详细信息，请参阅《*Cluster Manager 解决方案指南*》和《*Active Directory and Exchange Server Manager 解决方案指南*》。

详细信息：

使用多个 AIM 解决方案时如何建模环境 (p. 16)
使用多个 AIM 解决方案时删除模型 (p. 23)

第 2 章： 入门

本节介绍在安装和开始使用 Virtual Host Manager 时所需的基本信息。本节中的信息适用于 Virtual Host Manager 支持的所有虚拟技术。

此部分包含以下主题：

如何安装 Virtual Host Manager

安装 CA Spectrum 时，Virtual Host Manager 组件会自动安装且可供使用。但是，仅在也安装并配置适合您的解决方案的代理管理器之后，Virtual Host Manager 才可操作。对于 Huawei SingleCLOUD，请使用 CA Mediation Manager。对于支持的所有其他技术，请使用 CA SystemEDGE 代理的 CA Virtual Assurance for Infrastructure Managers AIM。

为了管理您的虚拟设备，CA Spectrum 必须能够联系代理管理器。而且，代理管理器必须能够与网络设备进行通信。

要安装 Virtual Host Manager，请完成以下任务：

1. 安装相应的代理管理器：
   - 对于 VMware、Solaris Zones、Hyper-V 和 IBM LPAR 解决方案，安装 CA SystemEDGE 代理，并加载相应的 CA Virtual Assurance for Infrastructure Managers AIM。使用适合您的虚拟技术的位置，如下所示：
     - VMware：安装在可以远程联系 vCenter 的单独服务器上。
     - Solaris Zones：在具有对每个 Solaris 区域主机的 SSH 访问权限的 32 位 Windows 系统上进行安装。
     - Hyper-V：在每个 Hyper-V 主机上进行安装。
     - IBM LPAR：在管理 IBM LPAR 的 HMC (请参阅本页中的定义 256) 以外的 Windows 服务器上进行安装。

       注意：仅监控具有 IBM LPAR AIM 的一个 IBM LPAR 主机实例。不要采用多个 HMC 来管理单个 IBM LPAR 主机。监控多个实例可能会导致 CA Spectrum 中出现重复模型。

注意：有关用于您的虚拟技术的 AIM 的安装说明和详细信息，请参阅《*CA Virtual Assurance for Infrastructure Managers 实施指南*》。

- 对于 Huawei SingleCLOUD，安装并配置 CA Mediation Manager 和 Huawei SingleCLOUD 设备包。不要在安装了 CA Spectrum 的同一服务器上安装 CAMM 组件。

  重要说明！在配置 Huawei SingleCLOUD 设备包时，可以设置虚拟 IP 地址。安装了 CAMM 展示器的设备或虚拟机的主 IP 地址不能用作虚拟 IP 地址。

  注意：有关详细信息，请参阅 CA Mediation Manager 文档。

2. 安装附带有 Virtual Host Manager 的 CA Spectrum。

   重要说明！不要在 Virtual Host Manager 将管理的虚拟机上安装 SpectroSERVER。

   注意：有关特定的安装说明，请参阅《*安装指南*》。

   现在可以在 CA Spectrum 中为虚拟网络建模。

详细信息：

发现 VMware 网络 (p. 31)
系统要求 (p. 10)
Solaris Zones 入门 (p. 87)
发现 Hyper-V 网络 (p. 134)
发现 IBM LPAR 网络 (p. 172)
发现 Huawei SingleCLOUD 网络 (p. 214)

使用多个 AIM 解决方案时如何建模环境

根据您的环境，可以将 Virtual Host Manager 与其他 CA Spectrum AIM 解决方案一起使用来管理基础架构。有些配置（如以下示例）需要多个解决方案进行综合管理：

- 群集节点是虚拟机。
- Active Directory 或 Exchange Server 主机是虚拟机。

每个 CA Spectrum AIM 解决方案都提供特定于它支持的技术的信息。例如：

- Virtual Host Manager 提供特定于虚拟技术的数据。
- Cluster Manager 提供特定于群集技术的数据。
- Active Directory and Exchange Server (ADES) Manager 提供特定于支持的 Active Directory 和 Exchange Server 角色的数据。

这些功能组合在一起可提供完整的监控解决方案。要设置多个 AIM 解决方案的实施，建议使用以下方法。

重要说明！ 使用多个 AIM 时，只能在 CA SystemEDGE 主机上安装一个 AIM。

遵循这些步骤:

1. 在 VNM 模型上配置 AutoDiscovery 设置。
2. 配置与虚拟技术相关的 Virtual Host Manager 设置。
3. 通过为虚拟技术管理器和所有虚拟技术组件建模来设置 Virtual Host Manager。
4. 通过为群集技术管理器和所有群集组件建模来设置 Cluster Manager。
5. 通过为 ADES Host Manager 以及所有的 Active Directory 和 Exchange Server 主机建模来设置 ADES Manager。

注意：有关详细信息，请参阅《*Cluster Manager 解决方案指南*》和《*Active Directory and Exchange Server Manager 解决方案指南*》。

详细信息：

虚拟设备管理和多个 CA Spectrum AIM 解决方案 (p. 14)
使用多个 AIM 解决方案时删除模型 (p. 23)

查看虚拟环境

Virtual Host Manager 旨在提供虚拟环境的可见性。此可见性允许您查看设备之间的逻辑关联关系，查看单个实体的性能数据，以及报告所发现的数据。虚拟环境必然会连接到您的物理环境。Virtual Host Manager 可以帮助您查看这些连接的位置，以及它们的运行状况。

Virtual Host Manager 提供了几种查看虚拟环境的方法，如下所示：

- “导航”面板中的“资源管理器”选项卡层次结构显示了逻辑关联关系。
- 各个模型的图标提供了状态和模型类型的概要信息。
- 图形拓扑视图可帮助您可视化虚拟实体和物理实体之间的连接。
- “内容”和“组件详细信息”面板中的信息视图提供了有关虚拟环境中各个事件的详细信息。

了解这些方法可以帮助您监控虚拟环境、排除问题和优化性能。

注意：有关使用 OneClick 界面的详细信息，请参阅《*操作员指南*》。

虚拟设备的图标

Virtual Host Manager 提供了专用于区分虚拟环境中设备的图标。为了区分物理实体和虚拟实体，虚拟设备图标的外部边缘会显示光晕效果。例如，虚拟设备模型图标的边缘显示有光晕，如下所示：

对于承载虚拟设备的物理服务器，Virtual Host Manager 在设备图标上使用独特的蜂窝形图案，如下所示：

在 CA Spectrum 中查找虚拟模型

为虚拟环境创建的模型将集成到 CA Spectrum 中的下列三个位置：

Universe 组

显示在“导航”面板中，可提供分层树结构，以显示物理设备和虚拟设备之间的逻辑关联关系。

Virtual Host Manager 组

显示在“导航”面板中，可提供分层树结构。此结构可帮助您可视化在虚拟技术中配置的虚拟/物理设备和逻辑实体之间的关联关系。

拓扑选项卡

显示在“内容”面板中，可提供物理网络、虚拟网络和虚拟机的图形视图。拓扑提供了网络的第 2 层视图，以显示虚拟网络和物理网络的连接方式。可以使用此视图来解决有关这些虚拟网络模型的警报。

注意：此选项卡仅可用于 Universe 组中的项目。

可以从“导航”面板的“资源管理器”选项卡中访问所有这些视图。对于确定用于查看虚拟实体的最佳视图来说，了解虚拟环境信息在 CA Spectrum 中的显示方式将十分重要。

注意：有关使用 OneClick 界面的详细信息，请参阅《*操作员指南*》。

在资源管理器选项卡上查找模型

在 OneClick 控制台中使用模型时，可以在“资源管理器”选项卡上快速找到选定的模型。为“内容”和“组件详细信息”面板中引用单个模型的项目提供了此位置功能。这些项目包括警报或事件表中的行。还可以在搜索结果表中使用此功能。

查看不同“资源管理器”选项卡组中的相同模型，以便洞悉其在物理和虚拟网络中的关联关系。

要在“资源管理器”选项卡上查找模型，请使用以下过程。

遵循这些步骤:

1. 在“内容”或“组件详细信息”面板中查找引用了单个模型的项目。
2. 右键单击该项目，并从以下选项中进行选择：

位置

更改 OneClick 控制台视图以在“导航”面板的“资源管理器”选项卡层次结构中查找选定的模型。可以从以下位置选项中进行选择：

Universe

在“资源管理器”选项卡上的 Universe 组层次结构中查找模型。

Virtual Host Manager

在“资源管理器”选项卡上的 Virtual Host Manager 组层次结构中查找模型。

OneClick 控制台将在“资源管理器”选项卡中查找相关模型。“内容”和“组件详细信息”面板将显示有关选定模型的详细信息。

拓扑视图

CA Spectrum 拓扑视图提供了对物理网络、虚拟网络和虚拟机的图形化说明。“内容”面板的“拓扑”选项卡上提供了这些拓扑视图。可使用“拓扑”选项卡中的视图来解决有关这些虚拟网络模型的警报。这些视图显示了第 2 层连接，其中指明了虚拟网络和物理网络的连接方式。

CA Spectrum 提供了用于在大多数拓扑视图中排列模型的选项，如树状布局、辐射状布局或手动布局。在选择树状布局时，Universe 组的“拓扑”选项卡中包含以下三个*未标记*的模型层：

顶层

显示通过 SNMP 发现的路由器。这些路由器是虚拟网络环境中的第一级路由器，用于将虚拟主机设备连接到物理网络。

中间层

包含在环境中发现的任何可管理的交换机。这些交换机提供到数据中心内虚拟主机设备的连接。

底部层

包含虚拟主机设备模型和任何非受管交换机。虚拟主机设备是用于运行虚拟化技术的物理服务器。

从“资源管理器”选项卡中选择用于承载虚拟机的服务器时，仅可在“拓扑”选项卡中使用一个布局选项。此自动布局被组织到树结构中，并包含以下三个*已标记*的层：

物理网络

包含对用于检测特定虚拟机通信的任何物理交换机的离页引用。这些实体是物理网络的组件，用于连接到虚拟网络。

虚拟网络

表示虚拟机设备提供的内部交换或虚拟交换。当使用多个虚拟机配置某个虚拟交换机时，CA Spectrum 将在名为“中继器段”或“扇出”的虚拟网络层中创建模型。此扇出模型表示存在虚拟交换机。

虚拟机

包括在“导航”面板中选择的虚拟主机设备上配置的虚拟机。

信息选项卡和子视图

“内容”和“组件详细信息”面板中的选项卡提供了用于帮助您监控虚拟环境的信息。“信息”选项卡提供了有关环境中单个实体的详细信息。

展开各个子视图可查看详细信息。大多数“信息”选项卡中包括一个“常规信息”子视图，其中列出了有关选定模型的常规详细信息。详细信息包括 IPv4 地址、连接状态和其他信息。

更新视图

在运行初始发现时，Virtual Host Manager 将使用虚拟设备模型填充“资源管理器”选项卡。在 Virtual Host Manager 构建此初始层次结构之后，可以频繁更改您的虚拟网络配置。因此，Virtual Host Manager 会持续更新此信息。仅当此信息可准确反映虚拟环境时，它才可用于排除问题和优化性能。

了解如何以及何时更新信息可有助于评估数据以及监控虚拟环境。

详细信息：

Virtual Host Manager 中的 Solaris Zones 数据更新方式 (p. 113)
Virtual Host Manager 中的 Hyper-V 数据更新方式 (p. 150)
Virtual Host Manager 中的 IBM LPAR 数据更新方式 (p. 189)
Virtual Host Manager 中的 Huawei SingleCLOUD 数据更新方式 (p. 232)

搜索

使用 CA Spectrum 搜索虚拟环境是一个基本的网络管理任务。Virtual Host Manager 不提供仅限于虚拟的拓扑视图。相反，CA Spectrum 在“定位器”选项卡上提供了一组专门用于虚拟网络的搜索。这些搜索可识别虚拟网络上的特定模型或模型组。使用这些搜索，可以帮助您找到可用于监控虚拟环境性能的详细信息。

详细信息：

用于 Solaris Zones 的定位器选项卡 (p. 115)
用于 Hyper-V 搜索的定位器选项卡 (p. 153)
用于 IBM LPAR 搜索的定位器选项卡 (p. 192)
用于 Huawei SingleCLOUD 搜索的定位器选项卡 (p. 235)

警报和故障隔离

为了就虚拟网络中出现的问题向您报警，CA Spectrum 将生成警报，并使用高级故障管理技术来隔离根本原因。虚拟网络可提供独特的管理机会，因为除了标准设备监控外，它们还提供了备用管理视角。直接从设备收集信息时，CA Spectrum 还同时从代理管理器收集信息。通过此额外的监控功能，除了“失去联系”警报外，还可能引发“代理已丢失”或“代理管理器不可用”警报。

警报和故障隔离根据虚拟技术的不同而异。Virtual Host Manager 使用的故障隔离类型取决于生成警报的设备和事件类型。CA Spectrum 使用所有可用信息将警报与相应的根本原因关联，从而避免多个警报或假警报。

初始模型上的警报

在 CA Spectrum 联系模型之前，模型保持初始（蓝色）状况。在初始状况下，警报通常在模型上不可见；但是，使用 Virtual Host Manager 时会出现例外。如果虚拟机在已关闭或已暂停状态下被置于 Virtual Host Manager 管理中，则关键的“已关闭”或“已暂停”警报将覆盖初始状况。

详细信息：

VMWare 的警报和故障隔离 (p. 70)
Huawei SingleCLOUD 的警报和故障隔离 (p. 237)
Solaris Zones 的警报和故障隔离 (p. 119)
Hyper-V 的警报和故障隔离 (p. 160)
IBM LPAR 的警报和故障隔离 (p. 200)

创建事件报告

使用事件筛选可在 Report Manager 中创建事件报告。可基于为 CA Spectrum 中的虚拟实体生成的任何陷阱和事件来创建这些报告。

为了报告 Virtual Host Manager 事件，Report Manager 中包含了下列事件筛选文件：

- vhm.xml
- vhmtrap.xml

注意：有关使用 Report Manager 从这些代码生成事件报告的详细信息，请参阅《*Report Manager 用户指南*》。有关使用预定义事件筛选文件生成报告的信息，请参阅《*Report Manager 安装和管理指南*》。

使用多个 AIM 解决方案时删除模型

如果将 Virtual Host Manager 与其他 CA Spectrum AIM 解决方案一起使用，请在您的环境中删除模型时考虑以下几点：

- 如果计划停止使用 Virtual Host Manager 管理设备模型，请配置 Virtual Host Manager 删除设置以保留模型。否则，Virtual Host Manager 最初将删除模型，从而丢失任何历史记录或自定义。然后其他 AIM 解决方案会重新创建该模型。

  注意：用于在删除技术管理器时保留模型的 Virtual Host Manager 设置仅适用于启用了 SNMP 的设备模型。对于 ICMP (Pingable) 模型，Virtual Host Manager 将删除模型，然后其他 AIM 解决方案会重新创建该模型。

- Virtual Host Manager 取消管理设备且保留模型时，其他 AIM 解决方案会自动将该模型置于其管理中。

- 当解决方案不再管理设备时，将按排定的顺序重新应用剩余解决方案的规则。通常会在下一个轮询周期完成相应的任何更改。
- 清空 Lost and Found (LostFound) 后，“资源管理器”视图层次结构将进行同步。

详细信息：

虚拟设备管理和多个 CA Spectrum AIM 解决方案 (p. 14)
使用多个 AIM 解决方案时如何建模环境 (p. 16)

第 3 章： VMware

本节适用于 VMware 用户，将介绍如何使用 Virtual Host Manager 来管理通过 VMware vCenter 创建的虚拟实体。

此部分包含以下主题：

Virtual Host Manager 如何使用 VMware

除 CA Spectrum 中的物理网络实体之外，Virtual Host Manager 还能无缝监控虚拟网络实体。您可以全面了解网络情况，并在网络中排除这两类实体的网络问题。虽然虚拟网络实体的行为与物理组件的行为类似，但是对这些实体的监控过程不同于一般 CA Spectrum 监控过程。了解此过程的工作原理可帮助您找到并解决与虚拟网络相关的网络问题。

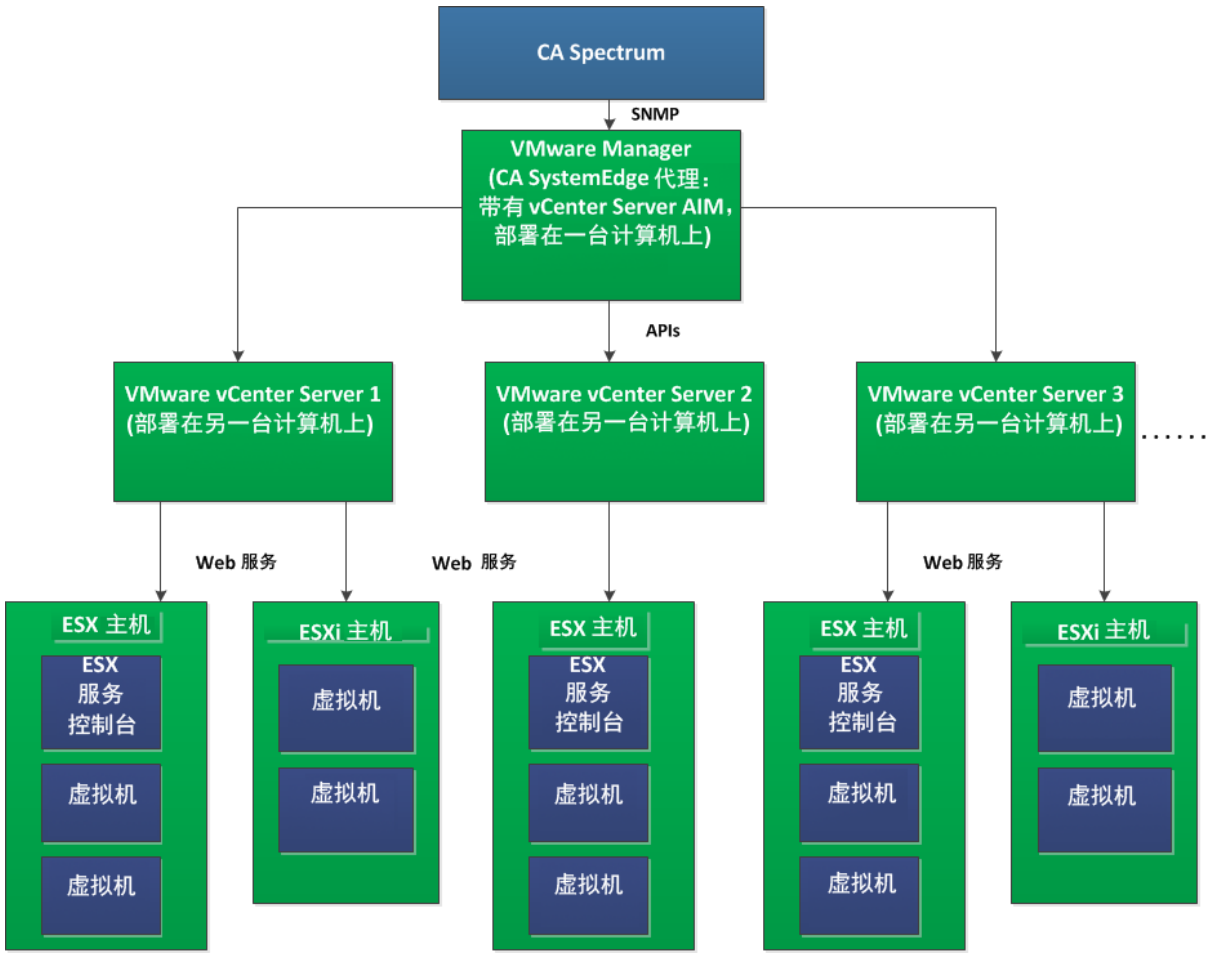
该版 CA Spectrum 仅支持远程部署最新 CA SystemEDGE。最新 CA SystemEDGE 带有最新的 vCenter Server AIM，能够管理多个 vCenter Server 实例（多实例）。因此，您可以远程部署一个或多个 CA SystemEDGE，以便管理多个 VMware vCenter Server。建议不要使用一个以上的远程 CA SystemEDGE 部署来管理同一台 VMware vCenter Server。

因此，请在升级到该版 CA Spectrum 之前，把所有远程 CA SystemEDGE 部署升级到最新版本并删除所有本地 CA SystemEDGE 部署。如果未删除所有本地 CA SystemEDGE 部署，那么升级 CA Spectrum 后将会在相应的 CA SystemEDGE 模型上生成“代理安装在 vCenter Server 本地”警报。

在升级之前，如果远程 CA SystemEdge 模型已存在，先前建模的虚拟实体将重新建模以支持多实例 vCenter。在相应过程中，这些虚拟实体的所有事件将丢失。

注意：CA SystemEDGE 的最新版本是 5.8。有关远程部署 CA SystemEDGE 的更多信息，请参阅《*CA Virtual Assurance for Infrastructure Managers 实施指南*》。

下图显示了 CA Spectrum 如何使用最新的远程 CA SystemEDGE 代理收集 VMware 虚拟环境的相关信息：



如图所示，收集有关 VMware 虚拟环境的信息的过程如下：

1. VMware vCenter 应用程序管理虚拟网络中的 ESX 主机。VMware vCenter 应用程序存储有关每个 ESX 主机及其虚拟机的详细数据。
2. CA SystemEDGE 代理与 vCenter 进行通信，以收集有关虚拟网络的详细信息。CA SystemEDGE 代理必须已加载 vCenter Server AIM。
3. CA Spectrum 定期从 CA SystemEDGE 检索信息，并使用此信息建模和监控 OneClick 中的虚拟实体。

由于 Virtual Host Manager 与 vCenter 进行通信，因此 CA Spectrum 能够发现自发的网络配置更改。示例包括由于 VMware VMotion、HA 技术或 DRS 方案而引起的更改。与这些事件关联的更改将快速反映到 OneClick 中，并用于分析根本原因。

详细信息：

Virtual Host Manager 的工作原理 (p. 11)
查看 VMware 虚拟网络 (p. 46)

为 VMware 创建的模型

Virtual Host Manager 提供了多个模型来表示 VMware 虚拟技术网络的组件。通过了解以下基本模型，可以帮助您更好地了解发现以及虚拟环境与物理环境的连接方式。

注意：在环境中部署 CA SystemEDGE 代理和 vCenter Server AIM 将影响 Virtual Host Manager 所显示的模型。

在*远程*部署方案中，针对 VMware 设备，Virtual Host Manager 包括以下模型和图标：

VMware Manager

表示包含已加载 vCenter Server AIM 的 CA SystemEDGE 代理的物理或虚拟主机。此 CA SystemEDGE 代理将远程监控在单独主机（由 VMware vCenter Server 模型表示）上运行的 vCenter 应用程序。

图标：  或 

VMware vCenter Server

表示包含用于管理 VMware 虚拟环境的 vCenter 应用程序的物理或虚拟主机。带有 vCenter Server AIM 的 CA SystemEDGE 代理远程监控 vCenter 应用程序。带有 vCenter Server AIM 的 CA SystemEDGE 代理位于单独的主机（由 VMware Manager 模型表示）上。

图标：  或 

ESX 主机

表示在 VMware 虚拟化技术中配置的 ESX 主机。*ESX 主机*是使用 ESX 服务器虚拟化软件来运行虚拟机的物理计算机。主机可提供虚拟机使用的 CPU 和内存资源，并为虚拟机提供存储访问和网络连接。在 Universe 拓扑中，这些模型会将虚拟实体分组到单独的视图中，同时显示虚拟环境如何与物理网络进行交互。不能直接联系 ESX 主机以获取状态信息。而是将通过模型中所含项目的状态来推断这些模型的状态。

图标： 

ESX 服务控制台

表示虚拟环境的 ESX 服务控制台组件。*ESX 服务控制台*是在 ESX 主机上运行的 Linux 内核，可提供所承载虚拟机的管理接口。

图标： 

虚拟机

表示在 VMware 虚拟化技术中配置的虚拟机。*虚拟机 (VM)* 是一种软件计算机，它能像物理计算机那样运行操作系统和应用程序。虚拟机根据其工作负荷动态地消耗其物理主机上的资源。由于虚拟机是一种非常灵活的计算单元，因此其部署可以包括多种环境。示例包括数据中心、云计算、测试环境、台式机和笔记本电脑等环境。在数据中心实施中，可以利用它们来实现服务器整合、优化工作负荷或提高能效。

图标： 

Virtual Host Manager 还将为这些用于组织 ESX 主机及其虚拟机的其他 VMware 实体创建模型：

数据中心

表示在 VMware 虚拟化技术中配置的数据中心。*数据中心*用作主机、虚拟机、资源池或群集的容器。根据其虚拟配置，数据中心可以表示组织结构，如地理区域或单独的业务功能。也可以使用数据中心创建隔离的虚拟环境，以用于测试目的或组织您的基础架构。各组件可在数据中心内交互，但限制在各数据中心之间进行交互。数据中心可以包含群集或主机。

图标： 

群集

表示在 VMware 虚拟化技术中配置的群集。*群集*是一组 ESX 主机及其关联的虚拟机。在将主机添加到群集时，该主机的资源将成为群集资源的一部分。群集将管理它包含的所有主机的资源。群集可以包含主机、资源池或虚拟机。

图标： 

资源池

表示在 VMware 虚拟化技术中配置的资源池。*资源池*定义物理计算的分区和单个主机或群集的内存资源。您可以将任何资源池分割成更小的资源池，从而将资源分开并分配给具体的组或用于特殊目的。您也可以分层组织和嵌套资源池。资源池可以包含虚拟机或其他资源池。

图标： 

重要说明！在发现和建模期间将跳过名为“资源”的资源池。此名称仅供内部使用。因此，Virtual Host Manager 会将这些资源池从发现结果中筛选出来。通过为 VMware 资源池指定不同的名称，可以避免缺少资源池的模型以及它们包含的设备。

详细信息：

查看 VMware 虚拟网络 (p. 46)

发现 VMware 网络

本节介绍 Virtual Host Manager 的发现和建模过程。这些任务通常由 Virtual Host Manager 管理员执行。

如何配置发现选项

安装后，配置 Virtual Host Manager 以执行 vCenter 发现。通过选择首选项，可帮助 Virtual Host Manager 正确地为虚拟设备建模。

为下列选项选择首选项：

自动为新数据中心建模 (p. 32)

确定是否自动为在 vCenter 发现期间发现的新数据中心建模。

新虚拟机的维护模式 (p. 33)

允许您决定在可使用 CA Spectrum 管理新发现的虚拟机之前将其中哪些虚拟机置于维护模式。

在 vCenter 发现期间允许删除设备模型 (p. 33)

控制当 ESX 主机、ESX 服务控制台和虚拟机模型不再受 vCenter 管理时，CA Spectrum 如何处理它们。控制在将 CA Spectrum 配置为禁用对模型的父数据中心的管理时，如何处理这些模型。

搜索现有模型 (p. 35)

确定在 vCenter 发现期间 Virtual Host Manager 搜索的安全域。

发现支持 SNMP 的设备 (p. 36)

控制在 vCenter 发现期间如何为支持 SNMP 的设备建模。默认情况下，最初仅会将新模型创建为 VHM 模型。但是，此选项允许您覆盖默认设置，并为符合必要标准的设备立即创建 SNMP 模型。

在执行 VMware Manager 删除期间保留启用了 SNMP 的虚拟机 (p. 37)

控制在删除 VMware Manager 模型时，CA Spectrum 如何处理支持 SNMP 的虚拟机模型。

为新数据中心配置自动建模

对于网络环境中的每个 SpectroSERVER，您可以控制 CA Spectrum 是否自动为在 vCenter 发现期间找到的新数据中心建模。自动为数据中心建模意味着 CA Spectrum 将管理 vCenter 环境中的所有数据中心。

遵循这些步骤:

1. 在“导航”面板中打开 Virtual Host Manager (p. 46)。

   将在选定 Virtual Host Manager 的“内容”面板中打开主详细信息页面。

2. 单击“信息”选项卡。
3. 展开“配置”、“VMware”、“vCenter 发现”子视图。
4. 在“自动为新数据中心建模”字段中单击“设置”，然后选择下列选项之一：

   是

   （默认）为在 vCenter 发现期间找到的所有数据中心建模。包括所有包含的群集、资源池、ESX 主机、ESX 服务控制台和虚拟机。

   否

   阻止为在 vCenter 发现期间找到的新数据中心建模。CA Spectrum 不会为数据中心中包含的组件建模。

   如果网络环境中包括无需监控的数据中心，请使用此选项。然后手动为数据中心建模。

   将保存您的设置，并且会根据您的选择在 Virtual Host Manager 中为新数据中心建模。

详细信息：

管理从 vCenter 中删除的设备的设备模型 (p. 33)
如何配置发现选项 (p. 31)

为新虚拟机配置维护模式

Virtual Host Manager 会自动为 vCenter 管理的虚拟机建模。CA Spectrum 将尝试管理所有已发现的模型。但是，在最初建模某些虚拟机时，它们尚未准备好由 CA Spectrum 管理。例如，CA Spectrum 在检测到已关闭的虚拟机时，会生成“虚拟机已关闭”警报。要阻止在新模型上生成不需要的警报，您可以选择要立即置于维护模式的虚拟机模型。之后，可以在准备好管理这些设备时手动禁用维护模式。

在 OneClick 中为新虚拟机配置维护模式。

遵循这些步骤:

1. 在“导航”面板中打开 Virtual Host Manager (p. 46)。

   将在选定 Virtual Host Manager 的“内容”面板中打开主详细信息页面。

2. 单击“信息”选项卡。
3. 展开“配置”、“VMware”、“vCenter 发现”子视图。
4. 在“新虚拟机的维护模式”字段中单击“设置”，然后选择下列选项之一：

   仅将关闭的虚拟机置于维护模式

   （默认）在初始 vCenter 发现时仅向已关闭或挂起的虚拟机模型应用维护模式。

   将所有 VM 置于维护模式

   在初始 vCenter 发现期间，向所有新虚拟机模型应用维护模式。

   将保存您的设置，并且会根据您的选择将在 Virtual Host Manager 中建模的新虚拟机置于维护模式。

详细信息：

如何配置发现选项 (p. 31)

管理从 vCenter 中删除的设备的设备模型

虚拟网络中的设备及设备间的关联关系会频繁地发生更改。CA Spectrum 将尝试准确地反映这些更改。在 vCenter 中删除 ESX 主机或虚拟机时，CA Spectrum 将从 Virtual Host Manager 层次结构中删除相应的设备模型。“在 vCenter 发现期间允许删除设备模型”选项用于控制 CA Spectrum 是否删除模型。此外，如果在 Virtual Host Manager 中禁用了数据中心管理，则此选项还可以控制对数据中心内包含的设备模型的处理方式。

重要说明！删除模型时，这些模型上的所有注释或其他自定义也将丢失。如果以后可能会在 vCenter 中重新创建模型，则可以禁用此选项。

可以管理已从 vCenter 中删除的设备的设备模型。

遵循这些步骤:

1. 在“导航”面板中打开 Virtual Host Manager (p. 46)。

   将在选定 Virtual Host Manager 的“内容”面板中打开主详细信息页面。

2. 单击“信息”选项卡。
3. 展开“配置”、“VMware”、“vCenter 发现”子视图。
4. 在“在 vCenter 发现期间允许删除设备模型”字段中单击“设置”，然后选择下列选项之一：

   是

   （默认）删除与不再受 vCenter 管理的实体对应的 Virtual Host Manager 模型。此外，删除在 Virtual Host Manager 中为其禁用建模的数据中心模型。

   否

   如果 Virtual Host Manager 模型对应的实体不再受 vCenter 管理，则将它们放置在 LostFound 容器中。此外，当在 Virtual Host Manager 中为数据中心禁用建模时，将数据中心模型放置在 LostFound 容器中。

   注意：将以不同的方式处理具有更多关联的模型（如全局集合中包括的模型）。将从 Universe 中删除这些模型，但是不会将其移动到 LostFound 容器中。

   将保存您的设置，并且会在从 vCenter 中删除设备之后按照您的设置处理设备模型。

详细信息：

针对 VMware 的 Virtual Host Manager 警报 (p. 70)
删除 Virtual Host Manager 模型 (p. 66)
如何配置发现选项 (p. 31)
为新数据中心配置自动建模 (p. 32)
删除 VMware Manager 后管理启用了 SNMP 的虚拟机模型 (p. 37)

跨安全域配置模型搜索

vCenter 发现将尝试查找 SpectroSERVER 中存在的模型，而不是创建新模型。在已部署 Secure Domain Manager 的环境中，vCenter 发现将搜索与 VMware Manager 位于同一个安全域中的模型。此域是“本地”域。但是，某些虚拟环境设备可存在于不同的安全域中。在这种情况下，可以配置 vCenter 发现以搜索所有安全域中的现有模型。

可以跨安全域配置模型搜索。

遵循这些步骤:

1. 在“导航”面板中打开 Virtual Host Manager (p. 46)。

   将在选定 Virtual Host Manager 的“内容”面板中打开主详细信息页面。

2. 单击“信息”选项卡。
3. 展开“配置”、“VMware”、“vCenter 发现”子视图。
4. 在“搜索现有模型”字段中单击“设置”，然后从下列选项中进行选择：

   在 vCenter 的安全域中

   （默认）搜索与 vCenter Server 位于同一个安全域中的现有模型。

   在所有安全域中

   搜索由 SpectroSERVER 管理的所有安全域中的现有模型。仅在下列情况下选择此选项：

   - 所有设备具有唯一的 IP 地址。
   - 当安全域用于安全目的或用于隔离网络通信时。

   注意：不要为 NAT 环境选择此选项。

   将保存您的设置。vCenter 发现将在 CA Spectrum 中搜索指定的模型。当多个安全域中存在重复的模型（具有相同 IP 地址的模型）时，Virtual Host Manager 将按如下所示处理此情况：

   - Virtual Host Manager 将在本地安全域中选择模型（如果有）。
   - 如果本地域中不存在重复的模型，Virtual Host Manager 将随机地从其他安全域中选择模型。
   - 在这两种情况下，Virtual Host Manager 将在 VMware Manager 模型上为重复的 IP 地址生成次要警报。

详细信息：

如何配置发现选项 (p. 31)

配置 SNMP 建模首选项

支持 SNMP 的虚拟机可支持丰富的设备监控功能，如进程和文件系统监控功能。但是，部署 SNMP 代理可能会花费较高的经济和时间成本。默认情况下，vCenter 发现会将 ESX 服务控制台和虚拟机创建为 VHM 模型(请参阅本页中的定义 255)。可在以后将它们升级为 SNMP 模型。不过，也可以将 vCenter 发现配置为将所有支持 SNMP 的新设备建模为 SNMP 模型。虽然完成 vCenter 发现可能需要更长的时间，但是初始建模为 SNMP 模型可避免以后手动升级这些模型。

重要说明！在为 vCenter Server 建模之*前*，请启用 SNMP 建模。如果首先为 vCenter Server 建模，则会将所有子模型创建为 VHM 模型，并且必须手动将其升级为 SNMP 模型。

遵循这些步骤:

1. 在“导航”面板中打开 Virtual Host Manager (p. 46)。

   将在选定 Virtual Host Manager 的“内容”面板中打开主详细信息页面。

2. 单击“信息”选项卡。
3. 展开“配置”、“VMware”、“vCenter 发现”、“SNMP 发现”子视图。

   重要说明！要准备设备和 CA Spectrum 以执行 SNMP 发现，请按照子视图中的步骤操作。如果在执行 vCenter 发现之前未正确准备设备，Virtual Host Manager 将无法创建 SNMP 模型。

4. 在“发现支持 SNMP 的设备”字段中单击“设置”，然后从下列选项中进行选择：

   是

   在 vCenter 发现期间启用 SNMP 建模。仅会将符合“SNMP 发现”子视图文本中指定标准的设备建模为 SNMP 设备。仅适用于*新*模型。

   否

   （默认）将在 vCenter 发现期间找到的所有新设备建模为 VHM 模型。可在以后手动将这些模型升级为 SNMP 模型。

   将保存您的设置。

详细信息：

如何发现和建模虚拟环境 (p. 38)
向 VHM 模型中添加 SNMP 功能 (p. 42)
vCenter 发现的工作方式 (p. 41)
删除 VMware Manager 后管理启用了 SNMP 的虚拟机模型 (p. 37)

删除 VMware Manager 后管理启用了 SNMP 的虚拟机模型

默认情况下，删除以下项时，将从 CA Spectrum 中删除启用了 SNMP 的设备：

- 设备的 VMware Manager 模型
- “导航”面板中的 VMware 文件夹

启用了 SNMP 的设备模型可包括要保留的重要自定义。可以调整设置以避免删除这些模型。将它们放置在 LostFound 容器中供以后使用。

删除 VMware Manager 或 VMware 文件夹后，可以保留启用了 SNMP 的设备模型。

遵循这些步骤:

1. 在“导航”面板中打开 Virtual Host Manager (p. 46)。

   将在选定 Virtual Host Manager 的“内容”面板中打开主详细信息页面。

2. 单击“信息”选项卡。
3. 展开“配置”、“VMware”、“vCenter 发现”子视图。
4. 在“在执行 VMware Manager 删除期间保留启用了 SNMP 的虚拟机”字段中单击“设置”，然后选择下列选项之一：

   是

   删除其 VMware Manager 或 VMware 文件夹时，将启用了 SNMP 的虚拟机模型保留在 LostFound 容器中。

   注意：将以不同的方式处理具有更多关联的模型（如全局集合中包括的模型）。将从 Universe 中删除这些模型，但是不会将其移动到 LostFound 容器中。

   否

   （默认）删除其 VMware Manager 或 VMware 文件夹时，将删除所有虚拟机模型。

   将保存您的设置，并且会在删除 VMware Manager 模型或 VMware 文件夹时相应地处理启用了 SNMP 的设备模型。

详细信息：

删除 Virtual Host Manager 模型 (p. 66)
管理从 vCenter 中删除的设备的设备模型 (p. 33)
如何配置发现选项 (p. 31)

如何发现和建模虚拟环境

要监控虚拟环境，需发现虚拟实体并为它们建模 - 数据中心、资源池、群集、ESX 主机、ESX 服务控制台和虚拟机。通过在 Virtual Host Manager 中为这些实体建模，您可以在一个工具中查看完整的网络拓扑。可以查看物理组件和虚拟组件之间的关联关系。

为虚拟环境建模的主要步骤如下所示：

1. 运行标准的 CA Spectrum 发现 (p. 39)。

   此发现过程可确保在运行 vCenter 发现之前为上游路由器和交换机建模。或者，如果已禁用“SNMP 建模”选项，则此步骤也可以为支持 SNMP 的 ESX 服务控制台和虚拟机建模。在为这些实体建模时，请确保正确设置建模选项以支持 Virtual Host Manager。

2. 升级 CA SystemEDGE 模型 (p. 40)。

   只有已在早于 CA Spectrum r9.1 的版本中为 vCenter Server 上的 CA SystemEDGE 代理建模的情况下，才需要执行此步骤。

3. 运行 vCenter 发现 (p. 41)。

   为 CA SystemEDGE 代理（带有 vCenter Server AIM）建模时，将自动启动 vCenter 发现。其中每个 vCenter Server 模型都具有自己的 vCenter 发现进程。vCenter 发现将查找由 vCenter 管理的虚拟实体，并为不存在的虚拟实体建模。然后，vCenter 发现将模型放置在“导航”面板的 Virtual Host Manager 视图中。

详细信息：

将 ESX 主机移至其他 vCenter (p. 45)
向 VHM 模型中添加 SNMP 功能 (p. 42)
如何配置管理选项 (p. 58)
配置 SNMP 建模首选项 (p. 36)

运行 CA Spectrum 发现

要发现您的 VMware 环境，请运行标准 CA Spectrum 发现。此发现可确保为上游路由器和交换机建模，以便将来可以从虚拟实体建立连接。您还可以在 CA Spectrum 发现期间为支持 SNMP 的 ESX 服务控制台和虚拟机建模。

注意：仅当在 vCenter 发现期间禁用了“SNMP 建模”选项时，才需要在 CA Spectrum 发现期间为支持 SNMP 的 ESX 服务控制台和虚拟机建模。

注意：只有管理员才可以执行此任务。

遵循这些步骤:

1. 打开发现控制台。

   注意：通过了解在非标准端口上运行的任何 SNMP 代理的正确团体字符串、IP 地址和端口号来做准备。

2. 在“导航”面板中单击  （新建配置）。
3. 配置选项以支持虚拟网络建模：
   a. 在“建模选项”组中单击“建模选项”按钮。

      此时将打开“建模配置”对话框。

   b. 单击“协议选项”按钮。

      此时将打开“协议选项”对话框。

   c. 选择“Pingable 项的 ARP 表”选项，然后单击“确定”。

      此时将打开“建模配置”对话框。

   d. （可选）在“高级选项”组中单击“高级选项”按钮。添加非标准 SNMP 端口（如 CA SystemEDGE 代理端口），然后单击“确定”。
4. 输入各个 IP 地址，或在“IP 边界列表”字段中输入开始 IP 地址和结束 IP 地址，然后单击“添加”。

   注意：确保 IP 地址范围中包括所有已安装 CA SystemEDGE 和 vCenter Server AIM 的服务器以及互连交换机和路由器。或者，也可以包括要为其创建 SNMP 模型的支持 SNMP 的 ESX 服务控制台和虚拟机。

5. 在发现控制台中输入任何其他值，然后单击“发现”。

   将创建以下模型，并会将其添加到 CA Spectrum 的网络拓扑中：

   - vCenter Server 以及用于将其连接到网络的交换机和路由器 - 有关虚拟环境的信息来自 vCenter Server。当 CA Spectrum 中存在这些 vCenter Server 模型时，vCenter 发现即可启动。
   - ESX 服务控制台和虚拟机 - 如果您决定不通过 CA Spectrum 发现为这些实体建模，则 vCenter 发现会将它们创建为 VHM 模型 (请参阅本页中的定义 255)。

   注意：也可以通过 IP 地址手动为虚拟网络建模。在这种情况下，建议首先为上游设备建模。按正确顺序建模可确保在拓扑中正确生成这些实体之间的关联关系。有关发现的详细信息，请参阅《*IT 基础架构建模与管理 - 管理员指南*》。

详细信息：

将 ESX 主机移至其他 vCenter (p. 45)
向 VHM 模型中添加 SNMP 功能 (p. 42)
如何配置管理选项 (p. 58)
配置 SNMP 建模首选项 (p. 36)

升级 CA SystemEDGE 模型

在安装 Virtual Host Manager 之前或者在代理上加载 vCenter Server AIM 之前，可能已在 CA Spectrum 中为 CA SystemEDGE 代理建模。在这种情况下，现有的 CA SystemEDGE 模型与 Virtual Host Manager 不兼容。升级该模型，以便 Virtual Host Manager 可以访问 CA SystemEDGE 中的 vCenter Server AIM 功能。*如果在安装 CA Spectrum 后为带有 vCenter Server AIM 的 CA SystemEDGE 代理建模，则不需要执行此过程。*

从本地 CA SystemEDGE 部署更改为最新的远程部署时，将会删除现有的 CA SystemEDGE 模型并在 OneClick 中为新的远程 CA SystemEDGE 重新建模。

注意：如果已在运行带最新 vCenter Server AIM 的最新远程 CA SystemEDGE，CA SystemEDGE 模型将会自动升级。

详细信息：

将 ESX 主机移至其他 vCenter (p. 45)
向 VHM 模型中添加 SNMP 功能 (p. 42)
如何配置管理选项 (p. 58)

vCenter 发现的工作方式

vCenter 发现是专门用于收集有关虚拟环境实体的详细信息的发现进程。vCenter 发现将查找由 vCenter 管理的虚拟实体，并为不存在的虚拟实体建模。然后，vCenter 发现将模型放置在“导航”面板的 Virtual Host Manager 视图中。

vCenter 发现的主要优点是，它在后台自动运行，可使 CA Spectrum 中的虚拟环境数据保持更新。通过了解 vCenter 发现的工作方式，可更有力地说明正确安装和建模各个 Virtual Host Manager 组件的重要性。

vCenter 发现进程的工作方式如下：

1. 当 CA SystemEDGE 代理和 vCenter Server AIM 正常运行时，AIM 会与 vCenter Server 进行通信以收集它管理的虚拟实体的相关信息。vCenter Server AIM 将存储此信息。

   重要说明！必须安装并配置 CA SystemEDGE 代理和 vCenter Server AIM，CA SystemEDGE、vCenter 和 CA Spectrum 才能进行通信。如果它们无法通信，vCenter 发现将无法运行。

2. 在 CA Spectrum 发现期间，CA Spectrum 将为步骤 1 中引用的每个服务器创建一个 vCenter Server 模型。1.将启用 CA Spectrum 智能，以处理 CA Spectrum 和 CA SystemEDGE 代理之间的通信。

3. CA Spectrum 轮询 vCenter Server AIM 以收集在步骤 1 中存储的 vCenter 信息。

4. CA Spectrum 启动 vCenter 发现。来自 AIM 的信息用于在 CA Spectrum“拓扑”选项卡和“导航”面板的 Virtual Host Manager 层次结构中更新建模，如下所示：

   a. 如果在步骤 2 之前启用 SNMP 发现，Virtual Host Manager 发现将为符合 SNMP 发现标准的所有支持 SNMP 的新模型创建 SNMP 模型。

      注意：默认情况下，将在 vCenter 发现期间禁用 SNMP 发现。

   b. 将为数据中心、群集和资源池创建 VHM 模型 (请参阅本页中的定义 255)。

      重要说明！在发现和建模期间将跳过名为“资源”的资源池。此名称仅供内部使用。因此，Virtual Host Manager 会将这些资源池从发现结果中筛选出来。通过为 VMware 资源池指定不同的名称，可以避免缺少资源池的模型以及它们包含的设备。

   c. 以前存在的 ESX 服务控制台和虚拟机模型将更改为 VHM 模型。

   d. 将为尚未在 CA Spectrum 中建模的 ESX 服务控制台和虚拟机创建 VHM 模型。

e. 将为 ESX 主机模型创建 VHM 模型。这些模型将在“导航”面板的 Virtual Host Manager 下以及 Universe 拓扑中显示其关联的 ESX 服务控制台和虚拟机模型。

f. 虚拟网络的所有模型将添加到“导航”面板的 Virtual Host Manager 部分中。

注意：在虚拟环境中，不同 ESX 主机上的设备可具有相同的 IP 地址或 MAC 地址。在这种情况下，CA Spectrum 将为每个 IP 地址或 MAC 地址创建重复的模型。

5. vCenter 发现将自动按每个定期排定的 vCenter 轮询时间间隔重复该过程。

注意：默认情况下，vCenter 轮询时间间隔由 VMware Manager 模型上的某项设置控制。或者，也可以使用 vCenter Server 应用程序模型独立于 vCenter Server 设备模型来控制 vCenter 轮询。

详细信息：

将 ESX 主机移至其他 vCenter (p. 45)
向 VHM 模型中添加 SNMP 功能 (p. 42)
如何配置管理选项 (p. 58)
控制 vCenter Server AIM 轮询 (p. 63)
跨安全域配置模型搜索 (p. 35)

向 VHM 模型中添加 SNMP 功能

具有 SNMP 功能的虚拟机支持丰富的设备监控功能（如进程和文件系统监控功能），使您的解决方案能够发挥更大的作用。但是，在整个企业中部署 SNMP 代理可能会花费较高的经济和时间成本。当 SNMP 代理不可用或禁用了 SNMP 发现时，Virtual Host Manager 会将 ESX 服务控制台和虚拟机创建为 VHM 模型 (请参阅本页中的定义 255)。

之后，您可以在任何虚拟机上安装 SNMP 代理。然后可以在 CA Spectrum 中升级其建模。根据您的需求，可以按如下所示升级到 SNMP 模型：

- **仅升级选定设备** - 当需要升级少量选定模型时，此方法可快速完成工作。此方法首先会删除 VHM 模型和子模型。在 CA Spectrum 删除模型之后，会在下一个 vCenter 发现期间创建新的 SNMP 模型并将其放置在 Virtual Host Manager 中。使用此方法时，您必须知道要升级的模型的 IP 地址。
- **升级所有支持 SNMP 的 VHM 模型** - 此方法可批量升级模型，在将 Virtual Host Manager 升级为新版本时，最好使用此方法。使用此方法时，您无需知道各个模型的 IP 地址。另一个优点是，在 CA Spectrum 删除 VHM 模型之后，会立即将升级后的 SNMP 模型放置在 Virtual Host Manager 层次结构中。您不必等待下一个轮询周期。因此，子模型不会处于非受管状态。此方法的缺点是可能需要很长时间才能完成。完成此升级所需的时间取决于在查找支持 SNMP 的设备时，Virtual Host Manager 必须搜索的团体字符串和 SNMP 端口的数量。

  注意： Virtual Host Manager 仅会尝试识别已启动的可 Ping 虚拟机上的 SNMP 代理。

重要说明！ 删除模型时，这些模型上的所有注释或其他自定义也将丢失。

详细信息：

删除 Virtual Host Manager 模型 (p. 66)
如何发现和建模虚拟环境 (p. 38)
配置 SNMP 建模首选项 (p. 36)

将选定 VHM 模型升级为 SNMP 模型

当 SNMP 代理不可用或在 vCenter 发现期间禁用了 SNMP 发现时，Virtual Host Manager 将创建 VHM 模型 (请参阅本页中的定义 255)。此建模适用于 ESX 服务控制台和虚拟机。之后，您可以在任何虚拟机上安装 SNMP 代理。然后可以在 CA Spectrum 中升级其建模。您需要知道要升级的设备模型的 IP 地址。手动选择要升级的模型可快速完成，但这些模型上的所有说明或自定义将会在升级期间丢失。

遵循这些步骤:

1. 根据需要在设备上部署或启用 SNMP 代理。
2. 使用下列方法之一重新建模设备：
   - CA Spectrum 发现
   - 按 IP 地址为设备逐个建模

在创建支持 SNMP 的新模型时，CA Spectrum 将从 Virtual Host Manager 中移除以前的模型，并删除该模型。在下一个 vCenter Server AIM 轮询周期中，CA Spectrum 将支持 SNMP 的模型添加到“导航”面板的 Virtual Host Manager 中。

重要说明！删除模型时，这些模型上的所有注释或其他自定义也将丢失。

详细信息：

删除 Virtual Host Manager 模型 (p. 66)
如何发现和建模虚拟环境 (p. 38)
管理从 vCenter 中删除的设备的设备模型 (p. 33)

将所有 VHM 模型升级为 SNMP 模型

在下列情况下，Virtual Host Manager 会将 ESX 服务控制台和虚拟机创建为 VHM 模型 (请参阅本页中的定义 255)：

- 在 SNMP 代理不可用时。
- 在 vCenter 发现期间禁用了 SNMP 发现时。

之后，您可以在任何虚拟机上安装 SNMP 代理，并在 CA Spectrum 中升级其建模。在执行批量升级时，CA Spectrum 将搜索 VHM 模型，以查找现在表示支持 SNMP 的设备的模型。然后，CA Spectrum 将它们转换为 SNMP 模型。此方法可能需要很长的时间，具体取决于 Virtual Host Manager 必须搜索的团体字符串和端口的数量。但是，此方法可确保在升级父模型时，子模型不处于非受管状态。

可以将 VMware 的所有 VHM 模型升级为 SNMP 模型。

遵循这些步骤:

1. 根据需要在设备上部署或启用 SNMP 代理。
2. 在“导航”面板中打开 Virtual Host Manager (p. 46)。

   将在选定 Virtual Host Manager 的“内容”面板中打开主详细信息页面。
3. 在“导航”面板中选择用于管理要升级的模型的 VMware Manager 模型。
4. 单击“信息”选项卡。

5. 展开“VMware Manager 建模控制”、“ICMP 专用设备升级”子视图。
6. 单击“升级 ICMP 专用设备”按钮。

   重要说明！删除模型时，这些模型上的所有注释或其他自定义也将丢失。

   Virtual Host Manager 将搜索由选定 VMware Manager 设备上的 vCenter Server AIM 管理的设备。Virtual Host Manager 升级所有符合 SNMP 设备标准的 ICMP 专用设备，并将它们放置在 Virtual Host Manager 层次结构中。

将 ESX 主机移至其他 vCenter

在将 ESX 主机从 CA Spectrum 管理的一个 vCenter 移至另一个 vCenter 时，如果这两个 vCenter 主机是在同一个 SpectroSERVER 上建模的，则可能会导致建模问题。这些建模问题的一些可能症状如下：

- CA Spectrum 删除与 ESX 主机关联的模型，并且不会在移动后重新创建它们。
- 创建并保留虚假“代理已丢失”警报，即使新的 vCenter 与 ESX 主机和承载的所有虚拟机取得了联系时也是如此。

如果按正确顺序移动 ESX 主机，则可以避免这些问题。

要将 ESX 主机移至其他 vCenter Server，请使用以下过程。

遵循这些步骤:

1. （可选）将“在 vCenter 发现期间允许删除设备模型”选项更改为“否” (p. 33)。

   注意: 仅当原始 vCenter 和目标 vCenter 在同一个 SpectroSERVER 中建模时，才需要执行此步骤。当现有 ESX 主机、ESX 服务控制台和虚拟机模型不再受第一个 vCenter Server 管理时，使用此设置可以保留它们。因此，这些模型的自定义或历史详细信息将保留，并在移动后可用。
2. 打开 VMware 并从第一个 vCenter Server 的管理中删除 ESX 主机。
3. 等待 Virtual Host Manager 在“导航”面板中反映这些更改。

4. 打开 VMware 并将 ESX 主机添加到目标 vCenter Server。

   注意：Virtual Host Manager 无法识别 DSS (请参阅本页中的定义 255)。因此，在将 ESX 主机移至在其他 SpectroSERVER 上建模的 vCenter Server 时，将创建一组新模型。这些模型表示 ESX 主机、ESX 服务控制台和承载的虚拟机。

5. （可选）在原始 vCenter Server 模型上将“在 vCenter 发现期间允许删除设备模型”选项更改回“是”。

   至此，就成功将 ESX 主机从一个 vCenter Server 移到了另一个 vCenter Server。

详细信息：

如何发现和建模虚拟环境 (p. 38)
运行 CA Spectrum 发现 (p. 39)
升级 CA SystemEDGE 模型 (p. 40)
vCenter 发现的工作方式 (p. 41)

查看 VMware 虚拟环境

本节介绍有关查看 VMware 虚拟环境和关联警报的概念。基本步骤与标准 CA Spectrum 步骤相同。但是，本节介绍仅适用于 VMware 虚拟技术的概念差异和详细信息。

查看 VMware 虚拟网络

在“资源管理器”选项卡上，Virtual Host Manager 节点提供了分层树结构。此布局可帮助您可视化虚拟环境资源之间的逻辑关联关系。

使用此信息，可以了解资源在虚拟主机之间的共享情况。此信息可以帮助您发现重新组织和优化虚拟环境的机会。通过此层次结构，还可以快速监控资源性能以及排除警报故障。

由于 Virtual Host Manager 无法识别 DSS 环境 (请参阅本页中的定义 255)，因此它位于格局层次结构中。以下示例显示了 Virtual Host Manager 在“导航”面板中“资源管理器”选项卡上的位置，并演示了虚拟环境的层次结构：

```
[-] SpectroSERVER 主机
    [+] Universe
    [-] Virtual Host Manager
        [-] VMware
            [-] VMware Manager 1
                [-] vCenter server 1
                    [-] 数据中心 1
                        [-] ESX 主机 1
                         。ESX 服务控制台 1
                         。虚拟机 1
                         。虚拟机 2
                [-] vCenter Server 2
                    [-] 数据中心 2
                        [-] ESX 主机 2
                             。ESX 服务控制台 2
                             。虚拟机 3
                             。虚拟机 4
                                [+] 资源池 1
                                 。虚拟机 A
                                 。虚拟机 B
                        [+] 群集 1
                        [-] 群集 2
                            [-] ESX 主机 A
                                 。ESX 服务控制台 A
                             。虚拟机 3
                             。虚拟机 4
                            [-] 资源池 2
                                 。虚拟机 C
                                [+] 资源池 A
                                [+] 资源池 B
                    [+] 数据中心 3
            [-] VMware Manager 2
                [-] vCenter Server 3
                    [-] 数据中心 4
                        [-] ESX 主机 1
                         。ESX 服务控制台 1
                         。虚拟机 1
                         。虚拟机 2
                [-] vCenter Server 4
                    [-] 数据中心 5
                        [-] ESX 主机 2
                             。ESX 服务控制台 2
                             。虚拟机 3
                             。虚拟机 4
```

Virtual Host Manager 是由此 SpectroSERVER 管理的整个虚拟环境的根节点。在“导航”面板中选择此节点后，将在“内容”面板中显示 Virtual Host Manager 详细信息。您可以查看与虚拟环境相关的事件和警报等详细信息。

虚拟环境将直接在 Virtual Host Manager 下表示关联技术的文件夹中进行组织。在上面的示例层次结构中，VMware 文件夹包含使用 VMware 虚拟化技术创建的虚拟环境部分。在此文件夹中，Virtual Host Manager 列出了带有 vCenter Server AIM 的所有 CA SystemEDGE 服务器，以及此 SpectroSERVER 管理的 vCenter Server。这些实体在层次结构中单独表示为 VMware Manager 模型，而且直接在其下方显示 vCenter Server 模型。

在“导航”面板中选择某个 VMware Manager 时，将在“内容”面板中显示相关详细信息，例如，配置、管理的环境和事件。

每个 vCenter server 仅包含它管理的虚拟环境部分。在“导航”面板中选择某个 vCenter Server 时，将在“内容”面板中显示相关详细信息，例如，选定 vCenter Server 的配置和利用率。

在每个 vCenter Server 下，层次结构表示下列虚拟实体之间的逻辑关联关系：

- **数据中心**

  数据中心可以包含群集或主机。在“导航”面板中选择某个数据中心后，将在“内容”面板中显示相关详细信息。这些详细信息包括与数据中心或一组群集相关的事件和警报。各组件可在数据中心内交互，但限制在各数据中心之间进行交互。

- **群集**

  群集可以包含 ESX 主机、资源池或虚拟机。在“导航”面板中选择某个群集后，将在“内容”面板中显示相关详细信息，包括：

  - 与该群集相关的事件和警报。
  - 该群集中包含的 ESX 主机和虚拟机的列表。
  - DRS 和 HA 设置。

- **资源池**

  资源池可以包含虚拟机或其他资源池。在“导航”面板中选择某个资源池后，将在“内容”面板中显示相关详细信息，包括：

  - 总体 CPU 使用率。
  - 与该资源池相关的事件和警报。
  - 该资源池中包含的其他虚拟网络对象的列表。

重要说明！在发现和建模期间将跳过名为“资源”的资源池。此名称仅供内部使用。因此，Virtual Host Manager 会将这些资源池从发现结果中筛选出来。通过为 VMware 资源池指定不同的名称，可以避免缺少资源池的模型以及它们包含的设备。

- **ESX 主机**

  ESX 主机可以包含 ESX 服务控制台、资源池或虚拟机。在“导航”面板中选择某个 ESX 主机后，将在“内容”面板中显示相关详细信息，包括：

  - 总虚拟机内存。
  - CPU 状态。
  - ESX 主机管理的虚拟机的列表。

  注意：当群集中包含 ESX 主机时，将不会在主机下对此主机关联的虚拟机进行分组。相反，这些虚拟机将显示在“资源管理器”选项卡上 ESX 主机旁边的群集中。

- **ESX 服务控制台**

  ESX 服务控制台模型显示为其相应 ESX 主机模型的子项。ESX 服务控制台模型始终为 Virtual Host Manager 层次结构树中的叶节点。此模型具有与其父项相同的名称。“内容”和“组件详细信息”面板中的模型图标用于区分 ESX 服务控制台模型及其父 ESX 主机模型。DeviceType 属性也可区分这些模型。在“导航”面板中选择某个 ESX 服务控制台后，将在“内容”面板中显示相关详细信息。

  注意：ESX 服务控制台模型是 Virtual Host Manager 中唯一不在“信息”选项卡中提供特定于 Virtual Host Manager 的子视图的 VMware 模型类型。

- **虚拟机**

  虚拟机始终为 Virtual Host Manager 层次结构树中的叶节点。在“导航”面板中选择某个虚拟机后，将在“内容”面板中显示相关详细信息，包括电源状态、内存使用率和相关的事件和警报。

详细信息：

虚拟实体类型的自定义子视图 (p. 52)
运行 CA Spectrum 发现 (p. 39)

了解 VMware 虚拟拓扑

为虚拟环境创建的 vCenter Server、ESX 主机、ESX 服务控制台和虚拟机模型将集成到各拓扑视图中。ESX 主机模型会自动分组其关联的 ESX 服务控制台和虚拟机。拓扑将显示这些 ESX 服务控制台和虚拟机如何连接到物理网络实体。

下列示例显示了这些模型在“导航”面板的“资源管理器”选项卡中 Universe 组下的显示方式：

```
[-] Universe
     .  物理交换机 1
     .  物理交换机 2
    [-] ESX 主机
          .  ESX 服务控制台
          .  扇出 1
          .  扇出 2
          .  虚拟机 1
          .  虚拟机 2
          .  虚拟机 3
```

选择这些模型之一后，将在“内容”面板的“拓扑”选项卡上以图形方式显示这些关联关系。

Virtual Host Manager 中的 VMware 数据更新方式

在初始 vCenter 发现期间，CA Spectrum 将使用您的虚拟设备模型填充“导航”面板中的 Virtual Host Manager 层次结构。在 CA Spectrum 构建此初始层次结构之后，可以频繁更改您的虚拟网络配置。Virtual Host Manager 将持续工作，以保持此信息在 CA Spectrum 中是准确的。例如，以下事件可能会更改虚拟网络配置：

- 添加一台新的 vCenter Server，让现有 CA SystemEDGE 进行管理。
- 在 vCenter 应用程序中创建或删除数据中心、群集、资源池、ESX 主机或虚拟机
- VMware 中的 HA 或 DRS 设置，这些设置可使虚拟机自发移动到新的 ESX 主机
- 手动将虚拟机从一个 ESX 主机迁移至另一个 ESX 主机

为了保持信息准确，Virtual Host Manager 通过轮询 vCenter Server AIM 来检测这些更改。因此，如果虚拟网络配置发生更改，则会在每个轮询周期内将这些更改反映到 CA Spectrum 中。CA Spectrum 还会从 AIM 接收陷阱，并生成相应的事件。通过查看事件日志，您可以找出配置发生更改的时间。配置更改示例包括由于 HA 或 DRS 而迁移虚拟设备的情况。在检测到虚拟网络配置中的更改时，CA Spectrum 将执行以下任务：

- 在“资源管理器”选项卡的 Virtual Host Manager 层次结构中，更新虚拟实体模型的放置
- *自动*重新发现与受影响的 ESX 服务控制台和虚拟机模型的连接，并将它们与 Universe 拓扑中的正确 ESX 主机关联

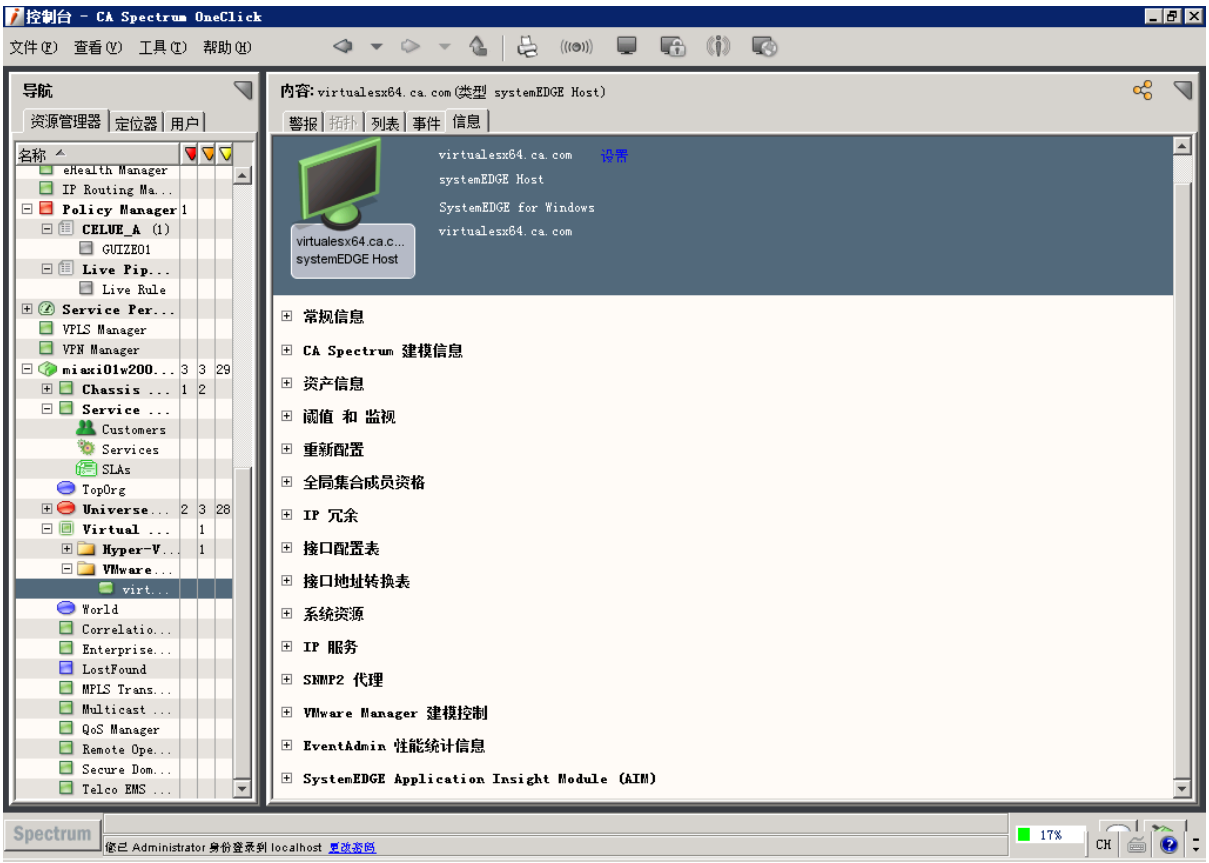
  重要说明！要正确重建与虚拟模型的连接，必须为物理网络中的所有互连路由器和交换机建模。如果在重新发现与虚拟设备的连接之前这些模型不存在，则 CA Spectrum 无法在 Universe 拓扑视图中解析这些连接。ESX 主机将与 CA SystemEDGE 模型放置在同一个 LAN 容器中。

详细信息：

配置和监控资源状态 (p. 62)
Virtual Host Manager 的工作原理 (p. 11)
将 ESX 主机移至其他 vCenter (p. 45)
管理从 vCenter 中删除的设备的设备模型 (p. 33)
查看 VMware 虚拟网络 (p. 46)

虚拟实体类型的自定义子视图

您的各个 Virtual Host Manager 模型将共同提供有关虚拟环境的信息。每个模型将单独提供特定的信息或配置设置，具体取决于其表示的虚拟实体类型。此自定义子视图显示在“内容”面板的“信息”选项卡上。这些子视图可包含实时数据，例如可用磁盘空间或内存利用率。此外，这些子视图还提供对阈值设置的访问。例如，针对群集的自定义子视图是“群集信息”子视图，如下所示：



ESX 服务控制台模型是 Virtual Host Manager 中唯一不提供特定于 Virtual Host Manager 的子视图的 VMware 模型类型。

注意：vCenter 模型为 vCenter 服务器管理的所有虚拟设备提供组合信息。在“导航”面板中选择 VMware Manager 模型，可查看选定管理器的相关信息及其所有实体的组合信息。这些实体包括 vCenter Server、ESX 主机、ESX 服务控制台、虚拟机、虚拟交换机、NIC 和数据存储。此信息与在每个单独实体模型的“信息”选项卡上显示的数据相同。VMware Manager 模型中的组合子视图很好地概览了它管理的所有虚拟实体。

详细信息：

配置和监控资源状态 (p. 62)
查看 VMware 虚拟网络 (p. 46)

用于 VMware 搜索的定位器选项卡

除了在“资源管理器”选项卡上查看有关虚拟环境的详细信息外，还可以使用“定位器”选项卡运行预配置的 Virtual Host Manager 搜索。搜索选项在“定位器”选项卡中的“虚拟主机管理”->“VMware”文件夹下进行分组，如下所示：

这些详细搜索可以帮助您调查仅与虚拟实体（如特定的资源池或 ESX 主机）相关的信息。例如，如果您知道特定 ESX 主机的名称，则可以搜索该主机管理的所有虚拟机。在检查一组虚拟机的状态时，创建此虚拟机列表会很有用。或者，可以使用此列表来确定 VMware 中需要更改管理的计算机。管理更改示例包括将虚拟机移至不同的 ESX 或将它们置于维护模式。

注意：虽然 Virtual Host Manager 无法识别 DSS (请参阅本页中的定义 255)，但是这些预配置搜索允许您在搜索参数中选择多个要搜索的格局。

“导航”面板的“定位器”选项卡中包含针对 Virtual Host Manager 信息的以下搜索：

所有群集

在 CA Spectrum 数据库中查找已为虚拟网络建模的所有群集。

所有数据中心

在 CA Spectrum 数据库中查找已为虚拟网络建模的所有数据中心。

所有 ESX 主机

在 CA Spectrum 数据库中查找已为虚拟网络建模的所有 ESX 主机服务器。

所有资源池

在 CA Spectrum 数据库中查找已为虚拟网络建模的所有资源池。

所有服务控制台

在 CA Spectrum 数据库中查找已为虚拟网络建模的所有 ESX 服务控制台。

所有 vCenter Server

在 CA Spectrum 数据库中查找已为虚拟网络建模的所有 VMware vCenter 主机服务器。

所有虚拟机

在 CA Spectrum 数据库中查找已为虚拟网络建模的所有虚拟机。

所有 VMware Manager

在 CA Spectrum 数据库中查找已为虚拟网络建模且承载已启用 vCenter Server AIM 的 CA SystemEDGE 代理的所有服务器。

群集

在 CA Spectrum 数据库中查找群集。结果将仅限于由下列搜索之一中所指定的容器管理的实体：

- 按 VMWare Manager 名称
- 按 vCenter Server 名称

数据中心

在 CA Spectrum 数据库中查找数据中心。结果将仅限于由下列搜索之一中所指定的容器管理的实体：

- 按 VMWare Manager 名称
- 按 vCenter Server 名称

主机

在 CA Spectrum 数据库中查找 ESX 主机服务器或 ESX 服务控制台。结果将仅限于由下列搜索之一中所指定的容器管理的实体：

- ESX 主机 - 按群集名称
- ESX 主机 - 按数据中心名称
- 按 VMWare Manager 名称
- 按 vCenter Server 名称

资源池

在 CA Spectrum 数据库中查找资源池。结果将仅限于由下列搜索之一中所指定的容器管理的实体：

- 按 VMWare Manager 名称
- 按 vCenter Server 名称

vCenter Server

在 CA Spectrum 数据库中查找 vCenter Server。结果将仅限于由下列搜索之一中所指定的容器管理的那些实体：

- 按 VMWare Manager 名称

虚拟机

在 CA Spectrum 数据库中查找虚拟机。结果将仅限于由下列搜索之一中所指定的容器管理的虚拟机：

- 按群集名称
- 按数据中心名称

- 按主机名
- 按资源池名称
- 按 VMWare Manager 名称
- 按 vCenter Server 名称

详细信息：

查看 VMware 虚拟网络 (p. 46)

状态监控选项

CA Spectrum 提供了多种用于监控虚拟网络资源状态的选项。为资源提供的状态信息将有所不同，具体取决于您监控的虚拟实体的类型。此外，您是否能够配置状态选项取决于其类型。例如，一些状态选项是只读选项，而另外一些状态选项则允许您配置阈值、启用行为或选择警报重要级别。通过提供此系列选项和自定义级别，CA Spectrum 允许您决定如何以最佳方式监控虚拟网络的性能。

状态字段位于 OneClick 子视图中。VMware Manager 模型上以表格格式提供了给定虚拟环境的所有状态信息。此外，在 CA Spectrum 中具有唯一模型的每个虚拟实体类型将提供相同状态信息的子集，以便于查看。可以从任一子视图位置设置与状态相关的设置，包括报警类型、监控器和阈值。

下表概述了为每个虚拟实体类型提供的状态信息的类型。“子视图位置”列介绍了相应状态字段在 OneClick 中的位置。例如，CA Spectrum 允许您监控资源池模型的“内存”信息。为此，您可以从 OneClick 中“信息”选项卡上的“资源池”和“VMware Manager”子视图获取相应的状态字段。要浏览可用于每个状态信息类型的确切状态选项，请在 OneClick 中查找子视图。

数据中心

状态信息类型	子视图位置
总体状态	数据中心和 VMware Manager

资源池

状态信息类型	子视图位置
总体状态	资源池和 VMware Manager
CPU	资源池和 VMware Manager
内存	资源池和 VMware Manager

虚拟机

状态信息类型	子视图位置
就绪百分比	虚拟机和 VMware Manager
CPU	虚拟机和 VMware Manager
内存	虚拟机和 VMware Manager
检测信号	虚拟机和 VMware Manager
电源	虚拟机和 VMware Manager
操作系统状态	虚拟机和 VMware Manager
已连接	虚拟机和 VMware Manager
VMware 工具	虚拟机和 VMware Manager
虚拟 NICs	仅 VMware Manager

ESX 主机

状态信息类型	子视图位置
CPU	ESX 主机和 VMware Manager
传感器 ■ CPU ■ 内存 ■ 风扇 ■ 温度 ■ 电压 ■ 电源	仅 VMware Manager
物理 NICs	仅 VMware Manager

ESX 服务控制台

状态信息类型	子视图位置
内存	ESX 主机和 VMware Manager

数据存储

状态信息类型	子视图位置
可用空间	仅 vCenter
容量	仅 vCenter

vCenter

状态信息类型	子视图位置
总体状态	vCenter
CPU	vCenter
内存	vCenter

详细信息：

针对 VMware 的 Virtual Host Manager 警报 (p. 70)
配置和监控资源状态 (p. 62)

如何配置管理选项

在为虚拟网络建模之后，可以配置 Virtual Host Manager 选项以查看和管理设备模型。通过配置首选项，可帮助确保 Virtual Host Manager 正确处理虚拟设备模型，并仅监控您需要的重要信息。

要配置 Virtual Host Manager 安装，请在发现并建模虚拟网络之后执行以下过程：

- 配置 vCenter Server AIM 选项。这些选项允许您选择 CA SystemEDGE vCenter Server AIM 的设置，例如 vCenter Server AIM 轮询时间间隔及各种陷阱。
- 配置阈值和其他状态监控选项 (p. 62)。这些选项允许您确定要监控的信息，以及 CA Spectrum 如何管理虚拟网络中发生的各种事件。

详细信息：

升级 CA SystemEDGE 模型 (p. 40)

配置 vCenter Server AIM

vCenter Server AIM 与 vCenter 进行通信，以管理和收集有关虚拟网络的信息。在 Virtual Host Manager 中，可以配置 AIM 以确定它处理陷阱与事件的方式。AIM 设置可以帮助您正确平衡要收集的信息与所需的资源量。

要在 Virtual Host Manager 中配置 vCenter Server AIM，请按以下过程操作。

遵循这些步骤:

1. 在“导航”面板中打开 Virtual Host Manager (p. 46)。

   将在选定 Virtual Host Manager 的“内容”面板中打开主详细信息页面。

2. 在“导航”面板的“资源管理器”选项卡上找到并单击 VMware Manager。

   vCenter Server 的相关详细信息将填充到“内容”面板上的各个选项卡中。

3. 单击“信息”选项卡。

4. 展开“SystemEDGE Application Insight Module (AIM)”、“VMware vCenter、“配置”子视图。

5. 根据需要，单击“设置”更改以下字段的设置：

   陷阱启用掩码

   确定 vCenter Server AIM 将发送的陷阱的类。此字段中输入的值用于确定类。值如下所示：

   0

   不发送陷阱。

   1

   发送检测到的 vCenter 更改陷阱。

   2

   发送检测到的 AIM 状态更改陷阱。

   3

   发送检测到的 vCenter 更改陷阱和 AIM 状态更改陷阱。

   4

   仅发送 AIM 配置更改陷阱。

   5

   发送 AIM 配置更改和检测到的 vCenter 更改陷阱。

6

发送 AIM 配置更改陷阱和检测到的 AIM 状态更改陷阱。

7

（默认）发送所有陷阱。

默认值：7

限制：0-7

日志级别

指定写入 vCenter Server AIM 日志文件的信息的级别。这些级别可累积（例如，日志级别 4 将写入从级别 0 到 4 的所有消息）。提供了以下日志级别：

- 0：致命
- 1：关键
- 2：警告
- 3：信息
- 4：调试
- 5：调试（低）
- 6：调试（更低）
- 7：调试（最低）

默认值：2

注意：建议不要将调试级别指定为大于 4。

6. 依次展开“配置”、“实例”子视图。

   将显示一个表，其中包含所有 vCenter Server 实例以及相应的参数。

7. 在“实例”表中，在必要的 vCenter Server 实例上设置以下任意参数。

   轮询时间间隔(秒)

   指定 vCenter Server AIM 在 vCenter Server 中轮询和缓存状态与建模信息的时间间隔（以秒为单位）。此轮询将检索下列状态和建模更新等：

   - 虚拟机已关闭状态
   - ESX 主机已断开连接
   - 新的数据中心可用
   - 新的 ESX 主机
   - 新虚拟机

   默认值： 120

   限制： 大于或等于 30 的数值

   注意： 为获得最佳结果，建议不要将此时间间隔设置为大于 CA Spectrum 轮询周期时间间隔。

   VC 事件轮询(秒)

   指定 vCenter Server AIM 在 vCenter Server 中轮询和缓存事件信息的时间间隔（以秒为单位）。此轮询时间间隔将影响 vCenter 事件队列的轮询。

   默认值： 120

   限制： 大于或等于 120 的数值

   VC 事件启用

   确定 Virtual Host Manager 如何处理从 vCenter Server 和 vCenter Server AIM 收集的事件。提供了以下选项：

   禁用

   指定不收集事件。

   收集

   指定收集事件，但不为具有陷阱的那些事件发送陷阱。

   收集并发送陷阱

   指定收集事件并发送陷阱。

   默认值： 禁用

VC 事件监控器信息

确定是否收集 vCenter 信息事件。选项包括“启用”和“禁用”。

默认值：禁用

VC 事件监控器用户

确定是否收集 vCenter 用户事件。选项包括“启用”和“禁用”。

默认值：禁用

VC 事件监控器错误

确定是否收集 vCenter 错误事件。选项包括“启用”和“禁用”。

默认值：禁用

VC 事件监控器警告

确定是否收集 vCenter 警告事件。选项包括“启用”和“禁用”。

默认值：禁用

将使用您的选择配置 vCenter Server AIM。

详细信息：

如何配置管理选项 (p. 58)

配置和监控资源状态

可以在 OneClick 中监控虚拟资源的状态。例如，可以查看总物理内存、已用物理内存、数据存储可用空间百分比等。此外，还可以设置监控选项，例如，启用报警以及设置陷阱阈值。此信息可以帮助您优化虚拟网络性能以及排除警报故障。

注意：vCenter Server AIM 将设置和管理陷阱，但您可以从 OneClick 子视图中配置这些阈值。在更改任何阈值或设置时，需要使用读取/写入团体字符串。

可以在“信息”选项卡上查看或配置虚拟设备的资源状态选项和信息。

遵循这些步骤:

1. 在“导航”面板中打开 Virtual Host Manager (p. 46)。

   将在选定 Virtual Host Manager 的“内容”面板中打开主详细信息页面。

2. 在“导航”面板的“资源管理器”选项卡上找到并单击虚拟设备。

   将在“内容”面板中显示设备的详细信息。

3. 单击“信息”选项卡。

   可查看多个子视图。通常，该选项卡底部的子视图中包括选定模型的资源分配和利用率信息。例如，数据中心模型将显示一个名为“数据中心信息”的子视图。此子视图中包括您在“导航”面板中选择的特定数据中心模型的详细信息。

4. 展开相应的子视图。

   将显示选定设备模型的所有可用资源状态详细信息和监控选项。

   注意： VMware Manager 模型提供由 VMware Manager 管理的所有虚拟设备的组合信息。在“导航”面板中选择 VMware Manager 模型，可查看有关 vCenter Server 的信息以及其中所有实体的相关组合信息。这些实体包括 ESX 主机、ESX 服务控制台、虚拟机、虚拟交换机、NIC 和数据存储。此信息与在每个单独实体模型的“信息”选项卡上显示的数据相同。VMware Manager 模型中的组合子视图很好地概览了它管理的所有虚拟实体。

详细信息：

针对 VMware 的 Virtual Host Manager 警报 (p. 70)
如何配置管理选项 (p. 58)
虚拟实体类型的自定义子视图 (p. 52)

控制 vCenter Server AIM 轮询

在调整 Virtual Host Manager 性能时，可以更改 vCenter Server 轮询速率，也可以禁用 vCenter 轮询。默认情况下，vCenter Server 设备模型上的轮询属性用于控制 VMware 相关的轮询行为。或者，也可以单独更改此 VMware 相关的轮询行为。vCenter 应用程序模型 VMWareVCAIMApp 用于控制 VMware 相关轮询。

此应用程序上的以下两个属性值专门用于控制 VMware 轮询逻辑：

- PollingStatus
- Polling_Interval

vCenter Server 和 VMWareVCAIMApp 应用程序模型中都包含这些属性。PollingStatus 用于启用和禁用轮询，而 Polling_Interval 用于控制轮询频率。如果它们的值不同，则优先考虑 VMWareVCAIMApp 应用程序模型属性值。

如上所述，CA Spectrum 允许您分别为设备模型和应用程序模型设置值。此功能允许您独立于 vCenter Server 设备轮询微调 VMware 相关轮询。对于这两个属性，如果它们的值相同，则在 vCenter Server 设备模型上修改属性时也会更改相应的应用程序模型属性。

详细信息：

vCenter 发现的工作方式 (p. 41)

配置 vCenter Server 轮询时间间隔

可以更改 vCenter Server 轮询速率以提高或降低频率。通过在 vCenter 应用程序模型上设置 Polling_Interval 属性来配置轮询时间间隔。

遵循这些步骤:

1. 打开 OneClick，并单击“导航”面板中的“定位器”选项卡。
2. 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。
3. 在“设备 IP 地址”字段中输入 vCenter Server 的 IP 地址，然后单击“确定”。

   将在“内容”面板中显示 vCenter Server 的应用程序模型的列表。
4. 选择 VMWareVCAIMApp 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. 单击“组件详细信息”面板中的“信息”选项卡。
6. 双击 CA Spectrum 的“建模信息”子视图。
7. 在“轮询时间间隔(秒)”字段中单击“设置”，然后输入新值。

   注意：如果值为 0，则将禁用 vCenter Server 轮询。

   vCenter Server 轮询时间间隔设置即已配置。

禁用 vCenter Server 轮询

可以禁用 vCenter 轮询。禁用 vCenter 轮询的过程与禁用 Virtual Host Manager 的过程相同。可以通过在 vCenter 应用程序模型上设置 PollingStatus 属性来禁用轮询。

要禁用应用程序模型上的 vCenter Server 轮询，请使用以下过程。

遵循这些步骤:

1. 打开 OneClick，并单击“导航”面板中的“定位器”选项卡。
2. 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。
3. 在“设备 IP 地址”字段中输入 vCenter Server 的 IP 地址，然后单击“确定”。

   将在“内容”面板中显示 vCenter Server 的应用程序模型的列表。
4. 选择 VMWareVCAIMApp 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. 单击“组件详细信息”面板中的“信息”选项卡。
6. 单击 CA Spectrum 的“建模信息”子视图。
7. 在“轮询”字段中单击“设置”，然后选择“关闭”。

   将为选定的 vCenter Server 禁用轮询。

禁用针对虚拟机的 DNS 查找

自 9.4 版本起，您可以禁用针对没有 IP 地址的虚拟机的 DNS 查找。您可能会出现不希望 CA Spectrum 针对没有 IP 地址的虚拟机执行 DNS 查找的情况。在这些情况下，您可以在 OneClick 中以 Virtual Host Manager 级别将属性“VMWare_vmDNSLookuponBlankIPAddr”设置为“No”。如果此属性设置为“No”，CA Spectrum 将跳过针对没有 IP 地址的虚拟机的 DNS 查找。这样就不会在 OneClick 中填充此类虚拟机的 IP 地址。

如果此属性设置为“Yes”，CA Spectrum 将执行 DNS 查找，找到没有 IP 地址的虚拟机的 IP 地址。如果 CA Spectrum 找到该虚拟机的 IP 地址，将在 OneClick 中自动填充此 IP 地址。

删除 Virtual Host Manager 模型

通常，您可以随时从 OneClick 中删除模型。但是，Virtual Host Manager 会限制您在“导航”面板的 Virtual Host Manager 层次结构中删除模型的能力。要手动删除模型，有以下两个选项可用：

- 在 Virtual Host Manager 中删除 VMware 文件夹或 vCenter Server 模型
- 使用 vCenter 从 VMware 虚拟环境中删除虚拟实体

在 Virtual Host Manager 中，有时会自动删除模型。下列情况会导致 CA Spectrum 自动删除 Virtual Host Manager 模型：

- **删除 VMware 文件夹或 VMware Manager 模型**

  如果删除 VMware Manager 模型或 VMware 文件夹，CA Spectrum 将会删除所有相关的子模型。删除的模型集包括与远程 VMware Manager 模型相关的 vCenter Server 模型。

- **从 VMware 中删除实体**

  在 VMware 中删除数据中心、资源池、群集、ESX 主机和虚拟机时，CA Spectrum 还会从 Virtual Host Manager 中删除这些模型及其子模型。

- **Virtual Host Manager 中禁用的数据中心**

  如果禁用对数据中心的管理，CA Spectrum 将删除与该数据中心相关的子模型。

- **存在已升级模型** - 在某些情况下，会首先为无 SNMP 功能的 Virtual Host Manager 创建 ESX 服务控制台或虚拟机模型。如果以后向 VHM 模型 (请参阅本页中的定义 255)添加 SNMP 功能，则之前的模型将被删除，并替换为支持 SNMP 的新模型。

注意：虽然默认设置是删除模型，但是您可以配置 Virtual Host Manager 以保留模型。在这种情况下，当从 Virtual Host Manager 中删除 ESX 主机、ESX 服务控制台和虚拟机模型时，Virtual Host Manager 会将它们放置在 LostFound 容器中。从 VMware 中删除实体或在 Virtual Host Manager 中禁用数据中心时，将应用此设置。在删除 VMware 文件夹或 VMware Manager 模型时，不会应用此设置。删除 VMware Manager 和 vCenter Server 模型或者升级 VHM 模型时，也不会应用此设置。

详细信息：

在 SNMP 和 vCenter 发现进程后创建的重复模型 (p. 247)
向 VHM 模型中添加 SNMP 功能 (p. 42)
管理从 vCenter 中删除的设备的设备模型 (p. 33)
删除 VMware Manager 后管理启用了 SNMP 的虚拟机模型 (p. 37)

分布式选择性管理

本节介绍有关在 vCenter Server 上有选择性地管理各个数据中心的概念和过程。本节还介绍如何跨多个 SpectroSERVER 分布式管理数据中心。

选择性数据中心建模

默认情况下，每个 vCenter Server 模型将监控它在虚拟环境中管理的所有数据中心。Virtual Host Manager 允许您选择仅监控这些数据中心的子集。要执行选择性建模，您可以配置每个 vCenter Server 模型，以便对它管理的各个数据中心启用或禁用建模。

此功能提供以下优势：

- 组织可以为无需监控的数据中心禁用管理功能，例如实验室环境。
- Virtual Host Manager 可以分布式管理虚拟环境。

详细信息：

分布式管理虚拟环境 (p. 68)

如何有选择性地管理数据中心

默认情况下，每个 vCenter Server 模型将监控它在虚拟环境中管理的所有数据中心。但是，您可以配置 vCenter Server 模型，以监控数据中心的子集。如果您具有无需监控的数据中心（例如实验室环境），则此功能十分有用。

以下过程介绍如何配置 vCenter Server 以仅监控选定的数据中心：

1. 选择您的首选项，以便在 Virtual Host Manager 中自动为数据中心建模 (p. 32)。此设置将在步骤 3 中用作数据中心模型的默认设置。
2. 为 vCenter Server 建模 (p. 39)。
3. 在每个 vCenter Server 上启用选定数据中心以进行监控。vCenter Server 仅会为已启用建模的数据中心及其包含的组件建模。

分布式管理虚拟环境

通过使用选择性数据中心建模功能，可跨多个 SpectroSERVER 分布式管理数据中心。对于具有在地理上分散的网络或大型虚拟环境的大型组织，潜在优势包括：

- 提高 Virtual Host Manager 性能 - 可跨多个 SpectroSERVER 分布建模每个数据中心所需的资源。理想情况下，建议使用单个 SpectroSERVER 进行建模，以减少从多个服务器轮询所需的资源。但是，如果单个 SpectroSERVER 无法有效地管理虚拟环境，则分布式环境可以提高 Virtual Host Manager 性能，尽管需要其他轮询资源。
- 组织灵活性 - 由于存在组织性或地理性边界，您可能希望跨多个 SpectroSERVER 分布式管理数据中心。

可以通过先在单独 SpectroSERVER 上为 vCenter Server 建模来完成分布式管理。在每个 SpectroSERVER 环境中，您可以有选择性地启用或禁用由每个 vCenter Server 管理的数据中心。

例如，在以下两个 SpectroSERVER 上为“cas”vCenter Server 建模：SS_1 和 SS_2。在完成 vCenter 发现后，Virtual Host Manager 发现“cas”管理以下三个数据中心：

- DCenter-A
- DCenter-B
- DCenter-C

在每个 SpectroSERVER 上，可以为“CA”配置数据中心建模，如下所示：

数据中心	SS_1 上的 cas	SS_2 上的 cas
DCenter-A	已启用	已禁用
DCenter-B	已启用	已禁用
DCenter-C	已禁用	已启用

在此方案中，将跨两个 SpectroSERVER 对“cas”的数据中心执行分布式管理。

重要说明！分布式数据中心管理不是可扩展的解决方案。对于在 SpectroSERVER 上建模的每个 vCenter Server，Virtual Host Manager 必须在每个轮询时间间隔期间轮询*所有*数据中心的数据。因此，即使您对某个数据中心禁用建模，Virtual Host Manager 也会轮询该数据中心。要在轮询时最大程度地减少重复，请注意有多少 SpectroSERVER 对同一 vCenter Server 进行建模。

详细信息：

选择性数据中心建模 (p. 67)

如何分布式管理虚拟环境

为帮助改善 Virtual Host Manager 性能或组织，可以使用选择性数据中心建模功能。分布式管理跨多个 SpectroSERVER 分布数据中心建模。

分布式管理过程类似于选择性数据中心建模过程，但是包含一些其他步骤，如下所示：

1. 选择您的首选项，以便在 Virtual Host Manager 中自动为数据中心建模 (p. 32)。在分布式数据中心管理环境中，必须决定如何处理添加到 VMware 的新数据中心。在配置 Virtual Host Manager 进行数据中心管理时，可使用以下两个选项：

   - 在所有 SpectroSERVER 上禁用自动数据中心建模 - 在这种情况下，您必须手动为希望 Virtual Host Manager 监控的所有新数据中心建模。虽然它需要手动建模，但是此选项可帮助确保 Virtual Host Manager 仅监控需要管理的数据中心。
   - 在一个 SpectroSERVER 上启用自动数据中心建模，并为所有其他 SpectroSERVER 禁用建模 - 此选项可确保在一个 SpectroSERVER 上为所有新数据中心建模。建议使用此选项，以便不会忘记重要的网络组件。在 Virtual Host Manager 中显示数据中心模型之后，您可以根据需要手动将其管理移至其他 SpectroSERVER。

   重要说明！ 不要在多个 SpectroSERVER 上启用自动数据中心建模。Virtual Host Manager 将在多个 SpectroSERVER 上为所有新数据中心建模，从而导致重复，这将会影响 Virtual Host Manager 性能。

2. 为 vCenter Server 建模 (p. 39)。确保在其中管理 vCenter Server 的一个或多个数据中心的每个 SpectroSERVER 上为此 vCenter Server 建模。
3. 在每个 SpectroSERVER 的每个 vCenter Server 上启用选定数据中心以进行监控。vCenter Server 仅会为已启用建模的数据中心及其包含的组件建模。
4. 配置 CA SystemEDGE 代理以将陷阱发送到每个 SpectroSERVER (p. 70)。为确保正确地监控数据中心，必须将陷阱发送到在其中建模 vCenter Server 的所有 SpectroSERVER 中。

分布式数据中心环境中的陷阱管理

要监控数据中心及其组件，相关陷阱必须访问在其中管理每个数据中心的 SpectroSERVER。在分布式数据中心管理方案中，配置 CA SystemEDGE 代理以将陷阱发送到在其中建模 vCenter Server 的每个 SpectroSERVER 中。

在正确配置后，CA Spectrum 会将 vCenter Server AIM 生成的所有陷阱发送到这些 SpectroSERVER。每个 SpectroSERVER 将筛选陷阱，并丢弃为数据中心生成的陷阱，且*不会*在该 SpectroSERVER 上为数据中心的组件建模。仅与建模的数据中心组件相关的陷阱才会生成事件和警报。

注意：有关在 vCenter Server AIM 上配置陷阱的详细信息，请参阅《*CA Virtual Assurance for Infrastructure Managers 实施指南*》。

VMWare 的警报和故障隔离

本节介绍 Virtual Host Manager 所使用的陷阱以及生成的警报。本节还说明 Virtual Host Manager 故障隔离与基础 CA Spectrum 故障隔离有何差异。

针对 VMware 的 Virtual Host Manager 警报

为了就虚拟网络中出现的问题向您报警，CA Spectrum 将生成警报。将以两种方式创建警报：

- 从 CA SystemEDGE 代理发送的陷阱
- 轮询

通过轮询可生成两种警报：“已关闭/已挂起”和“代理已丢失/不可用”。但是，有几个陷阱可以在虚拟设备上生成警报。CA Spectrum 支持由 vCenter Server AIM 从 CA SystemEDGE 代理发送的所有陷阱。为了优化这些陷阱，可以单独为每个虚拟设备配置阈值。

如果某个陷阱违反阈值并生成警报，CA Spectrum 将使用通过陷阱传递的“状态”varbind 的值来确定警报重要级别。所有状态 varbind 具有以下可能的值（将接收相同的 CA Spectrum 警报）：

- 0：未知
- 1：正常
- 2：警告
- 3：关键

CA Spectrum 将这些 vCenter 状态映射到 CA Spectrum 警报重要级别，如下所示：

vCenter 状态	CA Spectrum 警报重要级别
0：未知	清除
1：正常	清除
2：警告	次要（黄色）
3：关键	主要（橙色）

详细信息：

配置和监控资源状态 (p. 62)
管理从 vCenter 中删除的设备的设备模型 (p. 33)
删除 VMware Manager 后管理启用了 SNMP 的虚拟机模型 (p. 37)

CA Spectrum 如何从 CA SystemEDGE 转发陷阱

CA Spectrum 支持由 vCenter Server AIM 发送的所有陷阱。最初会将这些陷阱发送给 vCenter CA SystemEDGE 模型。如果陷阱的目标不是 vCenter 模型，则 CA Spectrum 会将陷阱转发给正确的虚拟模型。

注意：对于与陷阱相关的特定事件代码，请使用事件配置应用程序并针对“0x056e”进行筛选。或者，可以启动 MIB 工具以便在“EMPIRE-CAVMVCA-MIB”MIB 的“陷阱支持”表中查看陷阱。有关使用事件配置应用程序的详细信息，请参阅《*事件配置用户指南*》。有关使用 MIB 工具的详细信息，请参阅《*IT 基础架构建模与管理 - 管理员指南*》。

CA Spectrum 使用以下过程确定要将陷阱转发到的位置：

1. CA Spectrum 在接收到陷阱时会将实体类型的 UID 映射到已知的 varbind 位置。

   注意：对于主机传感器陷阱，CA Spectrum 将使用虚拟实体名称而不是 UID。如果多个主机具有相同的 vCenter 名称，则 CA Spectrum 将映射到第一个条目。

2. CA Spectrum 使用此 UID 来查找并定位与给定 UID 相关的 CA Spectrum 模型。将预先确定所有陷阱的实体类型。CA Spectrum 将根据查找结果按如下所示转发陷阱：

   - 如果它使用给定 UID 找到特定类型的 CA Spectrum 模型，CA Spectrum 会将事件和相应警报转发给目标模型。
   - 如果对于给定 UID 它找不到 CA Spectrum 模型，CA Spectrum 将在 vCenter 模型上生成新的常规事件 (0x56e109f)。此新事件包含以下详细信息：
     - 陷阱详细信息
     - 搜索的实体类型
     - 通过尝试查找模型信息而获取的其他信息

     注意：如果在 vCenter 中更改虚拟网络实体之后立即发送陷阱，CA Spectrum 通常会找不到相关模型。vCenter 发现尚未在 CA Spectrum 中标识和创建相应的模型。

Virtual Host Manager 中支持的陷阱

CA Spectrum 中支持 vCenter Server AIM 生成的所有陷阱。这些陷阱最初会发送给 vCenter 模型。然后，根据陷阱类型，陷阱会被转发到相应的虚拟实体类型（即“目标”实体）。通过使用这些陷阱，您可以监控虚拟网络的性能，解决生成的所有警报或触发事件。

注意：有关 vCenter Server AIM 所生成陷阱的详细信息，请参阅《*CA Virtual Assurance for Infrastructure Managers 管理指南*》和《*CA Virtual Assurance for Infrastructure Managers 管理指南*》。

下表列出了特定目标实体类型的陷阱，并指定陷阱是否生成警报。

群集陷阱

陷阱名称	陷阱 OID	生成警报？
vmvcAimClusterHADRSChangeTrap	1.3.6.1.4.1.546.1.1.0.165253	否
vmvcAimClusterRenamedTrap	1.3.6.1.4.1.546.1.1.0.165254	否
vmvcAimClusterDRSConfigChangeTrap	1.3.6.1.4.1.546.1.1.0.165255	否

数据中心陷阱

陷阱名称	陷阱 OID	生成警报？
vmvcAimDCRenamedTrap	1.3.6.1.4.1.546.1.1.0.165248	否
vmvcAimDCConfigChangeTrap	1.3.6.1.4.1.546.1.1.0.165249	否
vmvcAimDCOverallStateChangeTrap	1.3.6.1.4.1.546.1.1.0.165240	是
vmvcAimDCTotalCPUStateChangeTrap	1.3.6.1.4.1.546.1.1.0.165245	是
vmvcAimDCTotalMEMStateChangeTrap	1.3.6.1.4.1.546.1.1.0.165250	是

ESX 主机陷阱

陷阱名称	陷阱 OID	生成警报？
vmvcAimHostCpuStateChangeTrap	1.3.6.1.4.1.546.1.1.0.165208	是
vmvcAimHostTotalCpuStateChangeTrap	1.3.6.1.4.1.546.1.1.0.165209	是
vmvcAimHostTotalMemStateChangeTrap	1.3.6.1.4.1.546.1.1.0.165210	是
vmvcAimHostConfigChangeTrap	1.3.6.1.4.1.546.1.1.0.165212	否
vmvcAimHostTotalVMCpuStateChangeTrap	1.3.6.1.4.1.546.1.1.0.165213	是
vmvcAimHostThresholdChangeTrap	1.3.6.1.4.1.546.1.1.0.165215	否
vmvcAimHostVMotionTrap	1.3.6.1.4.1.546.1.1.0.165218	否
vmvcAimHostConnectionStateTrap	1.3.6.1.4.1.546.1.1.0.165219	否**
vmvcAimHostTotalVMMemStateChangeTrap	1.3.6.1.4.1.546.1.1.0.165220	是
vmvcAimPNICStateChangeTrap	1.3.6.1.4.1.546.1.1.0.165241	是
vmvcAimPNICAddedTrap	1.3.6.1.4.1.546.1.1.0.165242	否
vmvcAimPNICRemovedTrap	1.3.6.1.4.1.546.1.1.0.165243	否
vmvcAimPNICConfigChangeTrap	1.3.6.1.4.1.546.1.1.0.165244	否
vmvcAimHostDiskAddedTrap	1.3.6.1.4.1.546.1.1.0.165291	否
vmvcAimHostDiskRemovedTrap	1.3.6.1.4.1.546.1.1.0.165292	否
vmvcAimCPUSensorStateChangeTrap*	1.3.6.1.4.1.546.1.1.0.165281	是
vmvcAimMemSensorStateChangeTrap*	1.3.6.1.4.1.546.1.1.0.165282	是
vmvcAimFanSensorStateChangeTrap*	1.3.6.1.4.1.546.1.1.0.165283	是
vmvcAimVoltageSensorStateChangeTrap*	1.3.6.1.4.1.546.1.1.0.165284	是
vmvcAimTempSensorStateChangeTrap*	1.3.6.1.4.1.546.1.1.0.165285	是
vmvcAimPowerSensorStateChangeTrap*	1.3.6.1.4.1.546.1.1.0.165286	是

陷阱名称	陷阱 OID	生成警报？
vmvcAimHostFTConfigChangeTrap	1.3.6.1.4.1.546.1.1.0.165955	否
vmvcAimHostPowerStateTrap	1.3.6.1.4.1.546.1.1.0.165910	否
vmvcAimStatVMSRMStatusChangeTrap	1.3.6.1.4.1.546.1.1.0.165969	否

*vCenter ESX 主机名用于在 CA Spectrum 中查找 ESX 主机模型。如果存在两个具有相同名称的 ESX 主机模型，CA Spectrum 将在匹配该名称的第一个模型上生成警报。

**这些陷阱不会生成警报，因为 CA Spectrum vCenter 轮询智能将在下一个 vCenter 轮询周期中检测并生成这些警报。

ESX 服务控制台陷阱

陷阱名称	陷阱 OID	生成警报？
vmvcAimHostMemStateChangeTrap	1.3.6.1.4.1.546.1.1.0.165211	是
vmvcAimHostMemOtherStateChangeTrap	1.3.6.1.4.1.546.1.1.0.165214	是

注意：将使用 ESX 主机模型的“主机信息”子视图来配置用于生成这些陷阱的阈值。

资源池陷阱

陷阱名称	陷阱 OID	生成警报？
vmvcAimResourcePoolCpuStateChangeTrap	1.3.6.1.4.1.546.1.1.0.165258	是
vmvcAimResourcePoolConfigChangeTrap	1.3.6.1.4.1.546.1.1.0.165259	否
vmvcAimResourcePoolRenamedTrap	1.3.6.1.4.1.546.1.1.0.165260	否
vmvcAimResourcePoolMemStateChangeTrap	1.3.6.1.4.1.546.1.1.0.165264	是
vmvcAimResourcePoolHealthStateChangeTrap	1.3.6.1.4.1.546.1.1.0.165265	是
vmvcAimResourcePoolVCConfigChangeTrap	1.3.6.1.4.1.546.1.1.0.165962	否

vCenter Server 陷阱

CA Spectrum 将在 VMware Manager 和 vCenter Server 模型上断言 vCenter Server 陷阱，或者仅在 vCenter Server 模型上断言 vCenter Server 陷阱，具体取决于您的 CA SystemEDGE 部署方案。

陷阱名称	陷阱 OID	生成警报？
vmvcAimServerStateChangeTrap	1.3.6.1.4.1.546.1.1.0.165201	是
vmvcAimVCCPUStateChangeTrap	1.3.6.1.4.1.546.1.1.0.165203	是
vmvcAimVCMemStateChangeTrap	1.3.6.1.4.1.546.1.1.0.165206	是
vmvcAimHostAddedTrap***	1.3.6.1.4.1.546.1.1.0.165216	否

陷阱名称	陷阱 OID	生成警报？
vmvcAimHostRemovedTrap***	1.3.6.1.4.1.546.1.1.0.165217	否
vmvcAimVMAddedTrap***	1.3.6.1.4.1.546.1.1.0.165222	否
vmvcAimVMRemovedTrap***	1.3.6.1.4.1.546.1.1.0.165223	否
vmvcAimVMMigratedTrap***	1.3.6.1.4.1.546.1.1.0.165230	否
vmvcAimDCAddedTrap***	1.3.6.1.4.1.546.1.1.0.165246	否
vmvcAimDCRemovedTrap***	1.3.6.1.4.1.546.1.1.0.165247	否
vmvcAimClusterAddedTrap***	1.3.6.1.4.1.546.1.1.0.165251	否
vmvcAimClusterRemovedTrap***	1.3.6.1.4.1.546.1.1.0.165252	否
vmvcAimResourcePoolAddedTrap***	1.3.6.1.4.1.546.1.1.0.165256	否
vmvcAimResourcePoolRemovedTrap***	1.3.6.1.4.1.546.1.1.0.165257	否
vmvcAimTemplateAddedTrap	1.3.6.1.4.1.546.1.1.0.165261	否
vmvcAimTemplateRemovedTrap	1.3.6.1.4.1.546.1.1.0.165262	否
vmvcAimTemplateRenamedTrap	1.3.6.1.4.1.546.1.1.0.165263	否
vmvcAimCustomizationSpecAddedTrap	1.3.6.1.4.1.546.1.1.0.165266	否
vmvcAimCustomizationSpecRemovedTrap	1.3.6.1.4.1.546.1.1.0.165267	否
vmvcAimDatastoreAddedTrap	1.3.6.1.4.1.546.1.1.0.165271	否
vmvcAimDatastoreRemovedTrap	1.3.6.1.4.1.546.1.1.0.165272	否
vmvcAimDatastoreAccessibleStateChangeTrap	1.3.6.1.4.1.546.1.1.0.165273	是
vmvcAimDatastoreConfigChangeTrap	1.3.6.1.4.1.546.1.1.0.165274	否
vmvcAimDatastoreRenamedTrap	1.3.6.1.4.1.546.1.1.0.165275	否
vmvcAimDatastoreFreeSpaceStateChangeTrap	1.3.6.1.4.1.546.1.1.0.165276	是
vmvcAimDCFolderAddedTrap	1.3.6.1.4.1.546.1.1.0.165277	否
vmvcAimDCFolderRemovedTrap	1.3.6.1.4.1.546.1.1.0.165278	否
vmvcAimDCFolderConfigChangeTrap	1.3.6.1.4.1.546.1.1.0.165279	否
vmvcAimSnapshotAddedTrap	1.3.6.1.4.1.546.1.1.0.165287	否
vmvcAimSnapshotRemovedTrap	1.3.6.1.4.1.546.1.1.0.165288	否
vmvcAimSnapshotCurrentUpdateTrap	1.3.6.1.4.1.546.1.1.0.165289	否

陷阱名称	陷阱 OID	生成警报？
vmvcAimSCSIControllerAddedTrap	1.3.6.1.4.1.546.1.1.0.165296	否
vmvcAimSCSIControllerRemovedTrap	1.3.6.1.4.1.546.1.1.0.165297	否
vmvcAimServerTotalCPUStateChangeTrap	1.3.6.1.4.1.546.1.1.0.165293	是
vmvcAimServerTotalMemStateChangeTrap	1.3.6.1.4.1.546.1.1.0.165294	是
vmvcAimServerTotalDSFreeSpaceStateChangeTrap	1.3.6.1.4.1.546.1.1.0.165295	是
vmvcAimVSwitchStateChangeTrap	1.3.6.1.4.1.546.1.1.0.165235	是
vmvcAimVMGuestDiskAddedTrap	1.3.6.1.4.1.546.1.1.0.165920	否
vmvcAimVMGuestDiskRemovedTrap	1.3.6.1.4.1.546.1.1.0.165921	否
vmvcAimVMGuestDiskStateChangeTrap	1.3.6.1.4.1.546.1.1.0.165922	否
vmvcAimVMGuestDiskConfigChangeTrap	1.3.6.1.4.1.546.1.1.0.165923	否
vmvcAimStorageSensorStateChangeTrap	1.3.6.1.4.1.546.1.1.0.165905	是

***这些事件在 vCenter Server 上生成，因为 vCenter 发现进程会在通过 CA Spectrum 管理发现或删除的每个实体上生成类似事件。

VMware Manager 陷阱

陷阱名称	陷阱 OID	生成警报？
vmvcAimServerReadyTrap	1.3.6.1.4.1.546.1.1.0.165200	否
vmvcAimVCConfigChangeTrap	1.3.6.1.4.1.546.1.1.0.165202	否
vmvcAimVCThresholdChangeTrap	1.3.6.1.4.1.546.1.1.0.165204	否
vmvcAimVCEventReceivedTrap	1.3.6.1.4.1.546.1.1.0.165205	否
vmvcAimVSwitchAddedTrap	1.3.6.1.4.1.546.1.1.0.165915	否
vmvcAimVSwitchRemovedTrap	1.3.6.1.4.1.546.1.1.0.165916	否
vmvcAimVSwitchConfigChangeTrap	1.3.6.1.4.1.546.1.1.0.165917	否
vmvcAimHostVNICAddedTrap	1.3.6.1.4.1.546.1.1.0.165925	否
vmvcAimHostVNICRemovedTrap	1.3.6.1.4.1.546.1.1.0.165926	否
vmvcAimPortGroupAddedTrap	1.3.6.1.4.1.546.1.1.0.165930	否
vmvcAimPortGroupRemovedTrap	1.3.6.1.4.1.546.1.1.0.165931	否
vmvcAimPortGroupVCConfigChangeTrap	1.3.6.1.4.1.546.1.1.0.165932	否
vmvcAimDistribVSwitchAddedTrap	1.3.6.1.4.1.546.1.1.0.165935	否

陷阱名称	陷阱 OID	生成警报？
vmvcAimDistribVSwitchRemovedTrap	1.3.6.1.4.1.546.1.1.0.165936	否
vmvcAimDistribVSwitchStateChangeTrap	1.3.6.1.4.1.546.1.1.0.165937	是
vmvcAimDistribVSwitchConfigChangeTrap	1.3.6.1.4.1.546.1.1.0.165938	否
vmvcAimDistribVSwitchVCConfigChangeTrap	1.3.6.1.4.1.546.1.1.0.165939	否
vmvcAimDVPortGroupAddedTrap	1.3.6.1.4.1.546.1.1.0.165940	否
vmvcAimDVPortGroupRemovedTrap	1.3.6.1.4.1.546.1.1.0.165941	否
vmvcAimDVPortGroupVCConfigChangeTrap	1.3.6.1.4.1.546.1.1.0.165942	否
vmvcAimDVUplinkPortGroupAddedTrap	1.3.6.1.4.1.546.1.1.0.165943	否
vmvcAimDVUplinkPortGroupRemovedTrap	1.3.6.1.4.1.546.1.1.0.165944	否
vmvcAimDVUplinkPortGroupVCConfigChangeTrap	1.3.6.1.4.1.546.1.1.0.165945	否
vmvcAimDistribVSwitchPortPolicyChangeTrap	1.3.6.1.4.1.546.1.1.0.165950	否
vmvcAimDVPortGroupPortPolicyChangeTrap	1.3.6.1.4.1.546.1.1.0.165951	否
vmvcAimCustSpecNICAddedTrap	1.3.6.1.4.1.546.1.1.0.165960	否
vmvcAimCustSpecNICRemovedTrap	1.3.6.1.4.1.546.1.1.0.165961	否
vmvcAimVAppAddedTrap	1.3.6.1.4.1.546.1.1.0.165963	否
vmvcAimVAppRemovedTrap	1.3.6.1.4.1.546.1.1.0.165964	否
vmvcAimVAppVCConfigChangeTrap	1.3.6.1.4.1.546.1.1.0.165965	否
vmvcAimVMAddedTovAppTrap	1.3.6.1.4.1.546.1.1.0.165966	否
vmvcAimVMRemovedFromvAppTrap	1.3.6.1.4.1.546.1.1.0.165967	否
vmvcAimVMvAppVCConfigChangeTrap	1.3.6.1.4.1.546.1.1.0.165968	否
vmvcAimNetFolderAddedTrap	1.3.6.1.4.1.546.1.1.0.165970	否
vmvcAimNetFolderRemovedTrap	1.3.6.1.4.1.546.1.1.0.165971	否
vmvcAimNetFolderConfigChangeTrap	1.3.6.1.4.1.546.1.1.0.165972	否
vmvcAimCustomizationSpecChangeTrap	1.3.6.1.4.1.546.1.1.0.165280	否
vmvcAimCustSpecNICChangeTrap	1.3.6.1.4.1.546.1.1.0.165973	否

虚拟机陷阱

陷阱名称	陷阱 OID	生成警报？
vmvcAimVMCpuStateChangeTrap	1.3.6.1.4.1.546.1.1.0.165221	是
vmvcAimVMConfigChangeTrap	1.3.6.1.4.1.546.1.1.0.165224	否

陷阱名称	陷阱 OID	生成警报？
vmvcAimVMThresholdChangeTrap	1.3.6.1.4.1.546.1.1.0.165225	否
vmvcAimVMPercentReadyTrap	1.3.6.1.4.1.546.1.1.0.165226	是
vmvcAimVMRenamedTrap	1.3.6.1.4.1.546.1.1.0.165227	否
vmvcAimVMBehaviourChangeTrap	1.3.6.1.4.1.546.1.1.0.165228	否
vmvcAimVMConnectionStateChangeTrap	1.3.6.1.4.1.546.1.1.0.165229	否**
vmvcAimVMNICStateChangeTrap	1.3.6.1.4.1.546.1.1.0.165231	是
vmvcAimVMNICAddedTrap	1.3.6.1.4.1.546.1.1.0.165232	否
vmvcAimVMNICRemovedTrap	1.3.6.1.4.1.546.1.1.0.165233	否
vmvcAimVMNICConfigChangeTrap	1.3.6.1.4.1.546.1.1.0.165234	否
vmvcAimVMVDiskStateChangeTrap	1.3.6.1.4.1.546.1.1.0.165236	是
vmvcAimVMVDiskAddedTrap	1.3.6.1.4.1.546.1.1.0.165237	否
vmvcAimVMVDiskRemovedTrap	1.3.6.1.4.1.546.1.1.0.165238	否
vmvcAimVMVDiskConfigChangeTrap	1.3.6.1.4.1.546.1.1.0.165239	否
vmvcAimVMMemStateChangeTrap	1.3.6.1.4.1.546.1.1.0.165268	是
vmvcAimVMPowerStateChangeTrap	1.3.6.1.4.1.546.1.1.0.165269	否**
vmvcAimVMHBStateChangeTrap	1.3.6.1.4.1.546.1.1.0.165270	否
vmvcAimVMFTConfigChangeTrap	1.3.6.1.4.1.546.1.1.0.165956	否
vmvcAimVMFTFailoverTrap	1.3.6.1.4.1.546.1.1.0.165957	是
vmvcAimVMVCConfigChangeTrap	1.3.6.1.4.1.546.1.1.0.165958	否
vmvcAimVMVDiskSizeChangeTrap	1.3.6.1.4.1.546.1.1.0.165902	否

**这些陷阱不会生成警报，因为 CA Spectrum vCenter 轮询智能将在下一个 vCenter 轮询周期中检测并生成这些警报。

详细信息：

配置和监控资源状态 (p. 62)
如何配置管理选项 (p. 58)
CA Spectrum 如何从 CA SystemEDGE 转发陷阱 (p. 71)

用于虚拟网络的故障管理

故障隔离旨在缩小导致网络问题的根本原因的范围。通过查找根本原因，可以帮助您排除故障并快速更正问题，或使用自动化脚本以编程方式更正问题。确定哪些设备是导致警报的根本原因可能非常困难，因为单个设备中的问题会导致网络中的多个设备生成事件。

例如，与 ESX 主机失去联系通常意味着也与 ESX 管理的虚拟机失去联系。因此，ESX 设备模型和所有受影响的虚拟机都将生成警报。通过使用故障隔离技术，Virtual Host Manager 将关联这些警报以确定单个根本原因。

虚拟网络可提供独特的管理机会，因为它们针对 CA Spectrum 提供了备用管理视角。CA Spectrum 可通过直接与您的虚拟设备联系或通过虚拟网络管理应用程序 VMware vCenter 来收集信息。这种备用管理视角可通过两种方式来增强标准 CA Spectrum 故障管理：

- **增强失去联系警报** - 两个设备信息源可帮助 Virtual Host Manager 查明原因，并更轻松地将事件与单个根本原因关联。
- **代理故障警报** - *代理管理*是指使用备用管理源（代替主要管理器或与主要管理器一起）来管理网络设备的行为。例如，CA Spectrum 可通过直接与虚拟网络设备联系或使用虚拟技术应用程序与设备联系来管理这些虚拟网络设备。当 vCenter 与虚拟网络设备失去联系时，Virtual Host Manager 将为每个设备生成“失去代理管理”警报。这些警报具有唯一性，提醒您通过*代理*对设备执行的*管理*（而不是设备或直接 (SNMP) 管理的状态）受到影响。

丢失设备联系时故障隔离的工作方式

为了帮助您排除设备中的网络问题，CA Spectrum 使用故障隔离来缩小警报根本原因的范围。对于虚拟网络，Virtual Host Manager 将使用通过与设备直接联系获取的信息，以及由 vCenter 通过 vCenter Server AIM 提供的信息。在许多情况下，标准 CA Spectrum 故障管理可以查明根本原因。但是在一些特殊情况下，无法使用标准方法来隔离虚拟网络中的问题。

Virtual Host Manager 用于发现根本原因的故障隔离类型取决于生成警报的设备，以及设备生成的事件类型。下列方案介绍了两种独特的故障管理情况，以及 CA Spectrum 如何确定虚拟网络中的网络错误。

方案 1：虚拟机已关闭或已挂起

在虚拟环境中，与 CA Spectrum 通过标准设备监控发现的信息相比，虚拟管理应用程序可以提供更多的详细信息。例如，管理应用程序可发现虚拟机何时被置于下列模式之一：

- 已关闭
- 已挂起

如果虚拟机处于这些模式之一，并且与 CA Spectrum 失去联系，但是 ESX 主机的代理管理 (请参阅本页中的定义 255)未中断，则 CA Spectrum 将按如下所示确定根本原因：

1. 当 CA Spectrum 与虚拟机失去联系时，将生成“失去联系”警报。
2. 在其下一个轮询周期中，vCenter Server 模型将轮询 vCenter Server AIM 以收集有关虚拟机的信息。由于 vCenter 管理虚拟机，因此它可提供导致虚拟机所生成警报的可能原因的相关信息。
3. 如果 vCenter 发现虚拟机已关闭或已挂起，它将生成相应的警报。

   注意：在虚拟机启动后的第一个 vCenter 轮询周期中，将清除“已关闭”和“挂起”警报。
4. Virtual Host Manager 会将这些“已关闭”和“挂起”警报与 CA Spectrum 所创建的相应“失去联系”警报关联。Virtual Host Manager 将使“失去联系”警报显示为“已关闭”和“挂起”警报的症状。

方案 2：ESX 主机关闭

如果 CA Spectrum 与已建模的 ESX 服务控制台以及该主机上运行的所有虚拟机失去联系，它将检查上游路由器和交换机的状态。根据它们的状态，CA Spectrum 将按如下所示确定根本原因：

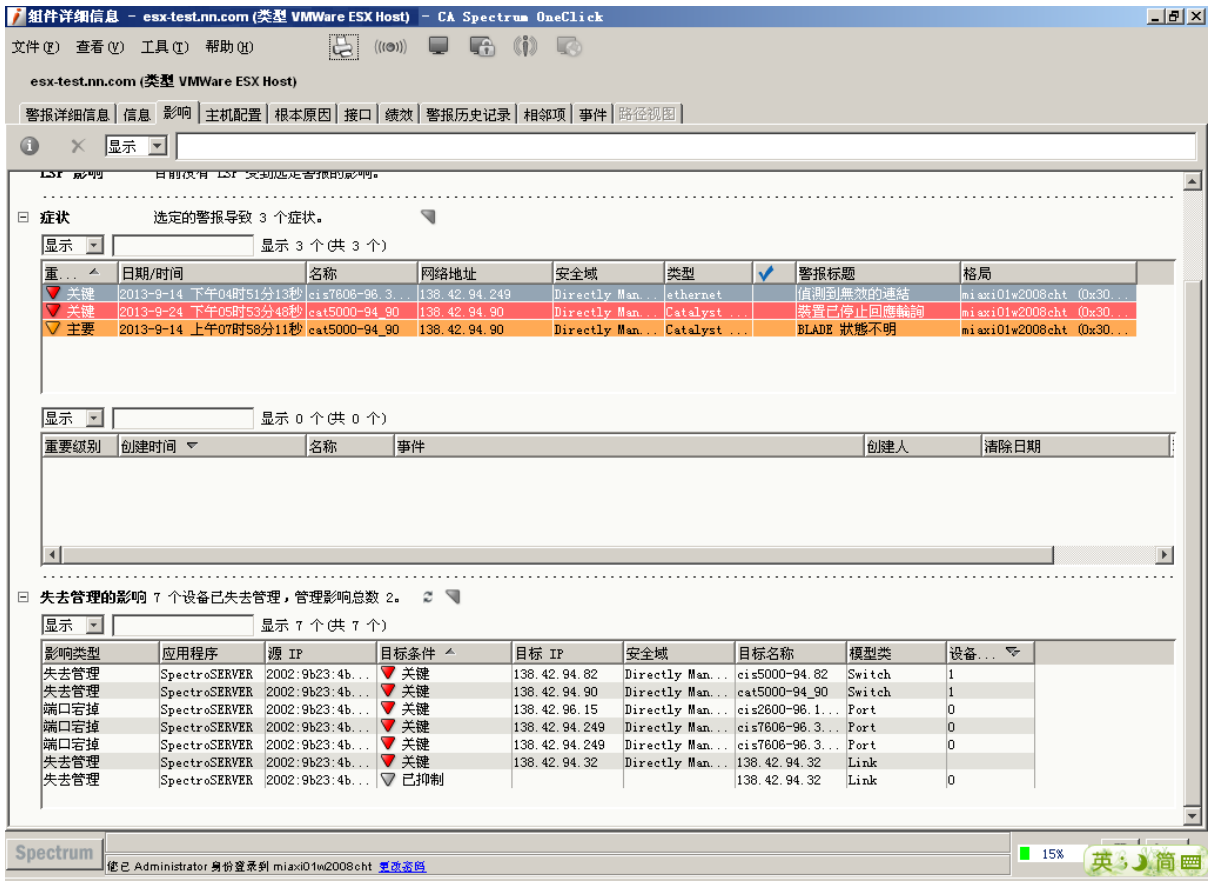
- 一个或多个虚拟机或 ESX 服务控制台的所有上游设备都不可用 - 标准 CA Spectrum 故障隔离技术将按如下所示确定根本原因：
  - “设备已停止响应轮询”警报 - 当任何虚拟机或 ESX 服务控制台的至少一个上游连接设备启动时在 ESX 主机上生成。
  - “网关不可访问”警报 - 当*所有*上游连接设备都关闭时在 ESX 主机上生成。
- 对于连接到 ESX 主机的每个虚拟机和 ESX 服务控制台模型，至少有一个上游设备可用 - CA Spectrum 推断 ESX 主机是根本原因，并按如下所示进行响应：
  a. ESX 服务控制台模型和直接连接到 ESX 服务控制台模型或虚拟机模型的 所有虚拟机、端口及扇出设备将生成标准故障隔离警报。
  b. Virtual Host Manager 为 ESX 主机模型创建“物理主机关闭”警报。

c. 为受影响设备（如虚拟机、ESX 服务控制台、端口和扇出）创建的所有故障隔离相关警报将关联到“物理主机关闭”警报，从而使它们成为“物理主机关闭”警报的症状。这些症状警报显示在“物理主机关闭”警报的“影响”选项卡上的“症状”表中。

注意：对于每个 ESX 主机模型，Virtual Host Manager 将创建一个“虚拟故障域”。此域中包括 ESX 主机、ESX 服务控制台和虚拟机，以及直接连接到 ESX 服务控制台模型或虚拟机的所有端口和扇出。当 ESX 主机生成“物理主机关闭”警报时，域中的所有标准故障隔离警报将与其关联。将这些警报作为症状关联可表明 ESX 主机上的“物理主机关闭”警报是根本原因。

d. “影响”选项卡上针对“物理主机关闭”警报的“失去管理的影响”表中列出了所有受影响设备。

注意：被抑制的设备在“症状”表中没有对应的警报，因此下列示例虽然仅显示了两个警报，但涉及六个受影响的设备：



e. 如果一个或多个虚拟机或 ESX 服务控制台的所有上游设备都已关闭，则 CA Spectrum 无法再可靠地指出故障是否源于 ESX 主机。因此，CA Spectrum 将清除“物理主机关闭”警报，并应用标准 CA Spectrum 故障隔离技术。

详细信息：

确定受 ESX 停机影响的虚拟机 (p. 84)

丢失代理管理时故障隔离的工作方式

用于创建虚拟网络的 VMware vCenter 应用程序为 CA Spectrum 提供了独特的管理机会。CA Spectrum 可以使用标准方法来直接联系您的虚拟设备，此外，CA Spectrum 可以同时从 vCenter 收集虚拟设备信息。从这个意义上讲，vCenter 是 CA Spectrum 可从其收集虚拟设备信息的“代理”。如果 CA Spectrum 与设备失去直接联系，则将生成警报。同样，如果 vCenter 与虚拟设备失去联系，或者如果 Virtual Host Manager 与 vCenter 应用程序失去联系，Virtual Host Manager 将生成警报 -“失去代理管理”警报 (请参阅本页中的定义 255)。

作为响应，CA Spectrum 将尝试隔离导致代理管理故障的原因。代理故障隔离类似于标准 CA Spectrum 故障隔离，不过，这些报警将提醒您虚拟设备的*代理*管理会受到影响。代理管理故障隔离无法指明虚拟设备是已启动还是已关闭。但是，了解何时失去通过代理进行的联系非常重要，因为您可能会丢失设备的重要虚拟信息。

Virtual Host Manager 用于发现根本原因的代理故障隔离类型取决于生成警报的设备，以及设备生成的事件类型。下列方案介绍了两种独特的代理故障管理情况，以及 Virtual Host Manager 如何确定虚拟网络中的网络错误。

方案 1：vCenter 与 ESX 之间失去联系

如果 vCenter 与其管理的一个 ESX 主机失去联系，则有关该 ESX 及承载的所有虚拟设备的 vCenter 数据将丢失。为了隔离该问题，Virtual Host Manager 将按如下所示确定根本原因：

1. 将在 ESX 主机、ESX 服务控制台、承载的所有虚拟机以及在该 ESX 中定义的任何资源池上生成“失去代理管理”警报。
2. 虚拟机警报将与 ESX“失去代理管理”警报关联，使它们成为 ESX 警报的症状。将这些警报作为症状关联可表明 ESX 警报是根本原因。
3. 如果 CA Spectrum 也与 ESX 主机失去联系并生成“物理主机关闭”警报，则为 ESX 生成的“失去代理管理”警报将与“物理主机关闭”警报关联。在这种情况下，“失去代理管理”警报成为“物理主机关闭”警报的症状。将此警报作为症状关联可表明 ESX 上的“物理主机关闭”警报是根本原因。

方案 2：CA Spectrum 与 vCenter 之间失去联系

如果 CA Spectrum 与 vCenter 模型失去联系，CA Spectrum 将丢失该 vCenter Server 管理的所有虚拟模型的 vCenter 数据。为了隔离该问题，Virtual Host Manager 将按如下所示确定根本原因：

1. CA Spectrum 将为该 vCenter Server 管理的所有虚拟模型（包括虚拟机、ESX 主机、ESX 服务控制台、数据中心、资源池和群集）生成“失去代理管理”警报。CA Spectrum 还将在 vCenter Server 模型上生成单独的“代理不可用”警报。
2. 虚拟机警报将与其相应的 ESX 模型警报关联。
3. ESX、数据中心、资源池和群集警报将与 vCenter 模型“代理不可用”警报关联。
4. vCenter 警报将与标准 CA Spectrum 故障管理生成的其他警报关联，例如为下列情况创建的警报：
   - vCenter 失去管理（即远程 SystemEDGE 代理发生问题）
   - 失去计算机联系
   - vCenter 处于维护模式

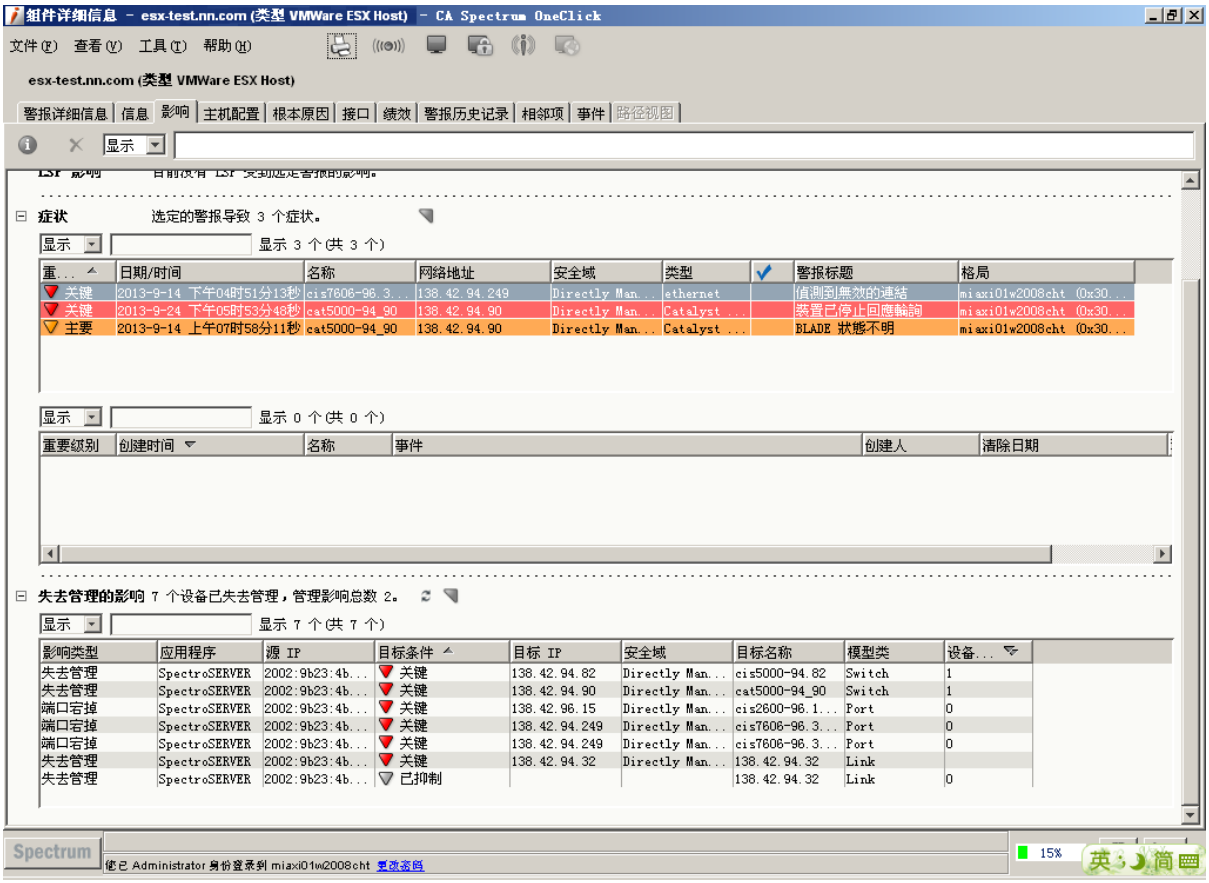
详细信息：

丢失设备联系时故障隔离的工作方式 (p. 79)

确定受 ESX 停机影响的虚拟机

当与 ESX 的联系中断或者 ESX 关闭时，该 ESX 承载的所有虚拟机都将受到影响。由于 vCenter 无法与 ESX 进行通信以获取使用情况信息，因此您可能不会接收到该 ESX 上承载的关键虚拟机的警报。要确定关键虚拟机是否受影响，请访问警报的“影响”选项卡上受影响虚拟机的列表。提供了以下视图：

- “症状”视图 - 显示受影响的虚拟机生成的所有症状警报
- “失去管理的影响”视图 - 列出受警报影响的虚拟机



详细信息：

丢失设备联系时故障隔离的工作方式 (p. 79)

第 4 章： Solaris Zones

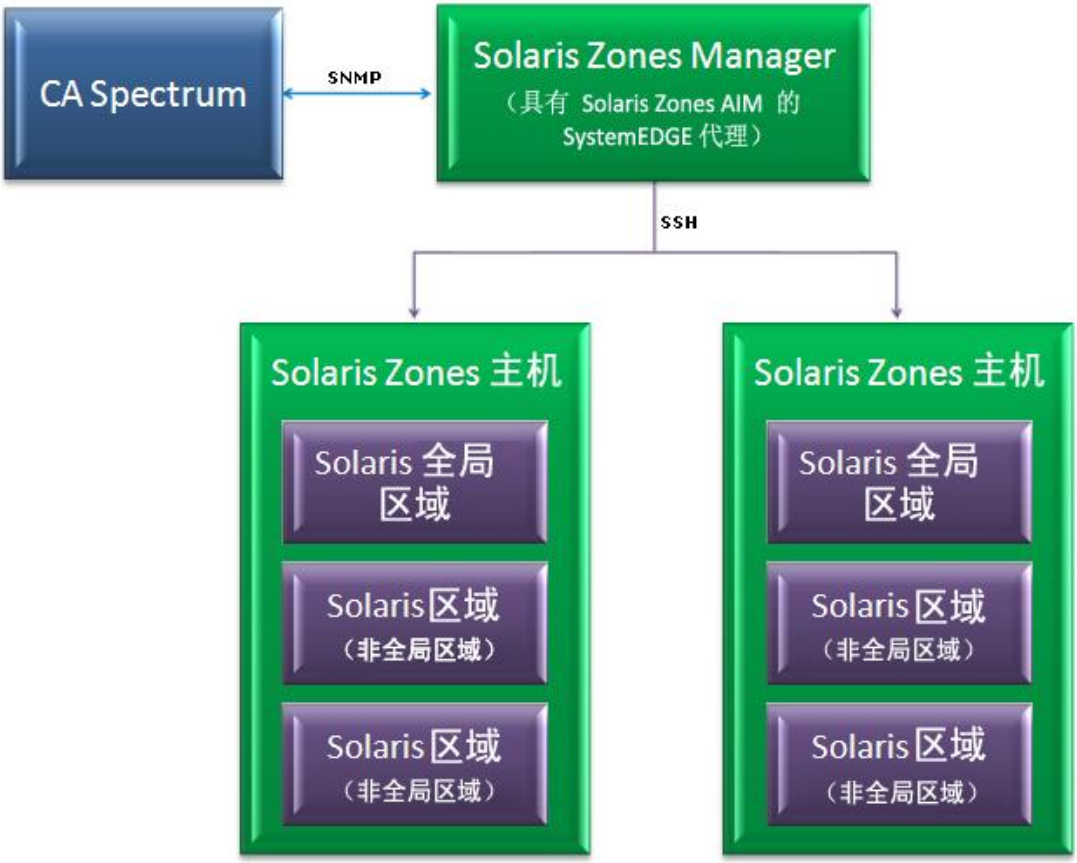
本节适用于 Solaris Zones 虚拟化技术用户，将介绍如何使用 Virtual Host Manager 来管理通过 Solaris Zones 创建的虚拟实体。

此部分包含以下主题：

Virtual Host Manager 如何使用 Solaris 区域

Virtual Host Manager 可以无缝地监控您的虚拟网络实体和物理网络实体。您可以全面了解网络情况，并在网络中排除这两类实体的网络问题。虽然虚拟网络实体的行为与物理组件的行为类似，但是对这些实体的监控过程不同于一般 CA Spectrum 监控过程。了解此过程的工作原理可帮助您找到并解决与虚拟网络相关的网络问题。

Virtual Host Manager 中的 *Solaris Zones Manager* 是已启用 Solaris Zones AIM 的 CA SystemEDGE 代理。Solaris Zones Manager 负责报告所有已配置的 Solaris 区域。Virtual Host Manager 与 Solaris Zones Manager 进行通信，以收集有关 Solaris Zones 虚拟环境的详细信息。下图显示了 CA Spectrum 如何使用 Solaris Zones Manager 收集有关 Solaris Zones 虚拟环境的信息：



如图所示，收集有关 Solaris Zones 虚拟环境的信息的过程如下：

1. 每个 Solaris Zones 主机中的 Solaris 全局区域与其包含的每个 Solaris 区域（即非全局区域）进行通信。
2. Solaris Zones Manager 使用 SSH 与每个 Solaris 全局区域进行通信，以收集有关虚拟环境的详细信息。
3. CA Spectrum 定期与 Solaris Zones Manager 进行通信以检索此信息。Solaris Zones Manager 安装有已启用 Solaris Zones AIM 的 CA SystemEDGE 代理。CA Spectrum 使用 SNMP 与 CA SystemEDGE 代理进行通信，并使用此信息在 CA Spectrum 中建模和监控虚拟环境。

详细信息：

Virtual Host Manager 的工作原理 (p. 11)
了解虚拟拓扑 (p. 109)
Virtual Host Manager 中的 Solaris Zones 数据更新方式 (p. 113)

为 Solaris Zones 创建的模型

Virtual Host Manager 提供了多个模型来表示 Solaris Zones 虚拟技术网络的组件。通过了解以下基本模型，可以帮助您更好地了解发现以及虚拟环境与物理环境的连接方式：

- **Solaris Zones Manager**

  每个 Solaris Zones Manager 表示一个包含已加载 Solaris Zones AIM 的 CA SystemEDGE 代理的服务器。

- **Solaris Zones 主机**

  *Solaris Zones 主机*表示由 Virtual Host Manager 管理的 Solaris 主机的物理硬件。这些模型充当 Universe 拓扑中的容器模型，以帮助将虚拟实体分组到单独的视图中，同时显示虚拟环境与物理网络的连接情况。不能直接联系 Solaris Zones 主机以获取状态信息。而是将通过模型中所含项目的状态来推断这些模型的状态。

- **Solaris 全局区域**

  *Solaris 全局区域*是在 Solaris Zones 主机上运行的管理操作系统，Solaris Zones 使用它来配置所承载的 Solaris 区域实例。Solaris 全局区域模型为 Virtual Host Manager 提供了一种收集有关 Solaris Zones 虚拟环境的信息的方法。

- **Solaris 区域**

  *Solaris 区域*是由在 Solaris Zones 主机上运行的 Virtual Host Manager 管理的非全局区域实例。

详细信息：

查看 Solaris Zones 虚拟环境 (p. 109)

Solaris Zones 入门

本节介绍 Virtual Host Manager 的配置和建模过程。通常，管理员仅对每个安装执行一次这些任务。

如何配置发现选项

在安装 Virtual Host Manager 后，可以配置 Virtual Host Manager 以执行 Solaris Zones 发现。通过配置首选项，可帮助确保 Virtual Host Manager 正确地为虚拟设备建模。

要为 Solaris Zones 发现配置 Virtual Host Manager 安装，请从下列选项中选择首选项：

- 新 Solaris 区域的维护模式 (p. 88) - 允许您决定在可使用 CA Spectrum 来管理新发现的 Solaris 区域实例之前将其中哪些实例置于维护模式。
- 允许在运行 Solaris Zones 发现期间删除设备模型 (p. 89) - 控制当 Solaris Zones 虚拟化技术模型不再受 Virtual Host Manager 管理时，CA Spectrum 如何处理它们。
- 搜索现有模型 (p. 90) - 确定在 Solaris Zones 发现期间 Virtual Host Manager 搜索的安全域。
- 发现支持 SNMP 的设备 (p. 92) - 控制如何在 Solaris Zones 发现期间为支持 SNMP 的设备建模。默认情况下，最初仅会将新模型创建为 VHM 模型。但是，此选项允许您覆盖默认设置，并为符合必要标准的设备立即创建 SNMP 模型。
- 在执行 Solaris Zones Manger 删除期间保留启用了 SNMP 的 Solaris Zones (p. 93) - 控制在删除 Solaris Zones Manager 模型时，CA Spectrum 如何处理启用了 SNMP 的 Solaris 区域模型。

为新 Solaris 区域实例配置维护模式

Virtual Host Manager 会在 Solaris Zones 虚拟环境中自动为 Solaris 区域实例建模。CA Spectrum 将尝试管理所有已发现的模型。但是，在最初建模某些新 Solaris 区域时，它们尚未准备好由 CA Spectrum 管理。例如，未运行的 Solaris 区域将导致 CA Spectrum 生成“失去联系”警报。为阻止在新 Solaris 区域模型上生成不需要的警报，您可以决定将哪些新模型立即置于维护模式。之后，可以在准备好由 CA Spectrum 管理这些设备时手动禁用维护模式。

遵循这些步骤:

1. 在“导航”面板中打开 Virtual Host Manager (p. 109)。

   将在选定 Virtual Host Manager 的“内容”面板中打开主详细信息页面。

2. 单击“信息”选项卡。
3. 展开“配置”、“Solaris Zones”、“Solaris Zones 发现”子视图。

4. 在“新 Solaris 区域的维护模式”字段中单击“设置”，然后选择下列选项之一：

   将未运行的 Solaris 区域置于维护模式

   （默认）在初始 Solaris Zones 发现期间，仅向未运行的 Solaris 区域模型应用维护模式。

   将所有 Solaris 区域置于维护模式

   在初始 Solaris Zones 发现期间，向所有新 Solaris 区域模型应用维护模式。

   将保存您的设置，并且会根据您的选择将 Virtual Host Manager 创建的新 Solaris 区域实例置于维护模式。

详细信息：

如何配置发现选项 (p. 88)
状态监控选项 (p. 116)

管理从 Solaris 中删除的设备的设备模型

虚拟环境中的设备及设备间的关联关系会频繁地发生更改。在 CA Spectrum 中维护有关虚拟环境的准确且及时的数据很具挑战性。例如，删除 Solaris Zones 主机或 Solaris 区域实例时，CA Spectrum 会在“导航”面板中从 Virtual Host Manager 删除相应的设备模型。但是，CA Spectrum 是应保留还是删除模型？您可以选择设置以控制是否删除模型。

重要说明！删除模型时，这些模型上的所有注释或其他自定义也将丢失。如果以后可能会在 Solaris Zones 环境中重新创建模型，则可以禁用此选项。

遵循这些步骤:

1. 在“导航”面板中打开 Virtual Host Manager (p. 109)。

   将在选定 Virtual Host Manager 的“内容”面板中打开主详细信息页面。

2. 单击“信息”选项卡。
3. 展开“配置”、“Solaris Zones”、“Solaris Zones 发现”子视图。

4. 在“允许在运行 Solaris Zones 发现期间删除设备模型”字段中单击“设置”，然后选择下列选项之一：

   是

   （默认）删除不再受 Solaris Zones 环境管理的实体的对应 Virtual Host Manager 模型。

   否

   如果 Virtual Host Manager 模型的对应实体不再受 Solaris Zones 环境管理，则将这些模型放置在 LostFound 容器中。

   注意：将以不同的方式处理具有更多关联的模型（如全局集合中包括的模型）。将从 Universe 中删除这些模型，但是不会将其移动到 LostFound 容器中。

   将保存您的设置，并且会在从 Solaris Zones 环境中删除设备之后相应地处理设备模型。

详细信息：

如何配置发现选项 (p. 88)
删除 Virtual Host Manager 模型 (p. 108)
针对 Solaris Zones 的 Virtual Host Manager 警报 (p. 119)
Virtual Host Manager 中支持的陷阱 (p. 121)
将 Solaris 区域实例移至新的 Solaris Zones 主机 (p. 102)
在 Solaris Zones 模型上生成了重复的 MAC、不同的 IP 地址警报 (p. 248)
删除 Solaris Zones Manager 后管理启用了 SNMP 的 Solaris 区域模型 (p. 93)

跨安全域配置模型搜索

Solaris Zones 发现将尝试查找 SpectroSERVER 中存在的模型，而不是创建新模型。在已部署 Secure Domain Manager 的环境中，Solaris Zones 发现将搜索与 Solaris Zones Manager 位于同一个安全域中的模型。此域是“本地”域。但是，某些虚拟环境设备可存在于不同的安全域中。在这种情况下，可以配置 Solaris Zones 发现以搜索所有安全域中的现有模型。

遵循这些步骤:

1. 在“导航”面板中打开 Virtual Host Manager (p. 46)。

   将在选定 Virtual Host Manager 的“内容”面板中打开主详细信息页面。

2. 单击“信息”选项卡。
3. 展开“配置”、“Solaris Zones”、“Solaris Zones 发现”子视图。

4. 在“搜索现有模型”字段中单击“设置”。
5. 从以下选项中进行选择：

   在区域管理器的安全域中

   （默认）搜索与 Solaris Zones Manager 服务器位于同一个安全域中的现有模型。

   在所有安全域中

   搜索由 SpectroSERVER 管理的所有安全域中的现有模型。仅在下列情况下选择此选项：

   - 所有设备具有唯一的 IP 地址。
   - 当安全域用于安全目的或用于隔离网络通信时。

   注意：不要为 NAT 环境选择此选项。

   将保存您的设置。Solaris Zones 发现会在 CA Spectrum 中搜索与您的选择匹配的现有模型。当多个安全域中存在重复的模型（共享相同 IP 地址的模型）时，Virtual Host Manager 将执行以下操作：

   - 在本地安全域中选择模型（如果有）。
   - 如果本地域中不存在重复的模型，Virtual Host Manager 将随机地从其他安全域中选择模型。
   - 在这两种情况下，Virtual Host Manager 将在 Solaris Zones Manager 模型上为重复的 IP 地址生成次要警报。

详细信息：

如何配置发现选项 (p. 88)

配置 SNMP 建模首选项

支持 SNMP 的设备可支持丰富的设备监控功能，如进程和文件系统监控功能。但是，部署 SNMP 代理可能会花费较高的经济和时间成本。默认情况下，Solaris Zones 发现将 Solaris 全局区域和 Solaris 区域实例创建为 VHM 模型 (请参阅本页中的定义 255)。可在以后将它们升级为 SNMP 模型。不过，也可以将 Solaris Zones 发现配置为将所有支持 SNMP 的新设备建模为 SNMP 模型。虽然完成 Solaris Zones 发现可能需要更长的时间，但是初始建模为 SNMP 模型可避免以后手动升级这些模型。

重要说明！在为 Solaris Zones 主机建模*之前*，请启用 SNMP 建模。如果首先为 Solaris Zones 主机建模，则会将所有子模型创建为 VHM 模型，并且必须手动将其升级为 SNMP 模型。

遵循这些步骤:

1. 在“导航”面板中打开 Virtual Host Manager (p. 46)。

   将在选定 Virtual Host Manager 的“内容”面板中打开主详细信息页面。

2. 单击“信息”选项卡。

3. 展开“配置”、“Solaris Zones”、“Solaris Zones 发现”、“SNMP 发现”子视图。

   重要说明！要准备设备和 CA Spectrum 以执行 SNMP 发现，请按照子视图中的步骤操作。如果在执行 Solaris Zones 发现之前未正确准备设备，Virtual Host Manager 将无法创建 SNMP 模型。

4. 在“发现支持 SNMP 的设备”字段中单击“设置”，然后选择下列选项之一：

   是

   在 Solaris Zones 发现期间启用 SNMP 建模。仅会将符合“SNMP 发现”子视图文本中指定标准的设备建模为 SNMP 设备。仅适用于*新*模型。

   否

   （默认）将 Solaris Zones 发现期间找到的所有新设备建模为 VHM 模型。可在以后手动将这些模型升级为 SNMP 模型。

   将保存您的设置，并且会根据您的选择在 Virtual Host Manager 中为新设备建模。

详细信息：

如何发现和建模虚拟环境 (p. 94)
Solaris Zones 发现的工作方式 (p. 97)
向 VHM 模型添加 SNMP 功能 (p. 99)
删除 Solaris Zones Manager 后管理启用了 SNMP 的 Solaris 区域模型 (p. 93)

删除 Solaris Zones Manager 后管理启用了 SNMP 的 Solaris 区域模型

默认情况下，删除以下项时，将从 CA Spectrum 中删除启用了 SNMP 的设备：

- 设备的 Solaris Zones Manager 模型
- “导航”面板中的 Solaris Zones 文件夹

启用了 SNMP 的设备模型可包括要保留的重要自定义。可以调整设置以避免删除这些模型。将它们放置在 LostFound 容器中供以后使用。

遵循这些步骤:

1. 在“导航”面板中打开 Virtual Host Manager (p. 46)。

   将在选定 Virtual Host Manager 的“内容”面板中打开主详细信息页面。

2. 单击“信息”选项卡。
3. 展开“配置”、“Solaris Zones”、“Solaris Zones 发现”子视图。
4. 在“在执行 Solaris Zones Manager 删除期间保留启用了 SNMP 的 Solaris Zones”字段中单击“设置”，然后选择下列选项之一：

   是

   删除其 Solaris Zones Manager 或 Solaris Zones 文件夹时，将启用了 SNMP 的 Solaris 区域模型保留在 LostFound 容器中。

   注意：将以不同的方式处理具有更多关联的模型（如全局集合中包括的模型）。将从 Universe 中删除这些模型，但是不会将其移动到 LostFound 容器中。

   否

   （默认）删除其 Solaris Zones Manager 或 Solaris Zones 文件夹时，将删除所有 Solaris 区域模型。

   将保存您的设置，并且会在删除 Solaris Zones Manager 模型或 Solaris Zones 文件夹时相应地处理启用了 SNMP 的设备模型。

详细信息：

如何配置发现选项 (p. 88)
管理从 Solaris 中删除的设备的设备模型 (p. 89)
删除 Virtual Host Manager 模型 (p. 108)

如何发现和建模虚拟环境

要监控虚拟环境，需发现并建模虚拟实体 - Solaris Zones 主机、Solaris 全局区域和 Solaris 区域实例。通过在 Virtual Host Manager 中为这些实体建模，可以在一个工具中查看完整的网络拓扑，其中显示了物理组件和虚拟组件之间的关联关系。

为虚拟环境建模的主要步骤如下所示：

1. 运行标准的 CA Spectrum 发现 (p. 95)。

   此发现的目的是确保在运行 Solaris Zones 发现之前为上游路由器和交换机建模。或者，如果已禁用“SNMP 建模”选项，则此步骤也可以为支持 SNMP 的 Solaris 全局区域和 Solaris 区域建模。在为这些实体建模时，请确保正确设置建模选项以支持 Virtual Host Manager。

2. 升级 CA SystemEDGE 模型 (p. 96)。

   只有已在早于 CA Spectrum r9.1.2 的版本中为 Solaris Zones Manager 主机上的 CA SystemEDGE 代理建模后，才需要执行此步骤。

3. 允许运行 Solaris Zones 发现 (p. 97)。

   在 Solaris Zones Manager 主机上为带有 Solaris Zones AIM 的 CA SystemEDGE 代理建模时，将自动启动 Solaris Zones 发现。其中每个 Solaris Zones Manager 模型都具有自己的 Solaris Zones 发现进程。Solaris Zones 发现的目的是找到 Solaris Zones 环境中的虚拟实体，为不存在的实体建模，以及将它们放置在“导航”面板的 Virtual Host Manager 视图中。

详细信息：

如何配置管理选项 (p. 103)
将 Solaris 区域实例移至新的 Solaris Zones 主机 (p. 102)
在 Solaris Zones 模型上生成了重复的 MAC、不同的 IP 地址警报 (p. 248)
向 VHM 模型添加 SNMP 功能 (p. 99)
配置 SNMP 建模首选项 (p. 92)

运行 CA Spectrum 发现

要发现您的 Solaris Zones 环境，请运行标准 CA Spectrum 发现。此发现可确保为上游路由器和交换机建模，以便将来可以从虚拟实体建立连接。您还可以在 CA Spectrum 发现期间为支持 SNMP 的 Solaris 全局区域和 Solaris 区域实例建模。

注意：仅当在 Solaris Zones 发现期间禁用了“SNMP 建模”选项时，才需要在 CA Spectrum 发现期间为支持 SNMP 的 Solaris 全局区域和 Solaris 区域实例建模。

注意：只有管理员才可以执行此任务。

遵循这些步骤:

1. 打开发现控制台。

   注意：在建模之前，请确保您知道在非标准端口上运行的任何 SNMP 代理的正确团体字符串、IP 地址和端口号。

2. 在“导航”面板中单击  （新建配置）按钮。

3. 配置选项以支持虚拟网络建模，如下所示：

   a. 在“建模选项”组中单击“建模选项”按钮。

      此时将打开“建模配置”对话框。

   b. 单击“协议选项”按钮。

      此时将打开“协议选项”对话框。

   c. 选择“Pingable 项的 ARP 表”选项，然后单击“确定”。

      此时将打开“建模配置”对话框。

   d. （可选）在“高级选项”组中单击“高级选项”按钮，添加非标准 SNMP 端口（如 SystemEDGE 代理端口），然后单击“确定”。

4. 输入各个 IP 地址，或在“IP 边界列表”字段中输入开始 IP 地址和结束 IP 地址，然后单击“添加”。

   注意：确保 IP 地址范围中包括 Solaris Zones Manager、互连交换机和路由器，以及需要 SNMP 模型的支持 SNMP 的 Solaris 全局区域和 Solaris 区域实例。

5. 在发现控制台中输入任何其他值，然后单击“发现”按钮。

   将创建以下模型，并将其添加到 CA Spectrum 的网络拓扑中：

   - Solaris Zones Manager 主机以及用于将其连接到网络的交换机和路由器 - 有关虚拟环境的信息来自 Solaris Zones Manager。当 CA Spectrum 中存在这些 Solaris Zones Manager 模型时，Solaris Zones 发现即可启动。
   - Solaris 全局区域和 Solaris 区域实例 - 如果您决定不使用 CA Spectrum 发现为这些实体建模，则 Solaris Zones 发现会将它们创建为 VHM 模型 (请参阅本页中的定义 255)。

   注意：也可以通过 IP 地址手动为虚拟网络建模。始终按正确顺序建模：所连接的路由器和交换机、支持 SNMP 的 Solaris 全局区域和 Solaris 区域实例，然后是 Solaris Zones Manager。按正确顺序建模可确保在拓扑中正确生成这些实体之间的关联关系。有关详细信息，请参阅《*IT 基础架构建模与管理 - 管理员指南*》。

详细信息：

如何配置管理选项 (p. 103)
将 Solaris 区域实例移至新的 Solaris Zones 主机 (p. 102)
向 VHM 模型添加 SNMP 功能 (p. 99)
配置 SNMP 建模首选项 (p. 92)

升级 CA SystemEDGE 模型

在安装 Virtual Host Manager 之前或者在代理上加载 Solaris Zones AIM 之前，可能已在 CA Spectrum 中为 CA SystemEDGE 代理建模。在这种情况下，现有的 CA SystemEDGE 模型与 Virtual Host Manager 不兼容。升级该模型，以便 Virtual Host Manager 可以访问 CA SystemEDGE 中的 Solaris Zones AIM 功能。*如果在安装 CA Spectrum 之后加载并建模带有 Solaris Zones AIM 的 CA SystemEDGE 代理，则不需要执行此过程。*

要升级 CA SystemEDGE 模型，请右键单击该模型并依次选择“重新配置”、“重新配置模型”。

CA SystemEDGE 模型将升级，以支持 Solaris Zones AIM。

注意：也可以使用 CLI 向 CA SystemEDGE 发送重新配置模型操作。有关详细信息，请参阅《*IT 基础架构建模与管理 - 管理员指南*》。

详细信息：

如何配置管理选项 (p. 103)
将 Solaris 区域实例移至新的 Solaris Zones 主机 (p. 102)
向 VHM 模型添加 SNMP 功能 (p. 99)

Solaris Zones 发现的工作方式

Solaris Zones 发现是专门用于收集有关虚拟网络实体的详细信息的发现进程。Solaris Zones 发现将获取 Solaris Zones 技术实体，为 CA Spectrum 中不存在的实体建模，并将它们放置在“导航”面板的 Virtual Host Manager 下。Solaris Zones 发现的主要优点是，它在后台自动运行，可使虚拟网络数据保持更新。通过了解 Solaris Zones 发现的工作方式，可更有力地说明正确安装和建模各个 Virtual Host Manager 组件的重要性。

Solaris Zones 发现进程的工作方式如下：

1. 在正确配置 Solaris Zones Manager（已安装启用了 Solaris Zones AIM 的 CA SystemEDGE 代理）之后，Solaris Zones Manager 使用 SSH 来联系它管理的每个 Solaris 全局区域。Solaris Zones Manager 将收集和存储此信息。

   重要说明！在 Solaris Zones Manager 主机上安装带有 Solaris Zones AIM 的 CA SystemEDGE 代理。Solaris Zones Manager 和 CA Spectrum 必须能够通信。如果它们无法通信，Solaris Zones 发现将无法运行。

2. 在 CA Spectrum 发现期间，CA Spectrum 将为步骤 1 中引用的每个 Solaris Zones Manager 创建一个模型。1.将在 CA Spectrum 和 CA SystemEDGE 代理之间启用通信。

3. CA Spectrum 轮询 Solaris Zones AIM 以收集在步骤 1 中存储的 Solaris Zones Manager 信息。

4. CA Spectrum 启动 Solaris Zones 发现。来自 AIM 的信息用于在 CA Spectrum “拓扑”选项卡和“导航”面板的 Virtual Host Manager 层次结构中更新建模，如下所示：

   a. 如果在步骤 2 之前启用 SNMP 发现，则 Virtual Host Manager 发现将为符合 SNMP 发现标准的所有支持 SNMP 的新模型创建 SNMP 模型。

      注意：默认情况下，将在 Solaris Zones 发现期间禁用 SNMP 发现。

   b. 将为其余非 SNMP Solaris Zones 主机、Solaris 全局区域和 Solaris 区域实例创建 VHM 模型 (请参阅本页中的定义 255)，如下所示：

      - 现有的 Solaris 全局区域和 Solaris 区域模型被提升为 VHM 模型。
      - 将为 CA Spectrum 中*不*存在的 Solaris 全局区域服务器和 Solaris 区域实例创建 VHM 模型。
      - 将为 Solaris Zones 主机模型创建 VHM 模型。这些模型将在“导航”面板的 Virtual Host Manager 下以及在 Universe 拓扑中对其关联的 Solaris 全局区域和 Solaris 区域模型进行分组。

   c. 虚拟网络的所有模型将添加到“导航”面板的 Virtual Host Manager 部分中。

   注意：在虚拟环境中，不同 Solaris Zones 主机上的设备可具有相同的 IP 地址或 MAC 地址。在这种情况下，CA Spectrum 将为每个 IP 地址或 MAC 地址创建重复的模型。

5. Solaris Zones 发现将自动按每个定期排定的 Solaris Zones 技术轮询时间间隔重复该过程。

   注意：默认情况下，Solaris Zones 轮询时间间隔由 Solaris Zones Manager 设备模型上的轮询时间间隔控制。或者，也可以独立于 Solaris Zones Manager 设备模型控制 Solaris Zones 轮询。使用 Solaris Zones 虚拟技术应用程序模型。

详细信息：

如何配置管理选项 (p. 103)
控制 Solaris Zones AIM 轮询 (p. 106)
将 Solaris 区域实例移至新的 Solaris Zones 主机 (p. 102)
向 VHM 模型添加 SNMP 功能 (p. 99)
跨安全域配置模型搜索 (p. 90)

向 VHM 模型添加 SNMP 功能

虽然 SNMP 可提供丰富的设备监控功能（如进程或文件监控），但是部署 SNMP 代理可能会花费较高的经济和时间成本。当 SNMP 代理不可用或禁用了 SNMP 发现时，Virtual Host Manager 会将 Solaris 全局区域和 Solaris 区域实例创建为 VHM 模型 (请参阅本页中的定义 255)。

之后，您可以在这些设备上安装 SNMP 代理，并在 CA Spectrum 中升级其建模。用于升级到 SNMP 模型的选项如下所示：

- **仅升级选定设备** - 当需要升级少量选定模型时，此方法可快速完成工作。首先将删除 VHM 模型和子模型。此方法的一个缺点是，在 CA Spectrum 删除模型之后，必须等待 Solaris Zones 发现创建新的 SNMP 模型并将其放置在 Virtual Host Manager 中。必须知道模型的 IP 地址才能进行升级。
- **升级所有支持 SNMP 的 VHM 模型** - 此方法可批量升级模型，在将 Virtual Host Manager 升级为新版本时，最好使用此方法。不必知道各个模型的 IP 地址。另一个优点是，在 CA Spectrum 删除 VHM 模型之后，会立即将升级后的 SNMP 模型放置在 Virtual Host Manager 层次结构中，而不必等待下一个轮询周期。因此，子模型不会处于非受管状态。

  此方法可能需要很长时间才能完成。所需的时间取决于在查找支持 SNMP 的设备时，Virtual Host Manager 必须搜索的团体字符串和 SNMP 端口的数量。

  注意：Virtual Host Manager 仅会尝试识别正常运行的 Solaris 区域实例上的 SNMP 代理。

重要说明！删除模型时，这些模型上的所有注释或其他自定义也将丢失。

详细信息：

如何发现和建模虚拟环境 (p. 94)
Solaris Zones 发现的工作方式 (p. 97)
删除 Virtual Host Manager 模型 (p. 108)
升级 CA SystemEDGE 模型 (p. 96)
配置 SNMP 建模首选项 (p. 92)

将选定 VHM 模型升级为 SNMP 模型

当 SNMP 代理不可用或在 Solaris Zones 发现期间禁用了 SNMP 发现时，Virtual Host Manager 会将 Solaris 全局区域和 Solaris 区域实例创建为 VHM 模型 (请参阅本页中的定义 255)。之后，您可以在这些设备上安装 SNMP 代理，并在 CA Spectrum 中升级其建模。您必须知道 IP 地址才能升级设备模型。手动选择要升级的模型可快速完成，但这些模型上的所有说明或自定义将会在升级期间丢失。

遵循这些步骤:

1. 根据需要在设备上部署或启用 SNMP 代理。
2. 使用下列方法之一重新建模设备：
   - CA Spectrum 发现
   - 按 IP 地址为设备逐个建模

   在创建支持 SNMP 的新模型时，CA Spectrum 将从 Virtual Host Manager 中删除以前的模型。在下一个 Solaris Zones AIM 轮询周期中，CA Spectrum 将支持 SNMP 的模型添加到“导航”面板的 Virtual Host Manager 中。

   重要说明！删除模型时，这些模型上的所有注释或其他自定义也将丢失。

详细信息：

管理从 Solaris 中删除的设备的设备模型 (p. 89)
如何发现和建模虚拟环境 (p. 94)
删除 Virtual Host Manager 模型 (p. 108)

将所有 VHM 模型升级为 SNMP 模型

当 SNMP 代理不可用或在 Solaris Zones 发现期间禁用了 SNMP 发现时，Virtual Host Manager 会将 Solaris 全局区域和 Solaris 区域实例创建为 VHM 模型 (请参阅本页中的定义 255)。之后，您可以在这些设备上安装 SNMP 代理，并在 CA Spectrum 中升级其建模。执行批量升级时，CA Spectrum 将搜索 VHM 模型，并查找现在表示支持 SNMP 的设备的模型。然后，CA Spectrum 将它们转换为 SNMP 模型。此方法可能需要很长的时间才能完成，具体取决于 Virtual Host Manager 必须搜索的团体字符串和端口的数量。但是，此方法可确保在升级父模型时，子模型不处于非受管状态。

遵循这些步骤:

1. 根据需要在设备上部署或启用 SNMP 代理。
2. 在“导航”面板中打开 Virtual Host Manager (p. 46)。

   将在选定 Virtual Host Manager 的“内容”面板中打开主详细信息页面。
3. 在“导航”面板中选择用于管理要升级的模型的 Solaris Zones Manager 模型。
4. 单击“信息”选项卡。
5. 展开“Solaris Zones Manager”、“CA Spectrum 建模控制”子视图。
6. 单击“升级 ICMP 专用设备”按钮。

   重要说明！删除模型时，这些模型上的所有注释或其他自定义也将丢失。

   Virtual Host Manager 将搜索由选定 Solaris Zones Manager 上的 Solaris Zones AIM 管理的设备。Virtual Host Manager 升级所有符合 SNMP 设备标准的 ICMP 专用设备，并将它们放置在 Virtual Host Manager 层次结构中。

将 Solaris 区域实例移至新的 Solaris Zones 主机

将 Solaris 区域从一个 Solaris Zones 主机移至另一个 Solaris Zones 主机可能会导致数据丢失。风险取决于 Virtual Host Manager 配置。Solaris Zones AIM 不支持区域迁移。对于 Virtual Host Manager，会将移动过程视为两个事件 - 从原始 Solaris Zones 主机中删除 Solaris 区域，然后向新 Solaris Zones 主机添加新 Solaris 区域。在这种情况下，Virtual Host Manager 将删除原始 Solaris 区域模型，并创建一个新的 Solaris 区域模型。如果您已自定义原始模型，则删除它可能会导致数据丢失。如果在移动 Solaris 区域实例之前正确配置 Virtual Host Manager 设置，则可以避免此数据丢失。

遵循这些步骤:

1. 将“允许在运行 Solaris Zones 发现期间删除设备模型”选项更改为“否” (p. 89)。

   注意：如果禁用此选项，则在从 Virtual Host Manager 管理中移除 Solaris 区域模型时，CA Spectrum 不会删除此模型。

2. 使用 Solaris Zones 虚拟化技术以从原始 Solaris Zones 主机中删除 Solaris 区域。
3. 在“导航”面板中，等待 Virtual Host Manager 反映这些更改。
4. 使用 Solaris Zones 虚拟化技术以将 Solaris 区域添加到其他 Solaris Zones 主机中。

   当 Solaris Zones 发现找到新的 Solaris 区域时，Virtual Host Manager 会将其与现有模型进行协调。Virtual Host Manager 将该模型置于 Virtual Host Manager 管理中。

5. （可选）在原始 Solaris Zones Manager 模型上将“允许在运行 Solaris Zones 发现期间删除设备模型”选项更改回“是”。

   已成功移动 Solaris 区域实例。

详细信息：

如何发现和建模虚拟环境 (p. 94)
Solaris Zones 发现的工作方式 (p. 97)
运行 CA Spectrum 发现 (p. 95)
Virtual Host Manager 中的 Solaris Zones 数据更新方式 (p. 113)
升级 CA SystemEDGE 模型 (p. 96)

如何配置管理选项

在为虚拟网络建模之后，可以配置 Virtual Host Manager 选项以查看和管理设备模型。通过配置首选项，可帮助确保 Virtual Host Manager 正确处理虚拟设备模型，并仅监控您需要的重要信息。

要配置 Virtual Host Manager 安装，请在发现并建模虚拟网络之后执行以下过程：

- 配置 Solaris Zones AIM 选项 (p. 103) - 这些选项允许您选择 CA SystemEDGE Solaris Zones AIM 的各种设置，如 AIM 轮询时间间隔和各种陷阱。
- 配置阈值和其他状态监控选项 (p. 105)- 这些选项允许您确定要监控的信息，以及 CA Spectrum 如何管理虚拟环境中发生的各种事件。

详细信息：

Virtual Host Manager 中的 Solaris Zones 数据更新方式 (p. 113)
升级 CA SystemEDGE 模型 (p. 96)

配置 Solaris Zones AIM

Solaris Zones AIM 与 Solaris Zones Manager 进行通信，以管理和收集有关虚拟环境的信息。在 Virtual Host Manager 中，可以配置 AIM 以确定它对轮询、陷阱和事件的处理方式。Solaris Zones AIM 配置设置可以帮助您正确平衡要收集的信息与所需的资源量。

遵循这些步骤:

1. 在“导航”面板中打开 Virtual Host Manager (p. 109)。

   将在选定 Virtual Host Manager 的“内容”面板中打开主详细信息页面。

2. 在“导航”面板的“资源管理器”选项卡上找到并单击 Solaris Zones Manager。

   “内容”面板上的各个选项卡中将填充有 Solaris Zones Manager 的相关详细信息。

3. 单击“信息”选项卡。

4. 展开“Solaris Zones Manager”、“Solaris Zones AIM”子视图。

5. 根据需要，单击“设置”更改以下字段的设置：

AIM 轮询时间间隔(秒)

指定 Solaris Zones AIM 在已配置的 Solaris Zones 主机中轮询和缓存状态与建模信息的时间间隔（以秒为单位）。此轮询将检索状态和建模更新，如 Solaris 区域未运行状态、Solaris Zones 主机已断开连接、新的 Solaris 区域可用、新的 Solaris Zones 主机等。

默认值： 120

限制： 大于或等于 120 的数值

注意： 为获得最佳结果，建议不要将此时间间隔设置为大于 CA Spectrum 轮询周期时间间隔。

AIM 日志级别

指定写入 Solaris Zones AIM 日志文件的信息的级别。这些级别可累积（例如，日志级别 4 将写入从级别 0 到 4 的所有消息）。日志级别如下所示：

- 0：致命
- 1：关键
- 2：警告
- 3：信息
- 4：调试
- 5：调试（低）
- 6：调试（更低）
- 7：调试（最低）

默认值： 2

注意： 建议不要将调试级别指定为大于 4。

将使用您的选择配置 Solaris Zones AIM。

详细信息：

如何配置管理选项 (p. 103)
在 Solaris Zones 模型上生成了重复的 MAC、不同的 IP 地址警报 (p. 248)

配置和监控资源状态

可以在 OneClick 中监控虚拟资源的状态。例如，可以查看总内存、已用内存、CPU 使用率百分比等。此外，还可以设置监控选项，例如，启用警报以及设置陷阱阈值。配置和查看此信息可帮助您优化虚拟网络性能以及排除警报故障。

注意：将在 Solaris Zones AIM 上设置陷阱，并由其来管理它们，但是您可以从 OneClick 子视图中配置这些阈值。在更改任何阈值或设置时，需要使用读取/写入团体字符串。

可以在“信息”选项卡上查看或配置虚拟设备的资源状态选项和信息。

遵循这些步骤:

1. 在“导航”面板中打开 Virtual Host Manager (p. 109)。

   将在选定 Virtual Host Manager 的“内容”面板中打开主详细信息页面。

2. 在“导航”面板的“资源管理器”选项卡上找到并单击虚拟设备。

   将在“内容”面板中显示设备的详细信息。

3. 单击“信息”选项卡。

   可查看多个子视图。通常，该选项卡底部的子视图中包括选定模型的资源分配和利用率信息。例如，Solaris Zones 主机模型将显示一个名为“Solaris 区域主机信息”的子视图，其中包括您在“导航”面板中选择的特定模型的详细信息。

4. 展开相应的子视图。

   将显示选定设备模型的所有可用资源状态详细信息和监控选项。

   注意：Solaris Zones Manager 模型提供由 Solaris Zones Manager 管理的所有虚拟设备的组合信息。也就是说，在“导航”面板中选择 Solaris Zones Manager 模型，可显示有关选定 Solaris Zones Manager 主机的信息，*以及*有关所有 Solaris Zones 主机、Solaris 全局区域、Solaris 区域实例、物理和虚拟 NIC、项目、主机磁盘等的组合信息。此信息与在每个单独实体模型的“信息”选项卡上显示的数据相同。Solaris Zones Manager 模型中的组合视图可以很好地概述它管理的所有虚拟实体。

详细信息：

如何配置管理选项 (p. 103)
虚拟实体类型的自定义子视图 (p. 114)
状态监控选项 (p. 116)
针对 Solaris Zones 的 Virtual Host Manager 警报 (p. 119)

控制 Solaris Zones AIM 轮询

在调整 Virtual Host Manager 性能时，可以更改 Solaris Zones Manager 轮询速率，或禁用 Solaris Zones 技术轮询。默认情况下，Solaris Zones Manager 模型上的轮询属性用于控制 Solaris Zones 相关的轮询行为。或者，也可以单独更改此 Solaris Zones 相关的轮询行为。Solaris Zones 虚拟技术应用程序模型 SolarisZoneAimApp 用于控制 Solaris Zones 相关轮询。

此应用程序上的以下两个属性值专门用于控制 Solaris Zones 技术轮询逻辑：

- PollingStatus
- Polling_Interval

Solaris Zones Manager 设备模型和 SolarisZoneAimApp 应用程序模型都包含这些属性。PollingStatus 用于禁用和启用轮询，而 Polling_Interval 用于控制轮询频率。如果这些模型的值不同，则优先考虑 SolarisZoneAimApp 应用程序模型属性值。对于 PollingStatus 和 Polling_Interval，修改 Solaris Zones Manager 设备模型上的属性时还将更改相应的应用程序模型属性（如果它们的值相同）。

通过为设备模型和应用程序模型设置值，您可以微调 Solaris Zones 的相关轮询。例如，可以将应用程序模型的轮询时间间隔设置为较大的值，而将设备模型的轮询时间间隔设置为较小的值。此方案可以通过降低对环境中非关键设备的轮询频率，来提高 Virtual Host Manager 性能。

详细信息：

Solaris Zones 发现的工作方式 (p. 97)

配置 Solaris Zones AIM 轮询时间间隔

您可以更改 Solaris Zones AIM 轮询速率。可通过设置 Solaris Zones 虚拟技术应用程序模型上的 Polling_Interval 属性来配置轮询时间间隔。

遵循这些步骤:

1. 打开 OneClick，并单击“导航”面板中的“定位器”选项卡。
2. 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。
3. 在“设备 IP 地址”字段中输入 Solaris Zones Manager 的 IP 地址，然后单击“确定”。

   将在“内容”面板中显示 Solaris Zones Manager 的应用程序模型的列表。

4. 选择 SolarisZoneAimApp 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. 单击“组件详细信息”面板中的“信息”选项卡。

6. 单击“建模信息”子视图。

7. 在“轮询时间间隔(秒)”字段中单击“设置”，然后输入新值。

   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 Solaris Zones AIM 轮询。但是，如果将“轮询时间间隔”设置为 0，并将“轮询”字段设置为“打开”，Solaris Zones AIM 轮询将按照为 Solaris Zones Manager 设备设置的轮询时间间隔继续运行。

   Solaris Zones AIM 轮询时间间隔设置即已配置。

禁用 Solaris Zones AIM 轮询

可以禁用 Solaris Zones AIM 轮询。禁用 Solaris Zones 轮询的过程与禁用 Virtual Host Manager 的过程相同。可以通过在 Solaris Zones 虚拟技术应用程序模型上设置 PollingStatus 属性来禁用轮询。

遵循这些步骤:

1. 打开 OneClick，并单击“导航”面板中的“定位器”选项卡。

2. 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。

3. 在“设备 IP 地址”字段中输入 Solaris Zones Manager 的 IP 地址，然后单击“确定”。

   将在“内容”面板中显示 Solaris Zones Manager 的应用程序模型的列表。

4. 选择 SolarisZoneAimApp 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. 单击“组件详细信息”面板中的“信息”选项卡。

6. 单击 CA Spectrum 的“建模信息”子视图。

7. 在“轮询”字段中单击“设置”，然后选择“关闭”。

   将在选定的 Solaris Zones Manager 上为 Solaris Zones AIM 禁用轮询。

删除 Virtual Host Manager 模型

通常，您可以随时从 OneClick 中删除模型。但是，Virtual Host Manager 会限制您在“导航”面板的 Virtual Host Manager 层次结构中删除模型的能力。要手动删除模型，有以下两个选项可用：

- 在 Virtual Host Manager 中删除 Solaris Zones 文件夹或 Solaris Zones Manager 模型
- 使用 Solaris Zones 虚拟化技术删除虚拟实体

在 Virtual Host Manager 中，有时会自动删除模型。下列情况会导致 CA Spectrum 自动删除 Virtual Host Manager 模型：

- **已删除 Solaris Zones 文件夹，或者已从 Virtual Host Manager 中删除 Solaris Zones Manager 模型**

  如果删除 Solaris Zones Manager 模型，或从“导航”面板中删除 Solaris Zones 文件夹，CA Spectrum 将会删除所有相关的子模型。

- **已从 Solaris Zones 虚拟环境中删除实体**

  使用 Solaris Zones 虚拟化技术删除 Solaris Zones 主机和 Solaris 区域时，CA Spectrum 还会从 Virtual Host Manager 中删除这些模型及其子模型。

- **存在已升级模型** - 在某些情况下，会首先为无 SNMP 功能的 Virtual Host Manager 建模 Solaris 全局区域或 Solaris 区域。如果以后向 VHM 模型 (请参阅本页中的定义 255)添加 SNMP 功能，则之前的模型将被删除，并替换为支持 SNMP 的新模型。

注意：虽然默认设置是删除模型，但是您可以配置 Virtual Host Manager，以便在从 Virtual Host Manager 中删除 Solaris Zones 主机、Solaris 全局区域和 Solaris 区域实例时将它们放置在 LostFound 容器中。仅当使用 Solaris Zones 虚拟环境删除设备时，才会应用此配置设置。但是，在删除 Solaris Zones 文件夹、删除 Solaris Zones Manager 模型或升级 VHM 模型时，不会应用此设置。

详细信息：

管理从 Solaris 中删除的设备的设备模型 (p. 89)
在 Solaris Zones 发现后创建了重复模型 (p. 248)
向 VHM 模型添加 SNMP 功能 (p. 99)
删除 Solaris Zones Manager 后管理启用了 SNMP 的 Solaris 区域模型 (p. 93)

查看 Solaris Zones 虚拟环境

本节介绍有关查看 Solaris Zones 虚拟环境和关联警报的概念。基本步骤与标准 CA Spectrum 步骤相同。但是，本节介绍仅适用于 Solaris Zones 虚拟技术的概念差异和详细信息。

详细信息：

运行 CA Spectrum 发现 (p. 95)
虚拟实体类型的自定义子视图 (p. 114)
用于 Solaris Zones 的定位器选项卡 (p. 115)
Virtual Host Manager 如何使用 Solaris 区域 (p. 85)
为 Solaris Zones 创建的模型 (p. 87)

了解虚拟拓扑

为 Solaris Zones 技术环境创建的模型将集成到“导航”面板中的下列位置：

- **Virtual Host Manager 节点** - Virtual Host Manager 节点提供了分层树结构，使您可查看在 Solaris Zones 技术中配置的虚拟环境资源之间的关联关系。
- **Universe 拓扑视图** - 此视图显示与 Solaris Zones 主机关联的 Solaris 全局区域和 Solaris 区域。它还将提供网络的第 2 层视图，以显示 Solaris 全局区域和 Solaris 区域实例连接到网络的方式。可以使用此视图来解决有关这些虚拟网络模型的警报。

注意：有关使用 OneClick 界面的详细信息，请参阅《*操作员指南*》。

导航面板中的 Virtual Host Manager

Virtual Host Manager 显示了在 Solaris Zones 虚拟技术中配置的虚拟环境资源之间的逻辑关联关系。使用此信息，可以查看如何在 Solaris Zones Manager 中共享资源，从而帮助您发现机会以重新组织和优化虚拟环境。通过此层次结构，还可以快速监控资源性能以及排除其警报。

由于 Virtual Host Manager 无法识别 DSS 环境 (请参阅本页中的定义 255)，因此它位于格局层次结构中。以下示例显示了 Virtual Host Manager 在“导航”面板中的位置，并演示了虚拟环境的层次结构：

```
[-] SpectroSERVER 主机
    [+] Universe
    [-] Virtual Host Manager
        [-] Solaris Zones
            [+] Solaris Zones Manager 1
            [-] Solaris Zones Manager 2
                [-] Solaris Zones 主机 1
                      Solaris 全局区域
                      Solaris 区域 1
                      Solaris 区域 2
                [+] Solaris Zones 主机 2
                [+] Solaris Zones 主机 3
```

Virtual Host Manager 是由此 SpectroSERVER 管理的整个虚拟环境的根节点。在“导航”面板中选择此节点后，将在“内容”面板中显示 Virtual Host Manager 详细信息。您可以查看与整体虚拟环境相关的事件和警报等详细信息。

虚拟环境将直接在 Virtual Host Manager 下表示用于创建这些虚拟环境的技术的文件夹中进行组织。在上面的示例层次结构中，Solaris Zones 文件夹包含使用 Solaris Zones 虚拟化技术创建的虚拟环境部分。在此文件夹中，Virtual Host Manager 列出了由此 SpectroSERVER 管理的所有 Solaris Zones Manager 主机。

每个 Solaris Zones Manager 仅包含它管理的虚拟环境部分。在“导航”面板中选择 Solaris Zones Manager 后，将在“内容”面板中显示相关详细信息，例如由选定 Solaris Zones Manager 管理的 Solaris Zones 主机或 Solaris 区域实例。您还可以查看常规统计信息，以及有关未在 CA Spectrum 中建模的其他组件的相关详细信息，例如以下信息：

- 资源池
- 项目
- 处理器集
- 物理 NIC 和虚拟 NIC
- 主机磁盘
- 容器

在每个 Solaris Zones Manager 下，层次结构表示下列实体之间的逻辑关联关系：

- **Solaris Zones 主机**

  Solaris Zones 主机包含其管理的 Solaris 全局区域和 Solaris 区域实例（即您的非全局区域 (p. 255)）。在“导航”面板中选择某个 Solaris Zones 主机后，将在“内容”面板中显示相关详细信息，例如与该 Solaris Zones 主机相关的事件和警报、内存使用率、状态等。

- **Solaris 全局区域**

  Solaris 全局区域模型显示为其相应 Solaris Zones 主机模型的子项，并且始终为 Virtual Host Manager 层次结构树中的叶节点。此模型与其父项共享相同的名称。“内容”和“组件详细信息”面板中的模型图标用于区分 Solaris 全局区域模型及其父 Solaris Zones 主机模型。DeviceType 属性也可区分这些模型。在“导航”面板中选择某个 Solaris 全局区域后，将在“内容”面板中显示相关详细信息，例如系统状态、CPU 使用率、内存使用率等。

- **Solaris 区域**

  Solaris 区域实例始终为 Virtual Host Manager 层次结构树中的叶节点。在“导航”面板中选择某个 Solaris 区域后，将在“内容”面板中显示相关详细信息，例如与该 Solaris 区域实例相关的事件和警报、内存使用率、状态等。

Universe 拓扑中的虚拟环境

为虚拟环境创建的 Solaris Zones Manager、Solaris Zones 主机、Solaris 全局区域及 Solaris 区域模型还将集成到 Universe 拓扑视图中。Solaris Zones 主机模型会自动分组其关联的 Solaris 全局区域和 Solaris 区域实例。该拓扑显示了这些 Solaris 全局区域和 Solaris 区域实例如何连接到物理网络实体。

下列示例显示了这些模型在“导航”面板中的 Universe 节点下的显示方式：

```
[-] Universe
        物理交换机 1
        物理交换机 2
    [-] Solaris Zones 主机
            扇出 A
            扇出 B
            Solaris 全局区域
            Solaris 区域 A
            Solaris 区域 B
            Solaris 区域 C
```

详细信息：

虚拟实体类型的自定义子视图 (p. 114)
Virtual Host Manager 中的 Solaris Zones 数据更新方式 (p. 113)
为 Solaris Zones 创建的模型 (p. 87)

虚拟设备的图标

Virtual Host Manager 提供了专用于区分虚拟环境中设备的图标。为了区分物理实体和虚拟实体，虚拟设备图标的外部边缘会显示光晕效果。例如，虚拟设备模型图标的边缘显示有光晕，如下所示：

对于承载虚拟设备的物理服务器，Virtual Host Manager 在设备图标上使用独特的蜂窝形图案，如下所示：

注意：对于 Solaris Zones 技术，仅会在 Virtual Host Manager 中为 Solaris 区域实例创建虚拟实体模型。为虚拟环境建模的所有其他实体（如 Solaris Zones 主机、Solaris 全局区域和 Solaris Zones Manager）都是物理设备。

Virtual Host Manager 中的 Solaris Zones 数据更新方式

在初始 Solaris Zones 发现期间，CA Spectrum 将使用您的虚拟设备模型填充“导航”面板中的 Virtual Host Manager 层次结构。在 CA Spectrum 构建此初始层次结构后，您的虚拟网络配置可能会发生更改，Virtual Host Manager 必须持续工作以保持此信息在 CA Spectrum 中的准确性。例如，以下事件可能会更改虚拟网络配置：

- 在 Solaris Zones 主机上创建或删除 Solaris 区域
- 手动将 Solaris 区域从一个 Solaris Zones 主机移至另一个 Solaris Zones 主机

为了保持信息准确，Virtual Host Manager 通过轮询 Solaris Zones AIM 来检测这些更改。因此，将于每个轮询周期在 CA Spectrum 中更新您的虚拟网络配置。CA Spectrum 还会从 AIM 接收陷阱，并生成相应的事件。通过查看事件日志，可以查明配置发生更改的时间（例如创建新 Solaris 区域的时间）。

在删除 Solaris 区域时，CA Spectrum 将从“导航”面板的 Virtual Host Manager 层次结构中删除模型。当 AIM 检测到向您的虚拟网络配置中添加了内容时（如配置新 Solaris 区域或将某个 Solaris 区域置于管理中时），CA Spectrum 将执行以下任务：

- 在“导航”面板的 Virtual Host Manager 层次结构中，更新虚拟设备模型的放置
- *自动*重新发现与受影响的 Solaris 全局区域和 Solaris 区域模型的连接，并将它们与 Universe 拓扑中的正确 Solaris Zones 主机关联。

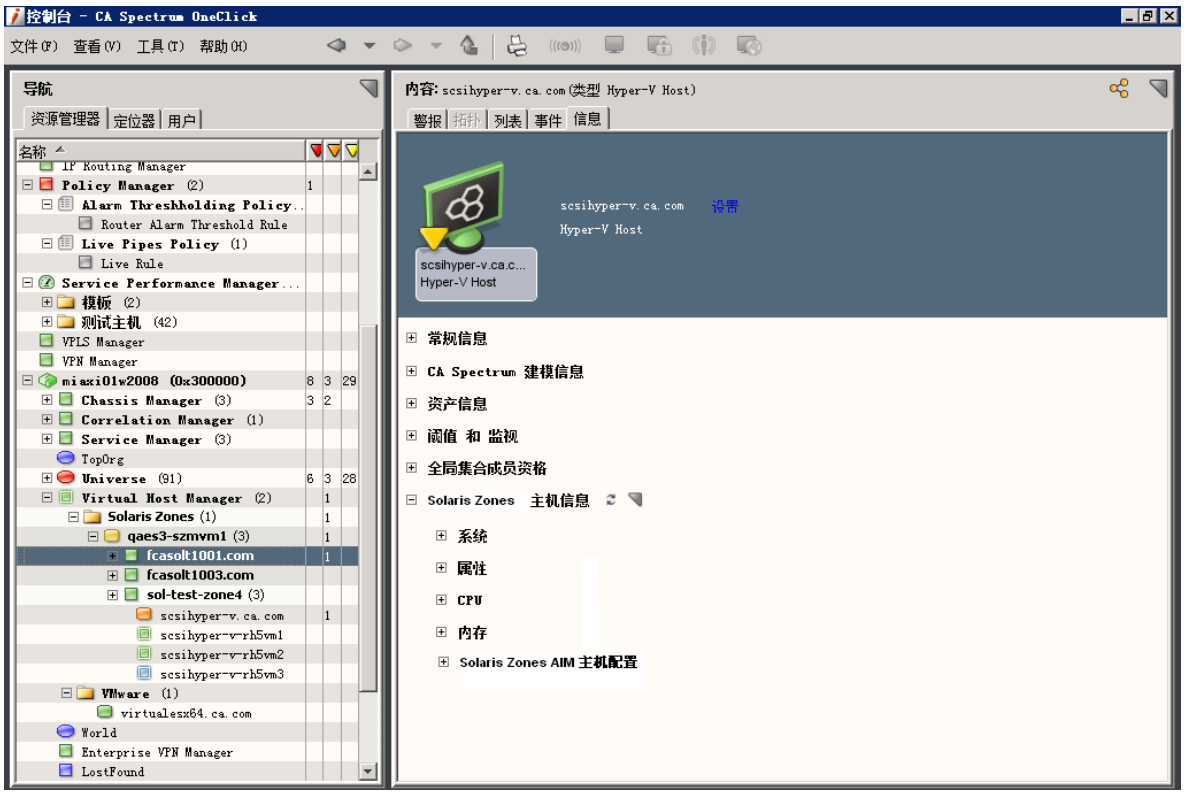
  重要说明！要正确重建与虚拟模型的连接，必须为物理网络中的所有互连路由器和交换机建模。如果在重新发现与虚拟设备的连接之前这些模型不存在，则 CA Spectrum 无法在 Universe 拓扑视图中解析这些连接并正确显示相关信息。Solaris Zones 主机将与 CA SystemEDGE 模型放置在同一个 LAN 容器中。

详细信息：

Virtual Host Manager 的工作原理 (p. 11)
管理从 Solaris 中删除的设备的设备模型 (p. 89)
配置和监控资源状态 (p. 105)
将 Solaris 区域实例移至新的 Solaris Zones 主机 (p. 102)
为 Solaris Zones 创建的模型 (p. 87)
查看 Solaris Zones 虚拟环境 (p. 109)

虚拟实体类型的自定义子视图

您的各个 Virtual Host Manager 模型将共同提供有关虚拟环境的信息。每个模型将单独提供特定的信息或配置设置，具体取决于其表示的虚拟实体类型。此自定义子视图显示在“内容”面板的“信息”选项卡上。这些子视图可包含实时数据（如 CPU 状态或内存利用率），并提供了对阈值设置的访问。例如，针对 Solaris Zones 主机的自定义子视图是“Solaris 区域主机信息”子视图，如下所示：



注意：Solaris Zones Manager 模型提供由 Solaris Zones Manager 管理的所有虚拟设备的组合信息。也就是说，在“导航”面板中选择 Solaris Zones Manager 模型，可显示有关选定 Solaris Zones Manager 主机的信息，*以及*有关所有 Solaris Zones 主机、Solaris 全局区域、Solaris 区域实例、物理和虚拟 NIC、项目、主机磁盘等的组合信息。此信息与在每个单独实体模型的“信息”选项卡上显示的数据相同。Solaris Zones Manager 模型中的组合视图可以很好地概述它管理的所有虚拟实体。

详细信息：

配置和监控资源状态 (p. 105)
了解虚拟拓扑 (p. 109)

用于 Solaris Zones 的定位器选项卡

除了在“资源管理器”选项卡上查看有关虚拟环境的详细信息外，还可以使用“定位器”选项卡运行预配置的 Virtual Host Manager 搜索。搜索选项在“定位器”选项卡中的“Virtual Host Manager”->“Solaris Zones”文件夹下进行分组，如下所示：

这些详细搜索可以帮助您调查仅与虚拟实体（如单个格局中的所有 Solaris Zones 主机）相关的信息。

注意：虽然 Virtual Host Manager 无法识别 DSS (请参阅本页中的定义 255)，但是这些预配置搜索允许您在搜索参数中选择多个要搜索的格局。

“导航”面板的“定位器”选项卡中包含针对 Solaris Zones 的以下搜索：

所有 Solaris 全局区域

在 CA Spectrum 数据库中查找已为虚拟网络建模的所有 Solaris 全局区域。

所有 Solaris 区域

在 CA Spectrum 数据库中查找已为虚拟网络建模的所有 Solaris 区域实例。

所有 Solaris Zones 主机

在 CA Spectrum 数据库中查找已为虚拟网络建模的所有 Solaris Zones 主机。

区域 - 按 Solaris Zones 主机名

在 CA Spectrum 数据库中查找已为虚拟网络建模的所有 Solaris 区域实例（包括 Solaris Zones 主机），仅限于由选定 Solaris Zones 主机管理的 Solaris 区域。

状态监控选项

CA Spectrum 提供了多种用于监控虚拟网络资源状态的选项。为资源提供的状态信息将有所不同，具体取决于您监控的虚拟实体的类型。此外，您是否能够配置状态选项取决于其类型。例如，一些状态选项是只读选项，而另外一些状态选项则允许您配置阈值、启用行为或选择警报重要级别。通过提供此系列选项和自定义级别，CA Spectrum 允许您决定如何以最佳方式监控虚拟网络的性能。

状态字段位于 OneClick 子视图中。Solaris Zones Manager 模型上以表格格式提供了给定虚拟环境的所有状态信息。此外，在 CA Spectrum 中具有唯一模型的每个虚拟实体类型将提供相同状态信息的子集，以便于查看。可以从任一视图位置设置与状态相关的设置，包括报警类型、监控器和阈值。

下表概述了为每个虚拟实体类型提供的状态信息的类型。“子视图位置”列介绍了相应状态字段在 OneClick 中的位置。例如，在“信息”选项卡上的以下两个位置中提供了 Solaris 区域模型的“内存”信息：

- Solaris 区域模型的“Solaris 区域信息”子视图
- Solaris Zones Manager 模型的“Solaris Zones Manager”->“管理的环境”->“区域”子视图

要浏览可用于每个状态信息类型的确切状态选项，请在 OneClick 中查找子视图。

Solaris Zones Manager

状态信息类型	子视图位置
总体状态	Solaris Zones Manager

Solaris Zones 主机

状态信息类型	子视图位置
总体状态	Solaris Zones 主机、Solaris Zones Manager
CPU	Solaris Zones 主机、Solaris Zones Manager
内存	Solaris Zones 主机、Solaris Zones Manager

Solaris 全局区域

状态信息类型	子视图位置
系统	Solaris 全局区域、Solaris Zones Manager
CPU	Solaris 全局区域、Solaris Zones Manager
内存	Solaris 全局区域、Solaris Zones Manager

Solaris 区域

状态信息类型	子视图位置
总体状态	Solaris 区域、Solaris Zones Manager
内存	Solaris 区域、Solaris Zones Manager
CPU	Solaris 区域、Solaris Zones Manager
聚合 CPU	Solaris 区域、Solaris Zones Manager

资源池

状态信息类型	子视图位置
总体状态	Solaris Zones Manager

项目

状态信息类型	子视图位置
总体状态	Solaris Zones Manager
内存	Solaris Zones Manager
CPU	Solaris Zones Manager

处理器集

状态信息类型	子视图位置
总体状态	Solaris Zones Manager

物理 NIC

状态信息类型	子视图位置
总体状态	Solaris Zones Manager
Connection	Solaris Zones Manager
链路状态	Solaris Zones Manager

虚拟 NIC

状态信息类型	子视图位置
总体状态	Solaris Zones Manager
Connection	Solaris Zones Manager
使用率	Solaris Zones Manager

主机磁盘

状态信息类型	子视图位置
总体状态	Solaris Zones Manager
容量	Solaris Zones Manager
用法	Solaris Zones Manager
可用空间	Solaris Zones Manager
读状态	Solaris Zones Manager
写状态	Solaris Zones Manager

详细信息：

配置和监控资源状态 (p. 105)
针对 Solaris Zones 的 Virtual Host Manager 警报 (p. 119)
Virtual Host Manager 中支持的陷阱 (p. 121)

Solaris Zones 的警报和故障隔离

本节介绍 Virtual Host Manager 所使用的陷阱以及生成的警报。本节还说明 Virtual Host Manager 故障隔离与基础 CA Spectrum 故障隔离有何差异。

针对 Solaris Zones 的 Virtual Host Manager 警报

为了就虚拟网络中出现的问题向您报警，CA Spectrum 将生成警报。将以两种方式创建警报：

- 从 CA SystemEDGE 代理发送的陷阱
- 轮询

通过轮询可生成四个警报：“Solaris Zones 代理已丢失”、“Solaris Zones 主机代理已丢失”、“Solaris Zones Manager 不可用”和“Solaris 区域未运行”。但是，有几个陷阱可以在虚拟设备上生成警报。CA Spectrum 支持 Solaris Zones AIM 从 CA SystemEDGE 代理发送的所有陷阱。为了优化这些陷阱，可以单独为每个虚拟设备配置阈值。

如果某个陷阱违反阈值并生成警报，CA Spectrum 将使用通过陷阱传递的“状态”varbind 的值来确定警报重要级别。所有状态 varbind 具有以下可能的值（将接收相同的 CA Spectrum 警报）：

- 1：正常
- 2：警告
- 3：关键

CA Spectrum 将这些 Solaris Zones 技术状态映射到 CA Spectrum 警报重要级别，如下所示：

Solaris Zones 状态	CA Spectrum 警报重要级别
1：正常	清除
2：警告	次要（黄色）
3：关键	主要（橙色）

详细信息：

管理从 Solaris 中删除的设备的设备模型 (p. 89)
配置和监控资源状态 (p. 105)
状态监控选项 (p. 116)
删除 Solaris Zones Manager 后管理启用了 SNMP 的 Solaris 区域模型 (p. 93)

CA Spectrum 如何从 CA SystemEDGE 转发陷阱

CA Spectrum 支持由 Solaris Zones AIM 发送的所有陷阱。最初会将这些陷阱发送给 Solaris Zones CA SystemEDGE 模型。如果陷阱的目标不是 Solaris Zones 模型，则 CA Spectrum 会将陷阱转发给正确的虚拟模型。

注意：对于与陷阱相关的特定事件代码，请使用事件配置应用程序并针对“0x056e”进行筛选。或者，可以启动 MIB 工具以便在“EMPIRE-CASUNZA-MIB”MIB 的“陷阱支持”表中查看陷阱。有关使用事件配置应用程序的详细信息，请参阅《*事件配置用户指南*》。有关使用 MIB 工具的详细信息，请参阅《*IT 基础架构建模与管理 - 管理员指南*》。

CA Spectrum 使用以下过程确定要将陷阱转发到的位置：

1. CA Spectrum 在接收到陷阱时会使用陷阱中的 varbind 信息来查找正确的虚拟实体。
   - 对于转发到 Solaris Zones 主机的陷阱，CA Spectrum 将使用 UID 来查找正确的主机。
   - 对于转发到 Solaris 区域的陷阱，CA Spectrum 将使用 UID 来确定第一个正确的 Solaris Zones 主机。然后，CA Spectrum 在此 Solaris Zones 主机管理的区域的列表中查找正确的 Solaris 区域。
2. CA Spectrum 使用此 UID 来查找并定位与给定 UID 相关的 CA Spectrum 模型。将预先确定与所有陷阱关联的实体类型。CA Spectrum 将根据查找结果按如下所示转发陷阱：
   - 如果它使用给定 UID 找到特定类型的 CA Spectrum 模型，CA Spectrum 会将事件和相应警报转发给目标模型。
   - 如果对于给定 UID 它找不到 CA Spectrum 模型，CA Spectrum 将在 Solaris Zones Manager 模型上生成新的常规事件。此新事件包括有关陷阱的详细信息。

     注意：如果在 Solaris Zones 中更改虚拟网络实体之后立即发送陷阱，CA Spectrum 通常会找不到相关模型。Solaris Zones 发现尚未在 CA Spectrum 中标识和创建相应的模型。

详细信息：

Virtual Host Manager 中支持的陷阱 (p. 121)

Virtual Host Manager 中支持的陷阱

CA Spectrum 中支持由 Solaris Zones AIM 生成的所有陷阱。这些陷阱最初会发送给 Solaris Zones Manager 模型。然后，根据陷阱类型，陷阱会被转发到相应的虚拟实体类型（即“目标”实体）。通过使用这些陷阱，您可以监控虚拟网络的性能，解决生成的所有警报或触发事件。

注意：有关 Solaris Zones AIM 生成的陷阱的详细信息，请参阅《*CA Virtual Assurance for Infrastructure Managers 实施指南*》。

下表列出了特定目标实体类型的陷阱，并指定陷阱是否生成警报。

Solaris Zones Manager 陷阱

陷阱名称	陷阱 OID	生成警报？
zoneAimHostDeleteTrap	1.3.6.1.4.1.546.1.1.0.165448	否
zoneAimHostAddTrap	1.3.6.1.4.1.546.1.1.0.165449	否

Solaris Zones 主机陷阱

陷阱名称	陷阱 OID	生成警报？
zoneAimHostConfigChangeTrap	1.3.6.1.4.1.546.1.1.0.165401	否
zoneAimHostStateChangeTrap	1.3.6.1.4.1.546.1.1.0.165402	是
zoneAimHostCPUStateChangeTrap	1.3.6.1.4.1.546.1.1.0.165403	是
zoneAimHostMemStateChangeTrap	1.3.6.1.4.1.546.1.1.0.165404	是
zoneAimHostTotalZoneCPUStateChangeTrap	1.3.6.1.4.1.546.1.1.0.165405	是
zoneAimHostTotalZoneMemStateChangeTrap	1.3.6.1.4.1.546.1.1.0.165406	是
zoneAimHostThresholdChangeTrap	1.3.6.1.4.1.546.1.1.0.165407	否
zoneAimHostConnectionStateChangeTrap	1.3.6.1.4.1.546.1.1.0.165408	否
zoneAimContainerAddedTrap	1.3.6.1.4.1.546.1.1.0.165416	否
zoneAimContainerRemovalTrap	1.3.6.1.4.1.546.1.1.0.165417	否
zoneAimPNICAddedTrap	1.3.6.1.4.1.546.1.1.0.165425	否
zoneAimPNICRemovalTrap	1.3.6.1.4.1.546.1.1.0.165426	否
zoneAimPNICConfigChangeTrap	1.3.6.1.4.1.546.1.1.0.165427	否
zoneAimPNICStateChangeTrap	1.3.6.1.4.1.546.1.1.0.165428	是

陷阱名称	陷阱 OID	生成警报？
zoneAimHostDiskAddedTrap	1.3.6.1.4.1.546.1.1.0.165433	否
zoneAimHostDiskRemovalTrap	1.3.6.1.4.1.546.1.1.0.165434	否
zoneAimHostDiskConfigChangeTrap	1.3.6.1.4.1.546.1.1.0.165435	否
zoneAimHostDiskStateChangeTrap	1.3.6.1.4.1.546.1.1.0.165436	是
zoneAimHostDiskAvailStateChangeTrap	1.3.6.1.4.1.546.1.1.0.165437	是
zoneAimHostDiskThresholdChangeTrap	1.3.6.1.4.1.546.1.1.0.165438	否
zoneAimResourcePoolAddedTrap	1.3.6.1.4.1.546.1.1.0.165439	否
zoneAimResourcePoolRemovalTrap	1.3.6.1.4.1.546.1.1.0.165440	否
zoneAimResourcePoolConfigChangeTrap	1.3.6.1.4.1.546.1.1.0.165441	否
zoneAimResourcePoolStateChangeTrap	1.3.6.1.4.1.546.1.1.0.165442	是
zoneAimResourcePoolSchedChangeTrap	1.3.6.1.4.1.546.1.1.0.165443	否
zoneAimProcessorSetAddedTrap	1.3.6.1.4.1.546.1.1.0.165444	否
zoneAimProcessorSetRemovalTrap	1.3.6.1.4.1.546.1.1.0.165445	否
zoneAimProcessorSetConfigChangeTrap	1.3.6.1.4.1.546.1.1.0.165446	否
zoneAimProcessorSetStateChangeTrap	1.3.6.1.4.1.546.1.1.0.165447	是

Solaris 全局区域和 Solaris 区域陷阱

陷阱名称	陷阱 OID	生成警报？
zoneAimZoneCPUStateChangeTrap	1.3.6.1.4.1.546.1.1.0.165409	是
zoneAimZoneMemStateChangeTrap	1.3.6.1.4.1.546.1.1.0.165410	是
zoneAimZoneConfigChangeTrap	1.3.6.1.4.1.546.1.1.0.165411	否
zoneAimZoneThresholdChangeTrap	1.3.6.1.4.1.546.1.1.0.165412	否
zoneAimZoneAddedTrap	1.3.6.1.4.1.546.1.1.0.165413	否
zoneAimZoneRemovedTrap	1.3.6.1.4.1.546.1.1.0.165414	否
zoneAimZoneRunningStateChangeTrap	1.3.6.1.4.1.546.1.1.0.165415	是
zoneAimProjectCPUStateChangeTrap	1.3.6.1.4.1.546.1.1.0.165418	是
zoneAimProjectMemStateChangeTrap	1.3.6.1.4.1.546.1.1.0.165419	是
zoneAimProjectAddedTrap	1.3.6.1.4.1.546.1.1.0.165420	否
zoneAimProjectRemovalTrap	1.3.6.1.4.1.546.1.1.0.165421	否
zoneAimProjectConfigChangeTrap	1.3.6.1.4.1.546.1.1.0.165422	否

陷阱名称	陷阱 OID	生成警报？
zoneAimProjectThresholdChangeTrap	1.3.6.1.4.1.546.1.1.0.165423	否
zoneAimProjectOverallStateChangeTrap	1.3.6.1.4.1.546.1.1.0.165424	是
zoneAimVNICAddedTrap	1.3.6.1.4.1.546.1.1.0.165429	否
zoneAimVNICRemovalTrap	1.3.6.1.4.1.546.1.1.0.165430	否
zoneAimVNICConfigChangeTrap	1.3.6.1.4.1.546.1.1.0.165431	否
zoneAimVNICStateChangeTrap	1.3.6.1.4.1.546.1.1.0.165432	是

详细信息：

配置和监控资源状态 (p. 105)
如何配置管理选项 (p. 103)
Virtual Host Manager 中的 Solaris Zones 数据更新方式 (p. 113)
状态监控选项 (p. 116)
CA Spectrum 如何从 CA SystemEDGE 转发陷阱 (p. 120)

用于虚拟网络的故障管理

故障隔离旨在缩小导致网络问题的根本原因的范围。通过查找根本原因，可以帮助您排除故障并快速更正问题，或使用自动化脚本以编程方式更正问题。确定哪些设备是导致警报的根本原因可能非常困难，因为单个设备中的问题会导致网络中的多个设备生成事件。

例如，与 Solaris Zones 主机失去联系通常意味着也会与其管理的 Solaris 区域实例失去联系。因此，Solaris Zones 主机设备模型和所有受影响的 Solaris 区域实例将生成警报。通过使用故障隔离技术，Virtual Host Manager 将关联这些警报以尝试确定单个根本原因。

虚拟网络可提供独特的管理机会，因为它们针对 CA Spectrum 提供了备用管理视角。也就是说，CA Spectrum 可通过直接与您的虚拟设备联系或通过虚拟网络管理技术 Solaris Zones 来收集信息。这种备用管理视角可通过两种方式来增强标准 CA Spectrum 故障管理：

- **增强失去联系警报** - 两个设备信息源可帮助 Virtual Host Manager 查明原因，并更轻松地将事件与单个根本原因关联。
- **代理故障警报** - *代理管理*是指使用备用管理源（代替主要管理器或与主要管理器一起）来管理网络设备的行为。例如，CA Spectrum 可通过直接与虚拟网络设备联系或使用虚拟技术应用程序与设备联系来管理这些虚拟网络设备。当 Solaris Zones 虚拟化技术与虚拟网络设备失去联系时，Virtual Host Manager 将为每个设备生成一个“失去代理管理”警报。这些警报具有唯一性，因为它们提醒您通过*代理*对设备执行的*管理*（而不是设备或直接 (SNMP) 管理的状态）受到影响。

丢失设备联系时故障隔离的工作方式

为了帮助您排除设备中的网络问题，CA Spectrum 使用故障隔离来缩小警报根本原因的范围。对于虚拟网络，Virtual Host Manager 将使用通过与设备直接联系获取的信息，以及由 Solaris Zones 技术通过 Solaris Zones AIM 提供的信息。在许多情况下，标准 CA Spectrum 故障管理可以查明根本原因。但是在一些特殊情况下，无法使用标准方法来隔离虚拟网络中的问题。

Virtual Host Manager 用于发现根本原因的故障隔离类型取决于生成警报的设备，以及设备生成的事件类型。下列方案介绍了两种独特的故障管理情况，以及 CA Spectrum 如何确定虚拟网络中的网络错误。

方案 1：Solaris 区域实例未运行

在虚拟环境中，与 CA Spectrum 通过标准设备监控发现的信息相比，虚拟管理应用程序可以提供更多的详细信息。例如，Solaris Zones 虚拟化技术可发现 Solaris 区域何时从“正在运行”状态更改为其他状态（如“已安装”）。

如果 Solaris 区域不再运行，并且 CA Spectrum 与其失去联系，但是 Solaris Zones Manager 的代理管理 (请参阅本页中的定义 255)未中断，则 CA Spectrum 将按如下所示确定根本原因：

1. 当 CA Spectrum 与 Solaris 区域失去联系时，将生成“失去联系”警报。
2. 在其下一个轮询周期内，Solaris Zones Manager 模型将轮询 Solaris Zones AIM 以收集有关 Solaris 区域的信息。由于 Solaris Zones 技术管理 Solaris 区域实例，因此它可提供导致 Solaris 区域所生成警报的可能原因的相关信息。

3. 如果 Solaris Zones 技术发现 Solaris 区域处于未运行模式中，它将生成“区域未运行”警报。

   注意：在 Solaris 区域重新运行后的第一个 Solaris Zones AIM 轮询周期内，将清除此警报。

4. Virtual Host Manager 将“失去联系”警报与 CA Spectrum 所创建的相应“区域未运行”警报关联。Virtual Host Manager 使“失去联系”警报显示为“区域未运行”警报的症状。

方案 2：Solaris Zones 主机关闭

如果 CA Spectrum 与已建模的 Solaris 全局区域以及该主机上运行的所有 Solaris 区域失去联系，它将检查上游路由器和交换机的状态。根据它们的状态，CA Spectrum 将按如下所示确定根本原因：

- 一个或多个 Solaris 区域实例或 Solaris 全局区域的所有上游设备都不可用 - 标准 CA Spectrum 故障隔离技术可确定根本原因，如下所示：
  - “设备已停止响应轮询”警报 - 当任何 Solaris 区域或 Solaris 全局区域的至少一个上游连接设备启动时在 Solaris Zones 主机上生成。
  - “网关不可访问”警报 - 当*所有*上游连接设备都关闭时在 Solaris Zones 主机上生成。
- 至少一个上游设备可用于连接到 Solaris Zones 主机的每个 Solaris 区域实例和 Solaris 全局区域模型 - CA Spectrum 推断 Solaris Zones 主机是根本原因，并按如下所示进行响应：

  a. 直接连接到 Solaris 全局区域模型或 Solaris 区域模型的 Solaris 全局区域模型和所有 Solaris 区域、端口和扇出将生成标准故障隔离警报。

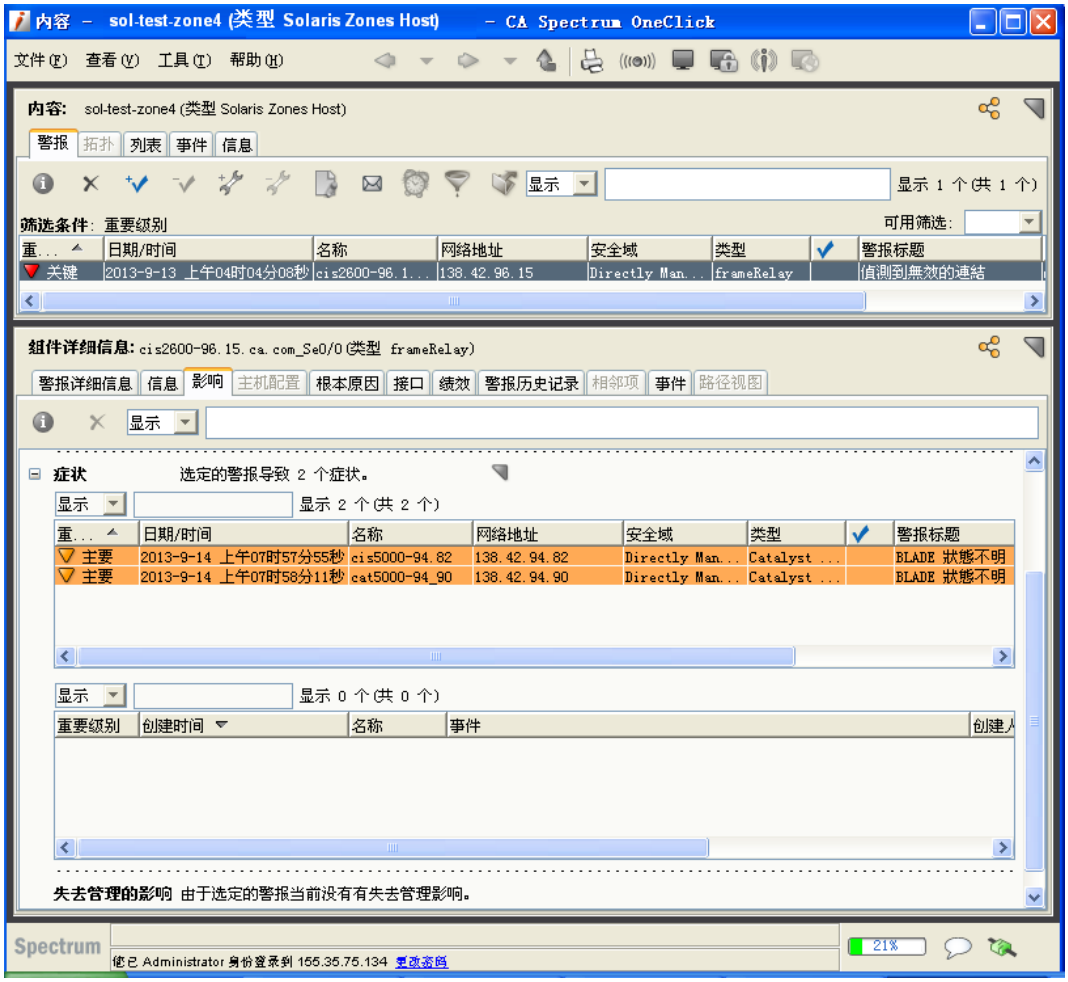
  b. Virtual Host Manager 为 Solaris Zones 主机模型创建“物理主机关闭”警报。

  c. 为受影响设备（如 Solaris 区域、端口和扇出）创建的所有故障隔离相关警报将关联到“物理主机关闭”警报，从而使它们成为“物理主机关闭”警报的症状。这些症状警报显示在“物理主机关闭”警报的“影响”选项卡上的“症状”表中。

     注意：对于每个 Solaris Zones 主机模型，Virtual Host Manager 将创建一个“虚拟故障域”。此域中包括 Solaris Zones 主机、Solaris 全局区域和 Solaris 区域实例，以及直接连接到 Solaris 全局区域模型或 Solaris 区域的所有端口和扇出。当 Solaris Zones 主机生成“物理主机关闭”警报时，域中的所有标准故障隔离警报将与其关联。将这些警报作为症状关联可表明 Solaris 区域主机上的“物理主机关闭”警报是根本原因。

d. “影响”选项卡上针对“物理主机关闭”警报的“失去管理的影响”表中列出了所有受影响设备。

注意：被抑制的设备在“症状”表中没有对应的警报，因此下列示例虽然仅显示了两个相关症状警报，但涉及四个受影响的设备：



e. 如果一个或多个 Solaris 区域实例或 Solaris 全局区域的所有上游设备都已关闭，则 CA Spectrum 无法再可靠地指出故障出自 Solaris Zones 主机。因此，CA Spectrum 将清除“物理主机关闭”警报，并应用标准 CA Spectrum 故障隔离技术。

详细信息：

确定受 Solaris Zones 主机停机影响的 Solaris 区域 (p. 129)
丢失代理管理时故障隔离的工作方式 (p. 127)

丢失代理管理时故障隔离的工作方式

用于创建虚拟网络的 Solaris Zones 虚拟化技术为 CA Spectrum 提供了独特的管理机会。CA Spectrum 可以使用标准方法来直接联系您的虚拟设备，此外，CA Spectrum 可以同时从 Solaris Zones 技术收集虚拟设备信息。从这个意义上讲，Solaris Zones 技术是 CA Spectrum 可从其收集虚拟设备信息的“代理”。如果 CA Spectrum 与设备失去直接联系，则将生成警报。同样，如果 Solaris Zones 技术与虚拟设备失去联系，或者如果 Virtual Host Manager 与 Solaris Zones Manager 失去联系，Virtual Host Manager 将生成警报 -“失去代理管理”警报 (请参阅本页中的定义 255)。

作为响应，CA Spectrum 将尝试隔离导致代理管理故障的原因。代理故障隔离类似于标准 CA Spectrum 故障隔离，不过，这些警报将提醒您虚拟设备的*代理*管理会受到影响。代理管理故障隔离无法指明虚拟设备是已启动还是已关闭。但是，了解何时失去通过代理进行的联系非常重要，因为您可能会丢失设备的重要虚拟信息。

Virtual Host Manager 用于发现根本原因的代理故障隔离类型取决于生成警报的设备，以及设备生成的事件类型。下列方案介绍了两种独特的代理故障管理情况，以及 Virtual Host Manager 如何确定虚拟网络中的网络错误。

方案 1：Solaris Zones Manager 与 Solaris Zones 主机之间失去联系

如果 Solaris Zones Manager 与其管理的一个 Solaris Zones 主机失去联系，则有关该 Solaris Zones 主机和承载的所有 Solaris 区域实例的 Solaris Zones Manager 数据将丢失。为了隔离该问题，Virtual Host Manager 将按如下所示确定根本原因：

1. 将在 Solaris Zones 主机、Solaris 全局区域和承载的所有 Solaris 区域上生成“代理已丢失”警报。
2. Solaris 区域警报将与 Solaris 全局区域的“代理已丢失”警报关联，使这些 Solaris 区域警报成为 Solaris 全局区域警报的症状。Solaris 全局区域警报将与 Solaris Zones 主机的“代理已丢失”警报关联，使其成为 Solaris Zones 主机警报的症状。将这些警报作为症状关联可表明 Solaris Zones 主机警报是根本原因。
3. 如果 CA Spectrum 也与 Solaris Zones 主机失去联系并生成“物理主机关闭”警报，则为 Solaris Zones 主机生成的“代理已丢失”警报将与“物理主机关闭”警报关联。在这种情况下，“代理已丢失”警报成为“物理主机关闭”警报的症状。将此警报作为症状关联可表明 Solaris Zones 主机上的“物理主机关闭”警报是根本原因。

方案 2：CA Spectrum 与 Solaris Zones Manager 之间失去联系

如果 CA Spectrum 与 Solaris Zones Manager 模型失去联系或停止轮询该模型，则将丢失该 Solaris Zones Manager 管理的所有虚拟模型的 Solaris Zones 技术数据。为了隔离该问题，Virtual Host Manager 将按如下所示确定根本原因：

1. CA Spectrum 将为该 Solaris Zones Manager 管理的所有虚拟模型（包括 Solaris 区域实例、Solaris 全局区域和 Solaris Zones 主机）生成“代理已丢失”警报。CA Spectrum 还将在 Solaris Zones Manager 模型上生成单独的“代理不可用”警报。
2. Solaris 区域警报将与其相应的 Solaris 全局区域模型警报关联。
3. Solaris 全局区域警报将与其相应的 Solaris Zones 主机模型警报关联。
4. Solaris Zones 主机模型警报将与 Solaris Zones Manager 模型的“代理不可用”警报关联。
5. 然后，此“代理不可用”警报将与正关闭的 Solaris Zones Manager 的根本原因关联。根本原因通常是由标准 CA Spectrum 故障管理生成的警报，例如为下列情况创建的警报：
   - 失去 Solaris Zones Manager 的管理（即，Solaris Zones Manager 主机上的 CA SystemEDGE 代理发生问题）
   - 失去计算机联系
   - Solaris Zones Manager 模型处于维护模式中

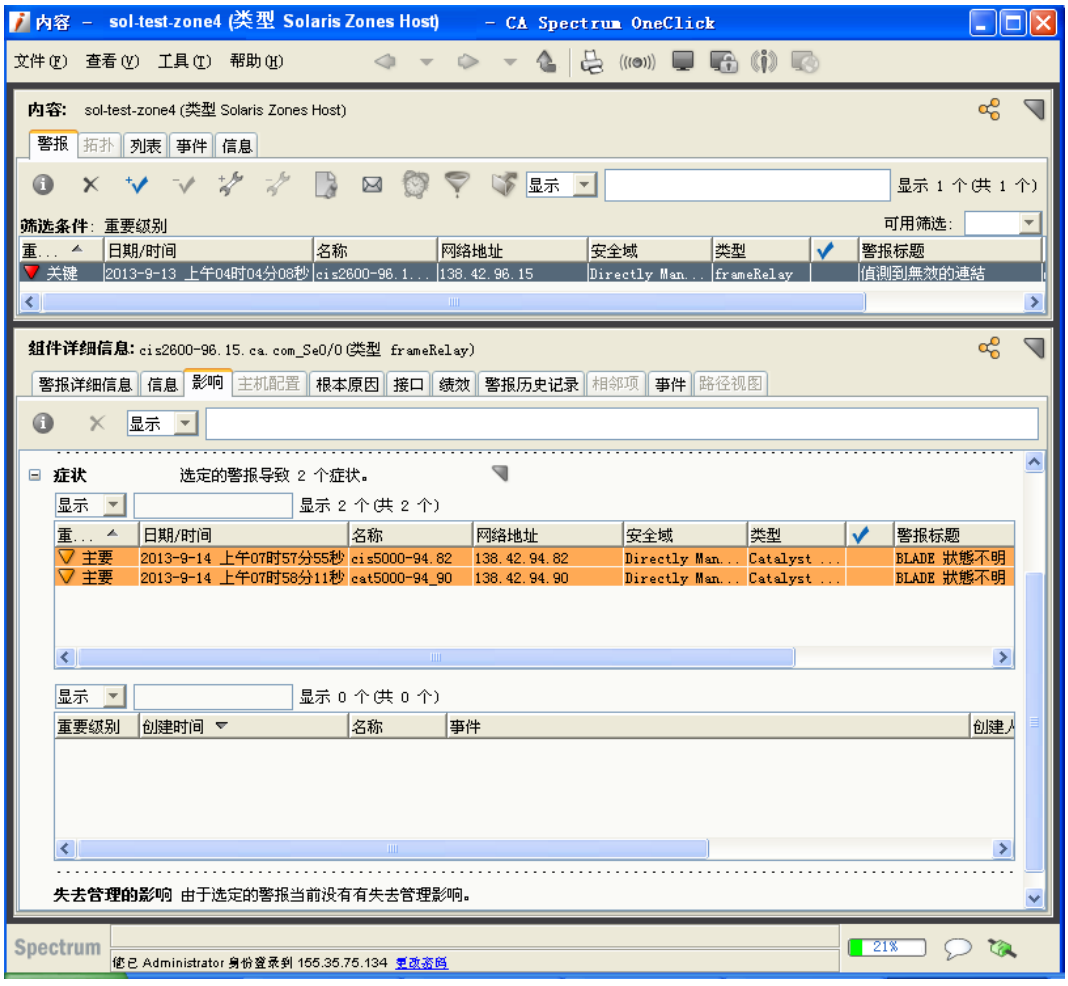
详细信息：

丢失设备联系时故障隔离的工作方式 (p. 124)

确定受 Solaris Zones 主机停机影响的 Solaris 区域

当与 Solaris Zones 主机的联系中断或者 Solaris Zones 主机关闭时，该 Solaris Zones 主机承载的所有 Solaris 区域实例都将受到影响。由于 Solaris Zones 技术无法与 Solaris Zones 主机进行通信以获取使用情况信息，因此您可能不会接收到该 Solaris Zones 主机上承载的关键 Solaris 区域的警报。要确定关键 Solaris 区域是否受到影响，可以在警报的“影响”选项卡上查看受影响 Solaris 区域实例的列表，如下所示：

- “症状”子视图 - 显示受影响的 Solaris 区域实例生成的所有症状警报
- “失去管理的影响”视图 - 列出受警报影响的 Solaris 区域实例



详细信息：

丢失设备联系时故障隔离的工作方式 (p. 124)

第 5 章： Microsoft Hyper-V

本节适用于 Microsoft Hyper-V 虚拟化技术用户，将介绍如何使用 Virtual Host Manager 来管理通过 Hyper-V 创建的虚拟实体。

此部分包含以下主题：

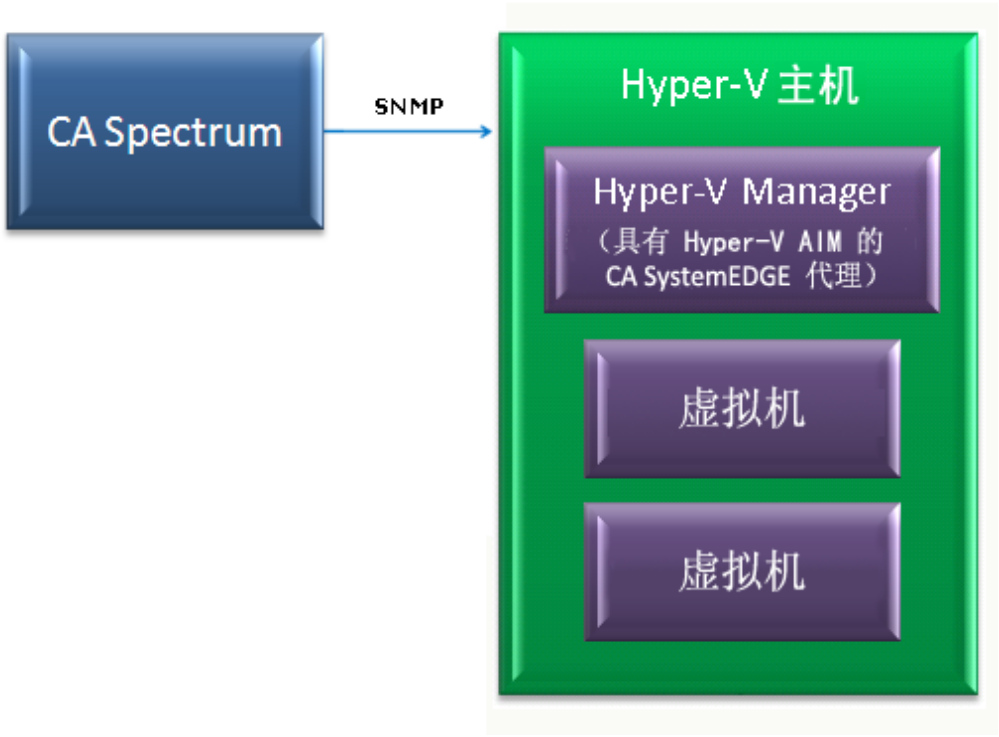
Virtual Host Manager 如何使用 Hyper-V

Microsoft Hyper-V AIM 通过服务器内部查询（而不必访问网络）收集所监控的 Hyper-V 资源的数据。因此，必须在要通过 CA Spectrum 监控的每个 Microsoft Hyper-V 服务器上运行 CA SystemEDGE 代理和 Hyper-V AIM。

如果您的 Microsoft Hyper-V 虚拟机是 Windows 平台虚拟机，建议在 Microsoft Hyper-V 环境中的每个虚拟机上安装 Microsoft Hyper-V 集成服务。Hyper-V 集成服务将优化虚拟机的虚拟化性能。如果没有这些工具，许多功能将不可用。

Microsoft Hyper-V 服务器提供了用于创建、运行和管理虚拟机的功能。Hyper-V AIM 和 CA SystemEDGE 代理与 Microsoft Hyper-V 服务器集成，并收集数据以通过 CA Spectrum 执行 Hyper-V 监控。

下图显示了 CA Spectrum 如何使用已加载 Hyper-V AIM 的 CA SystemEDGE 代理来收集有关 Microsoft Hyper-V 虚拟环境的信息：



如图所示，收集有关 Microsoft Hyper-V 虚拟环境的信息的过程如下：

1. Microsoft Hyper-V 管理操作系统 (请参阅本页中的定义 254)驻留在虚拟环境中的 Microsoft Hyper-V 主机上，其中存储了有关每个主机及其虚拟机的详细数据。
2. Microsoft Hyper-V Manager（其包含已加载 Microsoft Hyper-V AIM 的 CA SystemEDGE 代理）驻留在 Hyper-V 主机服务器上。通过加载该 AIM，CA SystemEDGE 代理可与 Microsoft Hyper-V 管理操作系统进行通信，以收集有关虚拟环境的详细信息。
3. CA Spectrum 定期从 Hyper-V Manager 检索信息，并使用该信息建模和监控虚拟实体。

详细信息：

Virtual Host Manager 的工作原理 (p. 11)
查看 Hyper-V 虚拟网络 (p. 148)
Virtual Host Manager 中的 Hyper-V 数据更新方式 (p. 150)

为 Hyper-V 创建的模型

Virtual Host Manager 提供了多个模型来表示 Microsoft Hyper-V 虚拟技术网络的组件。通过了解以下基本模型，可以帮助您更好地了解发现以及虚拟环境与物理环境的连接方式。

Virtual Host Manager 包括用于 Hyper-V 设备的以下模型和图标：

Hyper-V Manager

表示包含已加载 Hyper-V AIM 的 CA SystemEDGE 代理的服务器。每个 Hyper-V 主机只能有一个 Hyper-V Manager。

图标： 

注意： Hyper-V 管理操作系统在虚拟拓扑中表示为 Hyper-V Manager 模型的一部分。*Hyper-V 管理操作系统*是在 Hyper-V 主机上运行的原始操作系统。Microsoft Hyper-V 使用此操作系统来配置承载的 Hyper-V 虚拟机。此 Hyper-V Manager 模型将根据需要在层次结构和拓扑视图中重复，以表示 Hyper-V 管理操作系统。

Hyper-V 主机

表示在 Hyper-V 虚拟化技术中配置的 Hyper-V 主机。*Hyper-V 主机*是使用 Microsoft Hyper-V 虚拟化软件来运行虚拟机的物理计算机。主机提供 Hyper-V 虚拟机使用的 CPU 和内存资源。它们还为这些虚拟机提供存储访问和网络连接。这些模型充当拓扑视图中的容器模型，以帮助将虚拟实体分组到单独的视图中，同时显示虚拟环境与物理网络的连接情况。不能直接联系 Hyper-V 主机以获取状态信息。而是将通过模型中所含项目的状态来推断这些模型的状态。

图标： 

Hyper-V 虚拟机

表示在 Hyper-V 虚拟化技术中配置的 Hyper-V 虚拟机。*Hyper-V 虚拟机*是一种软件计算机，它能像物理计算机那样运行操作系统和应用程序。虚拟机根据其工作负荷动态地消耗其物理主机上的资源。

图标： 

详细信息：

查看 Hyper-V 虚拟环境 (p. 148)

发现 Hyper-V 网络

本节介绍 Virtual Host Manager 的发现和建模过程。这些任务通常由 Virtual Host Manager 管理员执行。

如何配置发现选项

在安装 Virtual Host Manager 后，可以配置 Virtual Host Manager 以执行 Hyper-V 发现。通过配置首选项，可帮助确保 Virtual Host Manager 正确地为虚拟设备建模。

要为 Hyper-V 发现配置 Virtual Host Manager 安装，请从下列选项中选择首选项：

- 新虚拟机的维护模式 (p. 135) - 允许您决定在可使用 CA Spectrum 来管理新发现的虚拟机之前将其中哪些虚拟机置于维护模式。
- 允许在运行 Hyper-V 发现期间删除设备模型 (p. 135) - 控制当 Hyper-V 主机和 Hyper-V 虚拟机模型不再受 Microsoft Hyper-V 管理时，CA Spectrum 如何处理它们。
- 搜索现有模型 (p. 137) - 确定在 Hyper-V 发现期间 Virtual Host Manager 搜索的安全域。
- 发现支持 SNMP 的设备 (p. 138) - 控制如何在 Hyper-V 发现期间为支持 SNMP 的设备建模。默认情况下，最初仅会将新模型创建为 VHM 模型。但是，此选项允许您覆盖默认设置，并为符合必要标准的设备立即创建 SNMP 模型。
- 在执行 Hyper-V Manager 删除期间保留启用了 SNMP 的虚拟机 (p. 139)- 控制在删除 Hyper-V Manager 模型时，CA Spectrum 如何处理启用了 SNMP 的虚拟机模型。

为新 Hyper-V 虚拟机配置维护模式

Virtual Host Manager 会自动为 Microsoft Hyper-V 管理的虚拟机建模。CA Spectrum 将尝试管理发现的所有模型。但是，某些新发现的 Hyper-V 虚拟机在最初建模时，并未准备好由 CA Spectrum 管理。为了防止在新 Hyper-V 虚拟机模型上生成不必要的警报，您可以决定将哪些新模型立即置于维护模式。之后，可以在准备好由 CA Spectrum 管理这些设备时，在单个模型上手动禁用维护模式。

遵循这些步骤:

1. 在“导航”面板中打开 Virtual Host Manager (p. 109)。

   将在选定 Virtual Host Manager 的“内容”面板中打开详细信息页面。

2. 单击“信息”选项卡。
3. 展开“配置”、“Hyper-V”、“Hyper-V 发现”子视图。
4. 在“新 Hyper-V 虚拟机的维护模式”字段中单击“设置”，然后选择下列选项之一：

   将未启用的 VM 置于维护模式

   （默认）在初始 Hyper-V 发现期间，仅向未启用的 Hyper-V 虚拟机模型应用维护模式。

   将所有 VM 置于维护模式

   在初始 Hyper-V 发现期间，向所有新发现的 Hyper-V 虚拟机模型应用维护模式。

   将保存您的设置，并且会根据您的选择将新发现的由 Virtual Host Manager 创建的 Hyper-V 虚拟机模型置于维护模式。

详细信息：

如何配置发现选项 (p. 134)
状态监控选项 (p. 154)

管理已从 Microsoft Hyper-V 删除的设备的设备模型

虚拟环境中的设备及设备间的关联关系会频繁地发生更改。在 CA Spectrum 中维护有关虚拟环境的准确且及时的数据很具挑战性。例如，删除 Hyper-V 虚拟机时，CA Spectrum 会在“导航”面板中从 Virtual Host Manager 删除相应的设备模型。但是，CA Spectrum 是应保留还是删除模型？您可以选择设置以控制是否删除模型。

重要说明！删除模型时，这些模型上的所有注释或其他自定义也将丢失。如果以后可能会在 Hyper-V 环境中重新创建模型，则禁用此选项。

遵循这些步骤:

1. 在“导航”面板中打开 Virtual Host Manager (p. 46)。

   将在选定 Virtual Host Manager 的“内容”面板中打开主详细信息页面。

2. 单击“信息”选项卡。
3. 展开“配置”、“Hyper-V”、“Hyper-V 发现”子视图。
4. 在“允许在运行 Hyper-V 发现期间删除设备模型”字段中单击“设置”，然后选择下列选项之一：

   是

   （默认）删除不再受 Microsoft Hyper-V 环境管理的实体的对应模型。

   否

   当 Virtual Host Manager 模型的相应实体不再受 Hyper-V 环境管理，但是未从 CA Spectrum 删除这些模型时，将这些模型放置在 LostFound 容器中。

   注意：将以不同的方式处理具有更多关联的模型（如全局集合中包括的模型）。将从 Universe 中删除这些模型，但是不会将其移动到 LostFound 容器中。

   将保存您的设置，并且会在从 Hyper-V 环境中删除设备之后相应地处理设备模型。

详细信息：

如何配置发现选项 (p. 134)
删除 Virtual Host Manager 模型 (p. 159)
针对 Hyper-V 的 Virtual Host Manager 警报 (p. 160)
Virtual Host Manager 中支持的陷阱 (p. 161)
删除 Hyper-V Manager 后管理启用了 SNMP 的虚拟机模型 (p. 139)

跨安全域配置模型搜索

在创建新模型之前，Hyper-V 发现会尝试在 SpectroSERVER 中查找模型。在已部署 Secure Domain Manager 的环境中，Hyper-V 发现将搜索与 Hyper-V Manager 位于同一个安全域中的模型。此域是“本地”域。但是，某些虚拟环境设备可存在于不同的安全域中。在这种情况下，可以配置 Hyper-V 发现以搜索所有安全域中的现有模型。

遵循这些步骤:

1. 在“导航”面板中打开 Virtual Host Manager (p. 46)。

   将在选定 Virtual Host Manager 的“内容”面板中打开详细信息页面。

2. 单击“信息”选项卡。
3. 展开“配置”、“Hyper-V”、“Hyper-V 发现”子视图。
4. 在“搜索现有模型”字段中单击“设置”，然后从下列选项中进行选择：

   在 Hyper-V Manager 的安全域中

   （默认）搜索与 Hyper-V Manager 服务器位于同一个安全域中的现有模型。

   在所有安全域中

   搜索由 SpectroSERVER 管理的所有安全域中的现有模型。仅在下列情况下选择此选项：

   - 所有设备具有唯一的 IP 地址
   - 当安全域用于安全目的或用于隔离网络通信时

   注意：不要为 NAT 环境选择此选项。

   将保存您的设置，并且 Hyper-V 发现会根据您的选择在 CA Spectrum 中搜索现有模型。当多个安全域中存在重复的模型（即共享相同 IP 地址的模型）时，Virtual Host Manager 将执行以下操作：

   - 在本地安全域中选择模型（如果有）。
   - 如果本地域中不存在重复的模型，Virtual Host Manager 将随机地从其他安全域中选择模型。
   - 在这两种情况下，Virtual Host Manager 将在 Hyper-V Manager 模型上为重复的 IP 地址生成次要警报。

详细信息：

如何配置发现选项 (p. 134)

配置 SNMP 建模首选项

支持 SNMP 的虚拟机可支持丰富的设备监控功能，如进程和文件系统监控功能。但是，部署 SNMP 代理可能会花费较高的经济和时间成本。默认情况下，Hyper-V 发现将虚拟机创建为 VHM 模型 (请参阅本页中的定义 255)，可在以后将它们升级为 SNMP 模型。不过，也可以将 Hyper-V 发现配置为将所有支持 SNMP 的新设备建模为 SNMP 模型。虽然完成 Hyper-V 发现可能需要更长的时间，但是初始建模为 SNMP 模型可避免以后手动升级这些模型。

重要说明！ 在为 Hyper-V Manager 服务器建模*之前*，请启用 SNMP 建模。如果首先为 Hyper-V Manager 服务器建模，则会将所有子模型创建为 VHM 模型，并且必须手动将其升级为 SNMP 模型。

遵循这些步骤:

1. 在“导航”面板中打开 Virtual Host Manager (p. 46)。

   将在选定 Virtual Host Manager 的“内容”面板中打开主详细信息页面。

2. 单击“信息”选项卡。

3. 展开“配置”、“Hyper-V”、“Hyper-V 发现”、“SNMP 发现”子视图。

   重要说明！ 要准备设备和 CA Spectrum 以执行 SNMP 发现，请按照子视图中的步骤操作。如果在执行 Hyper-V 发现之前未正确准备设备，Virtual Host Manager 将无法创建 SNMP 模型。

4. 在“发现支持 SNMP 的设备”字段中单击“设置”，然后从下列选项中进行选择：

   是

   在 Hyper-V 发现期间启用 SNMP 建模。仅会将符合“SNMP 发现”子视图文本中指定标准的设备建模为 SNMP 设备。仅适用于*新*模型。

   否

   （默认）将 Hyper-V 发现期间找到的所有新设备建模为 VHM 模型。可在以后手动将这些模型升级为 SNMP 模型。

   将保存您的设置，并且会根据您的选择在 Virtual Host Manager 中为新设备建模。

详细信息：

如何发现和建模虚拟环境 (p. 140)
Hyper-V 发现的工作方式 (p. 143)
向 VHM 模型中添加 SNMP 功能 (p. 144)
删除 Hyper-V Manager 后管理启用了 SNMP 的虚拟机模型 (p. 139)

删除 Hyper-V Manager 后管理启用了 SNMP 的虚拟机模型

默认情况下，删除以下项时，将从 CA Spectrum 中删除启用了 SNMP 的设备：

- 设备的 Hyper-V Manager 模型
- “导航”面板中的 Hyper-V 文件夹

启用了 SNMP 的设备模型可包括要保留的重要自定义。可以调整设置以避免删除这些模型。将它们放置在 LostFound 容器中供以后使用。

遵循这些步骤:

1. 在“导航”面板中打开 Virtual Host Manager (p. 46)。

   将在选定 Virtual Host Manager 的“内容”面板中打开主详细信息页面。

2. 单击“信息”选项卡。
3. 展开“配置”、“Hyper-V”、“Hyper-V 发现”子视图。
4. 在“在执行 Hyper-V Manager 删除期间保留启用了 SNMP 的虚拟机”字段中单击“设置”，然后选择下列选项之一：

   是

   删除其 Hyper-V Manager 或 Hyper-V 文件夹时，将启用了 SNMP 的虚拟机模型保留在 LostFound 容器中。

   注意：将以不同的方式处理具有更多关联的模型（如全局集合中包括的模型）。将从 Universe 中删除这些模型，但是不会将其移动到 LostFound 容器中。

   否

   （默认）删除其 Hyper-V Manager 或 Hyper-V 文件夹时，将删除所有虚拟机模型。

   将保存您的设置。删除 Hyper-V Manager 模型或 Hyper-V 文件夹时，将根据您的选择处理启用了 SNMP 的设备模型。

详细信息：

如何配置发现选项 (p. 134)
管理已从 Microsoft Hyper-V 删除的设备的设备模型 (p. 135)
删除 Virtual Host Manager 模型 (p. 159)

如何发现和建模虚拟环境

要监控虚拟环境，需发现并建模虚拟实体 - Hyper-V Manager、Hyper-V 主机和 Hyper-V 虚拟机。通过在 Virtual Host Manager 中为这些实体建模，可以在一个工具中查看完整的网络拓扑，其中显示了物理组件和虚拟组件之间的关联关系。

为虚拟环境建模的主要步骤如下所示：

1. 运行标准的 CA Spectrum 发现 (p. 141)。

   此发现的目的是确保在运行 Hyper-V 发现之前为上游路由器和交换机建模。或者，如果已禁用“SNMP 建模”选项，则此步骤也可以为支持 SNMP 的虚拟机和 Hyper-V 服务器建模。在为这些实体建模时，请确保正确设置建模选项以支持 Virtual Host Manager。

2. 升级 CA SystemEDGE 模型 (p. 142)。

   只有已在早于 CA Spectrum r9.2.1 的版本中为 Hyper-V 服务器上的 CA SystemEDGE 代理建模后，才需要执行此步骤。

3. 允许运行 Hyper-V 发现 (p. 143)。

   在 Hyper-V 服务器上为 CA SystemEDGE 代理（带有 Hyper-V AIM）建模时，将自动启动 Hyper-V 发现。其中每个 Hyper-V 服务器模型都具有自己的 Hyper-V 发现进程。Hyper-V 发现的目的是找到由 Hyper-V 管理的虚拟实体，为不存在的实体建模，以及将它们放置在“导航”面板的 Virtual Host Manager 视图中。

详细信息：

向 VHM 模型中添加 SNMP 功能 (p. 144)
将 Hyper-V 虚拟机移至其他 Hyper-V 主机 (p. 147)
如何配置管理选项 (p. 155)
配置 SNMP 建模首选项 (p. 138)

运行 CA Spectrum 发现

要发现您的 Hyper-V 环境，请运行标准 CA Spectrum 发现。此发现可确保为上游路由器和交换机建模，以便将来可以从虚拟实体建立连接。您还可以在 CA Spectrum 发现期间为支持 SNMP 的 Hyper-V 虚拟机建模。

注意：仅当在 Hyper-V 发现期间禁用了“SNMP 建模”选项时，才需要在 CA Spectrum 发现期间为支持 SNMP 的 Hyper-V 虚拟机建模。

注意：只有管理员才可以执行此任务。

遵循这些步骤:

1. 打开发现控制台。

   注意：在建模之前，请确保您知道在非标准端口上运行的任何 SNMP 代理的正确团体字符串、IP 地址和端口号。

2. 在“导航”面板中单击  （新建配置）按钮。
3. 配置选项以支持虚拟网络建模，如下所示：
   a. 在“建模选项”组中单击“建模选项”按钮。

      此时将打开“建模配置”对话框。

   b. 单击“协议选项”按钮。

      此时将打开“协议选项”对话框。

   c. 选择“Pingable 项的 ARP 表”选项，然后单击“确定”。

      此时将打开“建模配置”对话框。

   d. （可选）在“高级选项”组中单击“高级选项”按钮。添加非标准 SNMP 端口（如 CA SystemEDGE 代理端口），然后单击“确定”。
4. 输入各个 IP 地址，或在“IP 边界列表”字段中输入开始 IP 地址和结束 IP 地址，然后单击“添加”。

   注意：确保 IP 地址范围中包括所有已安装 CA SystemEDGE 和 Hyper-V AIM 的服务器以及互连交换机和路由器。或者，也可以包括需要 SNMP 模型的支持 SNMP 的 Hyper-V 虚拟机。

5. 在发现控制台中输入任何其他值，然后单击“发现”。

   将创建以下模型，并将其添加到 CA Spectrum 的网络拓扑中：

   - Hyper-V Manager 服务器以及用于将其连接到网络的交换机和路由器 - 有关虚拟环境的信息来自 Hyper-V Manager。当 CA Spectrum 中存在这些 Hyper-V Manager 模型时，Hyper-V 发现即可启动。
   - Hyper-V 主机和 Hyper-V 虚拟机 - 如果您决定不使用 CA Spectrum 发现为这些实体建模，则 Hyper-V 发现会将它们创建为 VHM 模型 (请参阅本页中的定义 255)。

   注意：也可以通过 IP 地址手动为虚拟网络建模。在这种情况下，建议首先为上游设备建模。按正确顺序建模可确保在拓扑中正确生成这些实体之间的关联关系。有关如何执行发现的详细信息，请参阅《*IT 基础架构建模与管理 - 管理员指南*》。

详细信息：

向 VHM 模型中添加 SNMP 功能 (p. 144)
将 Hyper-V 虚拟机移至其他 Hyper-V 主机 (p. 147)
如何配置管理选项 (p. 155)
配置 SNMP 建模首选项 (p. 138)

升级 CA SystemEDGE 模型

在安装 Virtual Host Manager 之前或者在代理上加载 Hyper-V AIM 之前，可能已在 CA Spectrum 中为 CA SystemEDGE 代理建模。在这种情况下，现有的 CA SystemEDGE 模型与 Virtual Host Manager 不兼容。升级该模型，以便 Virtual Host Manager 可以访问 CA SystemEDGE 中的 Hyper-V AIM 功能。*如果在安装 CA Spectrum 后为带有 Hyper-V AIM 的 CA SystemEDGE 代理建模，则不需要执行此过程。*

要升级 CA SystemEDGE 模型，请右键单击该模型并依次选择“重新配置”、“重新配置模型”。

CA SystemEDGE 模型将升级，以支持 Hyper-V AIM。

注意：也可以使用 CLI 向 CA SystemEDGE 发送重新配置模型操作。有关详细信息，请参阅《*IT 基础架构建模与管理 - 管理员指南*》。

详细信息：

向 VHM 模型中添加 SNMP 功能 (p. 144)
将 Hyper-V 虚拟机移至其他 Hyper-V 主机 (p. 147)
如何配置管理选项 (p. 155)

Hyper-V 发现的工作方式

Hyper-V 发现是专门用于收集有关虚拟环境的详细信息的发现进程。Hyper-V 发现的目的是获取由 Microsoft Hyper-V 管理的虚拟实体，为 CA Spectrum 中不存在的实体建模，以及将它们放置在“导航”面板中的 Virtual Host Manager 下。

Hyper-V 发现的主要优点是，它在后台自动运行，可使 CA Spectrum 中的虚拟环境数据保持更新。通过了解 Hyper-V 发现的工作方式，可更有力地说明正确安装和建模各个 Virtual Host Manager 组件的重要性。

Hyper-V 发现进程的工作方式如下：

1. 在安装 CA SystemEDGE 代理和 Hyper-V AIM 之后，Hyper-V AIM 将立即与 Hyper-V 主机进行通信，以收集有关其管理的虚拟实体的信息。Hyper-V AIM 将存储此信息。

   重要说明！ 必须安装 CA SystemEDGE 代理和 Hyper-V AIM，CA SystemEDGE、Hyper-V 虚拟化技术和 CA Spectrum 才能进行通信。如果它们无法通信，Hyper-V 发现将无法运行。

2. 在 CA Spectrum 发现期间，CA Spectrum 将为步骤 1 中的每个服务器创建一个 Hyper-V Manager 模型，并允许 CA Spectrum 处理 CA Spectrum 和 CA SystemEDGE 代理之间的通信。

3. CA Spectrum 将轮询 Hyper-V AIM，以收集在步骤 1 中存储的 Hyper-V 信息。

4. CA Spectrum 将启动 Hyper-V 发现，并使用来自 AIM 的此信息在 CA Spectrum“拓扑”选项卡和“导航”面板的 Virtual Host Manager 层次结构中更新建模，如下所示：

   a. 如果在步骤 2 之前启用 SNMP 发现，则 Virtual Host Manager 发现将为符合 SNMP 发现标准的所有支持 SNMP 的新模型创建 SNMP 模型。

      注意：默认情况下，将在 Hyper-V 发现期间禁用 SNMP 发现。

   b. 将为 Hyper-V Manager 创建 VHM 模型。

   c. 以前存在的 Hyper-V 虚拟机模型将更改为 VHM 模型。

   d. 将为 CA Spectrum 中不存在的 Hyper-V 虚拟机创建 VHM 模型。

e. 将为 Hyper-V 主机模型创建 VHM 模型，这些模型将在“导航”面板的 Virtual Host Manager 下以及 Universe 拓扑中对其关联的 Hyper-V 虚拟机模型进行分组。

f. 虚拟网络的所有模型将添加到“导航”面板的 Virtual Host Manager 部分中。

注意：在虚拟环境中，不同 ESX 主机上的设备可能具有相同的 IP 地址或 MAC 地址。在这种情况下，CA Spectrum 将为每个 IP 地址或 MAC 地址创建重复的模型。

5. Hyper-V 发现将自动按每个定期排定的 Hyper-V 轮询时间间隔重复该过程。

注意：默认情况下，通过在 Hyper-V Manager 模型上设置轮询时间间隔来控制 Hyper-V 轮询时间间隔。或者，也可以通过使用 Hyper-V 服务器应用程序模型来控制 Hyper-V 轮询。

详细信息：

向 VHM 模型中添加 SNMP 功能 (p. 144)
将 Hyper-V 虚拟机移至其他 Hyper-V 主机 (p. 147)
如何配置管理选项 (p. 155)
控制 Hyper-V AIM 轮询 (p. 157)
跨安全域配置模型搜索 (p. 137)

向 VHM 模型中添加 SNMP 功能

支持 SNMP 的虚拟机可支持丰富的设备监控功能，如进程和文件系统监控功能。但是，部署 SNMP 代理可能会花费较高的经济和时间成本。当 SNMP 代理不可用或禁用了 SNMP 发现时，Virtual Host Manager 会将 Hyper-V 虚拟机创建为 VHM 模型 (请参阅本页中的定义 255)。

之后，您可以在任何虚拟机上安装 SNMP 代理，并在 CA Spectrum 中升级其建模。用于升级到 SNMP 模型的选项如下所示：

- **仅升级选定设备** - 当需要升级少量选定模型时，此方法可快速完成工作。首先将删除 VHM 模型和子模型。此方法的一个缺点是，在 CA Spectrum 删除模型之后，必须等待下一个 Hyper-V 发现进程以创建新 SNMP 模型，并将它们放置在 Virtual Host Manager 中。必须知道模型的 IP 地址才能进行升级。
- **升级所有支持 SNMP 的 VHM 模型** - 此方法可批量升级模型。在将 Virtual Host Manager 升级为新版本时，最好使用此方法。对于此方法，不必知道各个模型的 IP 地址。另一个优点是，在 CA Spectrum 删除 VHM 模型之后，会立即将升级后的 SNMP 模型放置在 Virtual Host Manager 层次结构中，而不必等待下一个轮询周期。因此，子模型不会处于非受管状态。

  此方法的一个缺点是可能需要很长时间才能完成。完成此升级所需的时间取决于在查找支持 SNMP 的设备时，Virtual Host Manager 必须搜索的团体字符串和 SNMP 端口的数量。

  注意： Virtual Host Manager 仅会尝试识别已启动的可 Ping 虚拟机上的 SNMP 代理。

重要说明！ 删除模型时，这些模型上的所有注释或其他自定义也将丢失。

详细信息：

如何发现和建模虚拟环境 (p. 140)
删除 Virtual Host Manager 模型 (p. 159)
配置 SNMP 建模首选项 (p. 138)

将选定 VHM 模型升级为 SNMP 模型

当 SNMP 代理不可用或在 Hyper-V 发现期间禁用了 SNMP 发现时，Virtual Host Manager 会将 Hyper-V 虚拟机创建为 VHM 模型 (请参阅本页中的定义 255)。之后，您可以在任何虚拟机上安装 SNMP 代理，并在 CA Spectrum 中升级其建模。您必须知道 IP 地址才能升级设备模型。手动选择要升级的模型可快速完成，但这些模型上的所有说明或自定义将会在升级期间丢失。

遵循这些步骤:

1. 根据需要在设备上部署或启用 SNMP 代理。
2. 使用下列方法之一重新建模设备：
   - CA Spectrum 发现
   - 按 IP 地址为设备逐个建模

在创建支持 SNMP 的新模型时，CA Spectrum 将从 Virtual Host Manager 中移除以前的模型并将其删除。在下一个 Hyper-V AIM 轮询周期中，CA Spectrum 将支持 SNMP 的模型添加到“导航”面板的 Virtual Host Manager 中。

重要说明！删除模型时，这些模型上的所有注释或其他自定义也将丢失。

详细信息：

管理已从 Microsoft Hyper-V 删除的设备的设备模型 (p. 135)
如何发现和建模虚拟环境 (p. 140)
删除 Virtual Host Manager 模型 (p. 159)

将所有 VHM 模型升级为 SNMP 模型

当 SNMP 代理不可用或在 Hyper-V 发现期间禁用了 SNMP 发现时，Virtual Host Manager 会将 Hyper-V 虚拟机创建为 VHM 模型 (请参阅本页中的定义 255)。之后，您可以在任何虚拟机上安装 SNMP 代理，并在 CA Spectrum 中升级其建模。在执行批量升级时，CA Spectrum 将搜索所有 VHM 模型，以查找现在作为支持 SNMP 的设备的模型。CA Spectrum 会将它们转换为 SNMP 模型。此方法可能需要很长的时间才能完成，具体取决于 Virtual Host Manager 必须搜索的团体字符串和端口的数量。

遵循这些步骤:

1. 根据需要在设备上部署或启用 SNMP 代理。
2. 在“导航”面板中打开 Virtual Host Manager (p. 46)。

   将在选定 Virtual Host Manager 的“内容”面板中打开主详细信息页面。
3. 在“导航”面板中选择用于管理要升级的模型的 Hyper-V Manager 模型。
4. 单击“信息”选项卡。
5. 展开“Hyper-V Manager”、“CA Spectrum 建模控制”子视图。
6. 单击“升级 ICMP 专用设备”。

   重要说明！删除模型时，这些模型上的所有注释或其他自定义也将丢失。

   Virtual Host Manager 将搜索由选定 Hyper-V Manager 设备上的 Hyper-V AIM 管理的 VHM 模型。Virtual Host Manager 升级符合 SNMP 设备标准的 ICMP 专用设备，并将它们放置在 Virtual Host Manager 层次结构中。

将 Hyper-V 虚拟机移至其他 Hyper-V 主机

将 Hyper-V 虚拟机从一个 Hyper-V 主机移至另一个 Hyper-V 主机可能会导致数据丢失。风险取决于 Virtual Host Manager 配置。Hyper-V AIM 不支持虚拟机迁移。对于 Virtual Host Manager，会将移动过程视为两个事件 - 从原始 Hyper-V 主机中删除虚拟机，然后向新 Hyper-V 主机添加新虚拟机。在这种情况下，Virtual Host Manager 将删除原始虚拟机，并创建一个新的虚拟机。如果您已自定义原始模型，则删除它可能会导致数据丢失。如果在移动虚拟机之前正确配置 Virtual Host Manager 设置，则可以避免此数据丢失。

遵循这些步骤:

1. 将“允许在运行 Hyper-V 发现期间删除设备模型”选项更改为“否” (p. 135)。

   注意：如果禁用此选项，则在从 Virtual Host Manager 管理中移除虚拟机模型时，CA Spectrum 不会删除此模型。

2. 使用 Microsoft Hyper-V 虚拟化技术从原始 Hyper-V 主机中删除虚拟机。
3. 在“导航”面板中，等待 Virtual Host Manager 反映这些更改。
4. 使用 Microsoft Hyper-V 虚拟化技术向其他 Hyper-V 主机中添加虚拟机。

   当 Hyper-V 发现找到新虚拟机时，Virtual Host Manager 会将其与现有模型进行协调。Virtual Host Manager 将该模型置于 Virtual Host Manager 管理中。

5. （可选）在原始 Hyper-V Manager 模型上将“允许在运行 Hyper-V 发现期间删除设备模型”选项更改回“是”。

   将成功移动虚拟机。

详细信息：

如何发现和建模虚拟环境 (p. 140)
运行 CA Spectrum 发现 (p. 141)
升级 CA SystemEDGE 模型 (p. 142)
Hyper-V 发现的工作方式 (p. 143)
Virtual Host Manager 中的 Hyper-V 数据更新方式 (p. 150)

查看 Hyper-V 虚拟环境

本节介绍有关查看 Hyper-V 虚拟环境和关联警报的概念。基本步骤与标准 CA Spectrum 步骤相同。但是，本节介绍仅适用于 Hyper-V 虚拟技术的概念差异和详细信息。

查看 Hyper-V 虚拟网络

在“资源管理器”选项卡上，Virtual Host Manager 节点显示了分层树结构，可帮助您可视化虚拟环境资源间的逻辑关联关系。

使用此信息，可以了解资源在 Hyper-V Manager 之间的共享情况。此信息可以帮助您发现重新组织和优化虚拟环境的机会。通过此层次结构，还可以快速监控资源性能以及排除警报故障。

由于 Virtual Host Manager 无法识别 DSS 环境 (请参阅本页中的定义 255)，因此它位于格局层次结构中。以下示例显示了 Virtual Host Manager 在“导航”面板中“资源管理器”选项卡上的位置，并演示了虚拟环境的层次结构：

```
[-] SpectroSERVER 主机
    [+] Universe
    [-] Virtual Host Manager
        [-] Hyper-V
            [+] Hyper-V Manager 1
            [-] Hyper-V Manager 2
                [-] Hyper-V 主机
                    . Hyper-V Manager 2（管理操作系统）
                    . Hyper-V 虚拟机 1
                    . Hyper-V 虚拟机 2
```

注意：Hyper-V 管理操作系统在虚拟拓扑中表示为 Hyper-V Manager 模型的一部分。

Virtual Host Manager 是由此 SpectroSERVER 管理的整个虚拟环境的根节点。在“导航”面板中选择此节点后，将在“内容”面板中显示 Virtual Host Manager 详细信息。您可以查看与虚拟环境相关的事件和警报等详细信息。

虚拟环境将直接在 Virtual Host Manager 下表示关联技术的文件夹中进行组织。在上面的示例层次结构中，Hyper-V 文件夹包含使用 Microsoft Hyper-V 虚拟化技术创建的虚拟环境部分。在此文件夹中，Virtual Host Manager 列出了由此 SpectroSERVER 管理的所有 Hyper-V Manager 主机。

每个 Hyper-V Manager 仅包含它管理的虚拟环境部分。在“导航”面板中选择某个 Hyper-V Manager 后，将在“内容”面板中显示相关详细信息，例如由选定 Hyper-V Manager 管理的 Hyper-V 主机或 Hyper-V 虚拟机。

在每个 Hyper-V Manager 下，层次结构表示下列实体之间的逻辑关联关系：

- **Hyper-V 主机**

  Hyper-V 主机包含其管理的 Hyper-V 虚拟机。在“导航”面板中选择某个 Hyper-V 主机后，将在“内容”面板中显示相关详细信息，例如与该 Hyper-V 主机相关的事件和警报、内存使用率、状态等。

- **Hyper-V 管理操作系统**

  Hyper-V 管理操作系统模型显示为其相应 Hyper-V 主机模型的子项，并且始终为 Virtual Host Manager 层次结构树中的叶节点。此模型共享其父项的名称和模型类型。虽然此模型看起来与 Hyper-V Manager 模型相同，但是显示在 Hyper-V 主机模型下的实例将表示在 Hyper-V 主机上运行的管理操作系统。Hyper-V 使用此操作系统来配置承载的 Hyper-V 虚拟机。在“导航”面板中选择某个 Hyper-V 管理操作系统模型后，将在“内容”面板中显示相关详细信息，包括系统状态、CPU 和内存使用率。

- **Hyper-V 虚拟机**

  Hyper-V 虚拟机始终为 Virtual Host Manager 层次结构树中的叶节点。在“导航”面板中选择某个 Hyper-V 虚拟机后，将在“内容”面板中显示相关详细信息，例如与该虚拟机相关的事件和警报、内存使用率和状态。

详细信息：

Virtual Host Manager 如何使用 Hyper-V (p. 131)
为 Hyper-V 创建的模型 (p. 133)
运行 CA Spectrum 发现 (p. 141)
虚拟实体类型的自定义子视图 (p. 152)
用于 Hyper-V 搜索的定位器选项卡 (p. 153)

了解 Hyper-V 虚拟拓扑

为虚拟环境创建的 Hyper-V Manager/管理操作系统、Hyper-V 主机和 Hyper-V 虚拟机模型将集成到拓扑视图中。Hyper-V 主机模型会自动分组其关联的 Hyper-V 虚拟机。拓扑将显示这些 Hyper-V 虚拟机如何连接到物理网络实体。

注意：Hyper-V 管理操作系统在虚拟拓扑中表示为 Hyper-V Manager 模型的一部分。

下列示例显示了这些模型在“导航”面板的“资源管理器”选项卡中 Universe 组下的显示方式：

```
[-] Universe
     . 物理交换机 1
     . 物理交换机 2
   [-] Hyper-V 主机
        . 扇出 1
        . 扇出 2
        . Hyper-V Manager（管理操作系统）
        . Hyper-V 虚拟机 1
        . Hyper-V 虚拟机 2
        . Hyper-V 虚拟机 3
```

选择这些模型之一后，将在“内容”面板的“拓扑”选项卡上以图形方式显示这些关联关系。

详细信息：

为 Hyper-V 创建的模型 (p. 133)
Virtual Host Manager 中的 Hyper-V 数据更新方式 (p. 150)
用于 Hyper-V 搜索的定位器选项卡 (p. 153)

Virtual Host Manager 中的 Hyper-V 数据更新方式

在 CA Spectrum 构建初始 Hyper-V 层次结构之后，可以更改虚拟网络配置。Virtual Host Manager 将持续工作，以保持此信息在 CA Spectrum 中是准确的。例如，以下事件可能会更改虚拟网络配置：

- 在 Hyper-V 主机上创建或删除 Hyper-V 虚拟机
- 手动将 Hyper-V 虚拟机从一个 Hyper-V 主机移至另一个 Hyper-V 主机

为了保持信息准确，Virtual Host Manager 通过轮询 Hyper-V AIM 来检测这些更改。因此，如果虚拟网络配置发生更改，则会在每个轮询周期内将这些更改反映到 CA Spectrum 中。CA Spectrum 还会从 AIM 接收陷阱，并生成相应的事件。通过查看事件日志，可以查明配置发生更改的时间（例如创建新虚拟机的时间）。

在删除虚拟机时，CA Spectrum 将从“资源管理器”选项卡的 Virtual Host Manager 层次结构中删除模型。当 AIM 检测到向您的虚拟网络配置中添加了内容时（如创建新虚拟机或将某个虚拟机置于管理中时），CA Spectrum 将执行以下任务：

- 在“资源管理器”选项卡的层次结构中，更新虚拟设备模型的放置
- *自动*重新发现与受影响的 Hyper-V Manager 和虚拟机模型的连接，并将它们与拓扑中的正确 Hyper-V 主机关联

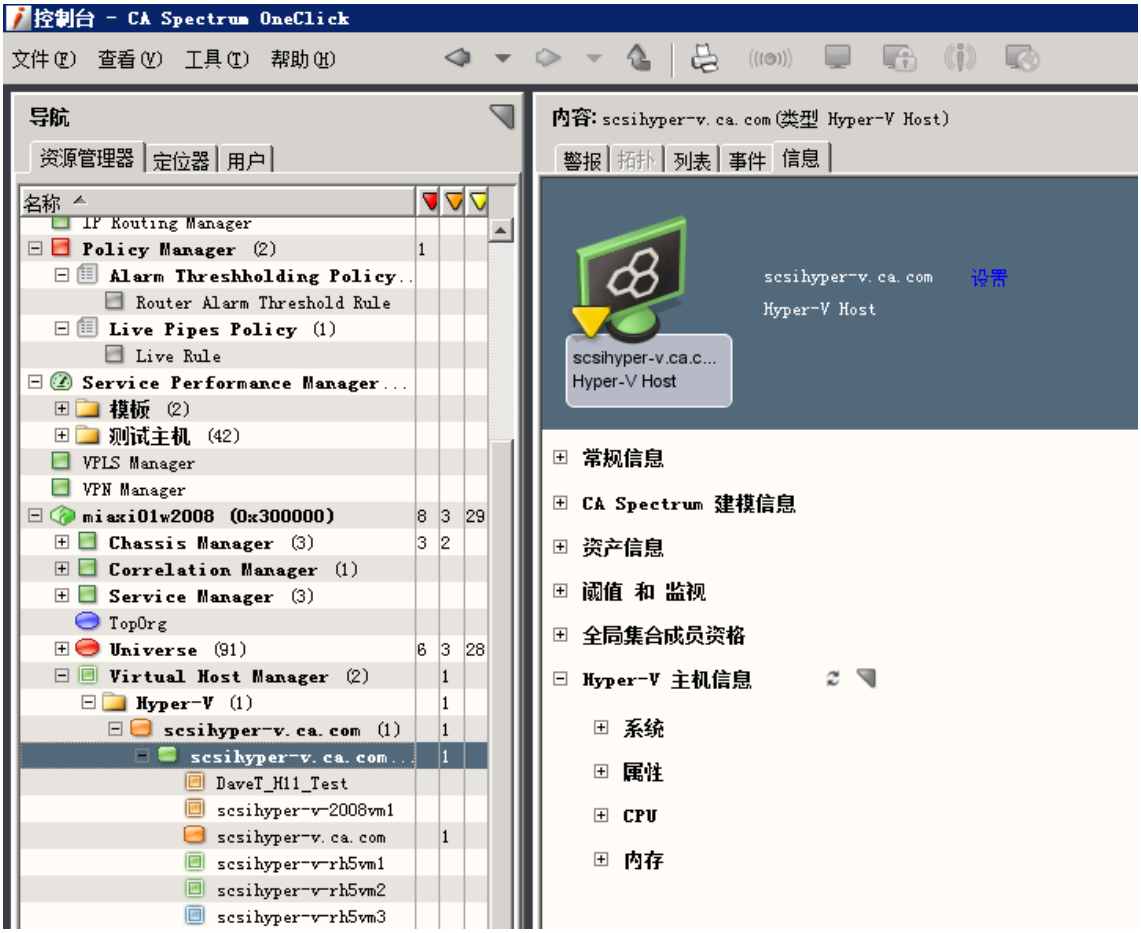
  注意：虽然会自动发现虚拟环境的大多数组件，但是 CA Spectrum 管理员应启动新的 SNMP 发现来为*新*交换机或路由器建模。仅当配置不与现有虚拟网络模型共享连接的新虚拟主机时，才有必要执行此发现。

详细信息：

Virtual Host Manager 的工作原理 (p. 11)
为 Hyper-V 创建的模型 (p. 133)
管理已从 Microsoft Hyper-V 删除的设备的设备模型 (p. 135)
将 Hyper-V 虚拟机移至其他 Hyper-V 主机 (p. 147)
查看 Hyper-V 虚拟网络 (p. 148)
配置和监控资源状态 (p. 156)

虚拟实体类型的自定义子视图

您的各个 Virtual Host Manager 模型将共同提供有关虚拟环境的信息。每个模型将单独提供特定的信息或配置设置，具体取决于其表示的虚拟实体类型。此自定义子视图显示在“内容”面板的“信息”选项卡上。这些子视图可包含实时数据，例如 CPU 状态或内存利用率。例如，针对 Hyper-V Manager 的自定义子视图是“Hyper-V Manager”子视图，如下所示：



注意：Hyper-V Manager 模型提供由 Hyper-V Manager 管理的所有虚拟设备的组合信息。也就是说，在“导航”面板中选择 Hyper-V Manager 模型，可显示有关选定 Hyper-V Manager 主机的信息，*以及*有关所有 Hyper-V 主机和 Hyper-V 虚拟机的组合信息。此信息与在每个单独实体模型的“信息”选项卡上显示的数据相同。Hyper-V Manager 模型中的组合视图可以很好地概述它管理的所有虚拟实体。

详细信息：

查看 Hyper-V 虚拟网络 (p. 148)
配置和监控资源状态 (p. 156)

用于 Hyper-V 搜索的定位器选项卡

除了在“资源管理器”选项卡上查看有关虚拟环境的详细信息外，还可以使用“定位器”选项卡运行预配置的 Virtual Host Manager 搜索。搜索选项在“定位器”选项卡中的“虚拟主机管理”->“Hyper-V”文件夹下进行分组，如下所示：

这些详细搜索可以帮助您调查仅与虚拟实体相关的信息，例如查找格局中的所有 Hyper-V 虚拟机。

注意：虽然 Virtual Host Manager 无法识别 DSS (请参阅本页中的定义 255)，但是这些预配置搜索允许您在搜索参数中选择多个要搜索的格局。

“导航”面板的“定位器”选项卡中包含针对 Virtual Host Manager 信息的以下搜索：

所有主机

在 CA Spectrum 数据库中查找已为虚拟网络建模的所有 Hyper-V 主机服务器。

所有管理操作系统

在 CA Spectrum 数据库中查找已为虚拟网络建模的所有 Hyper-V 管理操作系统 (请参阅本页中的定义 254)。

注意：Hyper-V 管理操作系统在虚拟拓扑中表示为 Hyper-V Manager 模型的一部分。

所有管理器

在 CA Spectrum 数据库中查找已为虚拟网络建模且承载已启用 Hyper-V AIM 的 CA SystemEDGE 代理的服务器。

所有虚拟机

在 CA Spectrum 数据库中查找已为虚拟网络建模的所有 Hyper-V 虚拟机。

虚拟机 - 按主机名

在 CA Spectrum 数据库中查找仅由一个或一组选定 Hyper-V 主机管理的虚拟机。

详细信息：

查看 Hyper-V 虚拟网络 (p. 148)

状态监控选项

CA Spectrum 提供了多种用于监控虚拟网络资源状态的选项。为资源提供的状态信息将有所不同，具体取决于您监控的虚拟实体的类型。此外，您是否能够配置状态选项取决于其类型。例如，一些状态选项是只读选项，而另外一些状态选项则允许您启用行为或选择警报重要级别。通过提供此系列选项和自定义级别，CA Spectrum 允许您决定如何以最佳方式监控虚拟网络的性能。

状态字段位于 OneClick 子视图中。Hyper-V Manager 模型上以表格格式提供了给定虚拟环境的所有状态信息。此外，在 CA Spectrum 中具有唯一模型的每个虚拟实体类型将提供相同状态信息的子集，以便于查看。可以从任一视图位置设置与状态相关的设置，包括报警类型和监控器设置。

下表概述了为每个虚拟实体类型提供的状态信息的类型。“子视图位置”列介绍了相应状态字段在 OneClick 中的位置。例如，在“信息”选项卡上的以下两个位置中提供了 Hyper-V 虚拟机模型的“内存”信息：

- Hyper-V 虚拟机模型的“虚拟机信息”子视图
- Hyper-V Manager 模型的“Hyper-V Manager”->“管理的环境”->“虚拟机”子视图

要浏览可用于每个状态信息类型的确切状态选项，请在 OneClick 中查找子视图。

Hyper-V Manager

状态信息类型	子视图位置
总体状态	Hyper-V Manager

Hyper-V 主机

状态信息类型	子视图位置
总体状态	Hyper-V 主机
CPU	Hyper-V 主机、Hyper-V Manager
内存	Hyper-V 主机、Hyper-V Manager

Hyper-V 虚拟机

状态信息类型	子视图位置
总体状态	Hyper-V 虚拟机、Hyper-V Manager
内存	Hyper-V 虚拟机、Hyper-V Manager
CPU	Hyper-V 虚拟机、Hyper-V Manager

详细信息：

配置和监控资源状态 (p. 156)
针对 Hyper-V 的 Virtual Host Manager 警报 (p. 160)
Virtual Host Manager 中支持的陷阱 (p. 161)

如何配置管理选项

在为虚拟网络建模之后，可以配置 Virtual Host Manager 选项以查看和管理设备模型。通过配置首选项，可帮助确保 Virtual Host Manager 正确处理虚拟设备模型，并仅监控您需要的重要信息。

要配置 Virtual Host Manager 安装，请在发现并建模虚拟网络之后执行以下过程：

- 配置阈值和其他状态监控选项 (p. 156)- 这些选项允许您确定要监控的信息，以及 CA Spectrum 如何管理虚拟网络中发生的各种事件。

详细信息：

升级 CA SystemEDGE 模型 (p. 142)
Virtual Host Manager 中的 Hyper-V 数据更新方式 (p. 150)

配置和监控资源状态

可以在 OneClick 中监控虚拟资源的状态。例如，可以查看总物理内存或已用物理内存等。还可以设置监控选项，如启用报警。此信息可以帮助您优化虚拟网络性能以及排除警报故障。

注意：将在 Hyper-V AIM 上设置陷阱，并由其来管理它们。

可以在“信息”选项卡上查看或配置虚拟设备的资源状态选项和信息。

遵循这些步骤:

1. 在“导航”面板中打开 Virtual Host Manager (p. 46)。

   将在选定 Virtual Host Manager 的“内容”面板中打开主详细信息页面。

2. 在“导航”面板的“资源管理器”选项卡上找到并单击虚拟设备。

   将在“内容”面板中显示设备的详细信息。

3. 单击“信息”选项卡。

   可查看多个子视图。通常，该选项卡底部的子视图中包括选定模型的资源分配和利用率信息。例如，Hyper-V 主机模型将显示一个名为“Hyper-V 主机信息”的子视图，其中包括您在“导航”面板中选择的特定 Hyper-V 主机模型的详细信息。

4. 展开相应的子视图。

   将显示选定设备模型的所有可用资源状态详细信息和监控选项。

   注意：Hyper-V Manager 模型提供由 Hyper-V Manager 管理的所有虚拟设备的组合信息。也就是说，在“导航”面板中选择 Hyper-V Manager 模型，可显示有关选定 Hyper-V Manager 主机的信息，*以及*有关所有 Hyper-V 主机和 Hyper-V 虚拟机的组合信息。此信息与在每个单独实体模型的“信息”选项卡上显示的数据相同。Hyper-V Manager 模型中的组合视图可以很好地概述它管理的所有虚拟实体。

详细信息：

虚拟实体类型的自定义子视图 (p. 152)
状态监控选项 (p. 154)
如何配置管理选项 (p. 155)
针对 Hyper-V 的 Virtual Host Manager 警报 (p. 160)

控制 Hyper-V AIM 轮询

在调整 Virtual Host Manager 性能时，可以更改 Hyper-V Manager 轮询速率，或禁用 Hyper-V 技术轮询。默认情况下，Hyper-V Manager 模型上的轮询属性用于控制 Hyper-V 轮询行为。或者，也可以单独更改此 Hyper-V 轮询行为。Hyper-V 技术应用程序模型 HyperVAimApp 用于控制 Hyper-V 轮询。

此应用程序上的以下两个属性值专门用于控制 Hyper-V 轮询逻辑：

- PollingStatus
- Polling_Interval

Hyper-V Manager 模型和 HyperVAimApp 应用程序模型都包含这些属性。PollingStatus 用于禁用和启用轮询，而 Polling_Interval 用于控制轮询频率。如果它们的值不同，则在确定 Hyper-V 技术轮询行为时，优先考虑 HyperVAimApp 应用程序模型属性值。

通过为设备模型和应用程序模型设置值，您可以微调 Hyper-V 技术轮询。对于 PollingStatus 和 Polling_Interval，修改 Hyper-V Manager 设备模型上的属性时还将更改相应的应用程序模型属性（如果它们的值相同）。

详细信息：

Hyper-V 发现的工作方式 (p. 143)

配置 Hyper-V AIM 轮询时间间隔

您可以更改 Hyper-V AIM 轮询速率。可通过设置 Hyper-V 技术应用程序模型上的 Polling_Interval 属性来配置轮询时间间隔。

遵循这些步骤:

1. 打开 OneClick，并单击“导航”面板中的“定位器”选项卡。
2. 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。
3. 在“设备 IP 地址”字段中输入 Hyper-V Manager 设备的 IP 地址，然后单击“确定”。

   将在“内容”面板中显示 Hyper-V Manager 的应用程序模型的列表。
4. 选择 HyperVAimApp 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. 单击“组件详细信息”面板中的“信息”选项卡。
6. 打开“建模信息”子视图。
7. 在“轮询时间间隔(秒)”字段中单击“设置”，然后输入新值。

   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 Hyper-V AIM 轮询。但是，如果将“轮询时间间隔”设置为 0，并将“轮询”字段设置为“打开”，Hyper-V AIM 轮询将按照为 Hyper-V Manager 设备设置的轮询时间间隔继续运行。

   Hyper-V AIM 轮询时间间隔设置即已修改。

禁用 Hyper-V AIM 轮询

可以禁用 Hyper-V AIM 轮询。禁用 Hyper-V 轮询的过程与禁用 Virtual Host Manager 的过程相同。可以通过在 Hyper-V 虚拟技术应用程序模型上设置 PollingStatus 属性来禁用轮询。

遵循这些步骤:

1. 打开 OneClick，并单击“导航”面板中的“定位器”选项卡。
2. 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。
3. 在“设备 IP 地址”字段中输入 Hyper-V Manager 设备的 IP 地址，然后单击“确定”。

   将在“内容”面板中显示 Hyper-V Manager 的应用程序模型的列表。

4. 选择 HyperVAimApp 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. 单击“组件详细信息”面板中的“信息”选项卡。

6. 打开 CA Spectrum 的“建模信息”子视图。

7. 单击“轮询”字段中的“设置”，然后选择“关闭”。

   将在选定的 Hyper-V Manager 上为 Hyper-V AIM 禁用轮询。

删除 Virtual Host Manager 模型

可以随时出于各种原因从 OneClick 中删除模型。但是，Virtual Host Manager 会限制您在“导航”面板的 Virtual Host Manager 层次结构中删除模型的能力。要手动删除模型，有以下两个选项可用：

- 在 Virtual Host Manager 中删除 Hyper-V 文件夹或 Hyper-V Manager 模型
- 使用 Microsoft Hyper-V 虚拟化技术删除虚拟实体

在 Virtual Host Manager 中，有时会自动删除模型。下列情况会导致 CA Spectrum 自动删除 Virtual Host Manager 模型：

- **已删除 Hyper-V 文件夹，或者已从 Virtual Host Manager 中删除 Hyper-V Manager 模型**

  如果删除 Hyper-V Manager 模型，或从“导航”面板中删除 Hyper-V 文件夹，CA Spectrum 将会删除所有相关的子模型。

- **已从 Hyper-V 虚拟环境中删除实体**

  使用 Microsoft Hyper-V 虚拟化技术删除 Hyper-V 主机和 Hyper-V Manager 时，CA Spectrum 可能还会根据您的配置设置从 Virtual Host Manager 中删除这些模型及其子模型。

- **存在已升级模型** - 在某些情况下，会首先为无 SNMP 功能的 Virtual Host Manager 建模 Hyper-V 主机。如果以后向 VHM 模型 (请参阅本页中的定义 255)添加 SNMP 功能，则之前的模型将被删除，并替换为支持 SNMP 的新模型。

注意：虽然默认设置是删除模型，但是您可以配置 Virtual Host Manager，以便在从 Virtual Host Manager 中删除 Hyper-V 主机和 Hyper-V 虚拟机模型时将它们放置在 LostFound 容器中。仅当使用 Microsoft Hyper-V 虚拟环境删除实体时，才应用此设置。但是，在删除 Hyper-V 文件夹、删除 Hyper-V Manager 模型或升级 VHM 模型时，不会应用此设置。

详细信息：

管理已从 Microsoft Hyper-V 删除的设备的设备模型 (p. 135)
向 VHM 模型中添加 SNMP 功能 (p. 144)
删除 Hyper-V Manager 后管理启用了 SNMP 的虚拟机模型 (p. 139)

Hyper-V 的警报和故障隔离

本节介绍 Virtual Host Manager 所使用的陷阱以及生成的警报。本节还说明 Virtual Host Manager 故障隔离与基础 CA Spectrum 故障隔离有何差异。

针对 Hyper-V 的 Virtual Host Manager 警报

为了就虚拟网络中出现的问题向您报警，CA Spectrum 将在轮询期间生成警报。通过轮询可生成四个警报：“Hyper-V 代理已丢失”、“Hyper-V 主机代理已丢失”、“Hyper-V Manager 不可用”和“Hyper-V 虚拟机未运行”。

详细信息：

管理已从 Microsoft Hyper-V 删除的设备的设备模型 (p. 135)
状态监控选项 (p. 154)
配置和监控资源状态 (p. 156)
删除 Hyper-V Manager 后管理启用了 SNMP 的虚拟机模型 (p. 139)

CA Spectrum 如何从 CA SystemEDGE 转发陷阱

CA Spectrum 支持由 Hyper-V AIM 发送的所有陷阱。最初会将这些陷阱发送给 Hyper-V CA SystemEDGE 模型。如果陷阱的目标不是 Hyper-V 模型，则 CA Spectrum 会将陷阱转发给正确的虚拟模型。

注意：对于与陷阱相关的特定事件代码，请使用事件配置应用程序并针对“0x056e”进行筛选。或者，可以启动 MIB 工具以便在“CAHYPERV-AIM-MIB”MIB 的“陷阱支持”表中查看陷阱。有关使用事件配置应用程序的详细信息，请参阅《*事件配置用户指南*》。有关使用 MIB 工具的详细信息，请参阅《*IT 基础架构建模与管理 - 管理员指南*》。

CA Spectrum 使用以下过程确定要将陷阱转发到的位置：

1. CA Spectrum 在接收到陷阱时会使用陷阱中的 varbind 信息来确定目标设备的 UID。
2. CA Spectrum 使用此 UID 来查找并定位与给定 UID 相关的 CA Spectrum 模型。将预先确定所有陷阱的实体类型。CA Spectrum 将根据查找结果按如下所示转发陷阱：
   - 如果它使用给定 UID 找到特定类型的 CA Spectrum 模型，CA Spectrum 会将事件和相应警报转发给目标模型。
   - 如果对于给定 UID 它找不到 CA Spectrum 模型，CA Spectrum 将在 Hyper-V Manager 模型上生成新的常规事件。此新事件包括有关陷阱的详细信息。

     注意：如果在 Hyper-V 虚拟化技术中更改虚拟网络实体之后立即发送陷阱，CA Spectrum 通常会找不到相关模型。Hyper-V 发现尚未在 CA Spectrum 中标识和创建相应的模型。

详细信息：

Virtual Host Manager 中支持的陷阱 (p. 161)

Virtual Host Manager 中支持的陷阱

CA Spectrum 中支持由 Hyper-V AIM 生成的所有陷阱。这些陷阱最初会发送给 Hyper-V Manager 模型。然后，根据陷阱类型，陷阱会被转发到相应的虚拟实体类型（即“目标”实体）。通过使用这些陷阱，您可以监控虚拟网络的性能，解决生成的所有警报或触发事件。

注意：有关 Hyper-V AIM 生成的陷阱的详细信息，请参阅《*CA Virtual Assurance for Infrastructure Managers 管理指南*》。

下表列出了特定目标实体类型的陷阱，并指定陷阱是否生成警报。

Hyper-V Manager 陷阱

陷阱名称	陷阱 OID	生成警报？
hypervAimStatVMAddTrap	1.3.6.1.4.1.546.1.1.6.16501	否
hypervAimStatVMRemoveTrap	1.3.6.1.4.1.546.1.1.6.16502	否
hypervAimStatVMMigrateTrap	1.3.6.1.4.1.546.1.1.6.16505	否

Hyper-V 虚拟机陷阱

陷阱名称	陷阱 OID	生成警报？
hypervAimStatVMEnabledTrap	1.3.6.1.4.1.546.1.1.6.16504	否

详细信息：

Virtual Host Manager 中的 Hyper-V 数据更新方式 (p. 150)
状态监控选项 (p. 154)
如何配置管理选项 (p. 155)
配置和监控资源状态 (p. 156)
CA Spectrum 如何从 CA SystemEDGE 转发陷阱 (p. 160)

用于虚拟网络的故障管理

故障隔离旨在缩小导致网络问题的根本原因的范围。通过查找根本原因，可以帮助您排除故障并快速更正问题，或使用自动化脚本以编程方式更正问题。确定哪些设备是导致警报的根本原因可能非常困难，因为单个设备中的问题会导致网络中的多个设备生成事件。

例如，与 Hyper-V 主机失去联系通常意味着也会与其管理的 Hyper-V 虚拟机失去联系。因此，Hyper-V 主机设备模型和所有受影响的虚拟机都将生成警报。通过使用故障隔离技术，Virtual Host Manager 将关联这些警报以尝试确定单个根本原因。

虚拟网络可提供独特的管理机会，因为它们针对 CA Spectrum 提供了备用管理视角。也就是说，CA Spectrum 可通过直接与您的虚拟设备联系或通过虚拟网络管理技术 Microsoft Hyper-V 来收集信息。这种备用管理视角可通过两种方式来增强标准 CA Spectrum 故障管理：

- **增强失去联系警报** - 两个设备信息源可帮助 Virtual Host Manager 查明原因，并更轻松地将事件与单个根本原因关联。
- **代理故障警报** - *代理管理*是指使用备用管理源（代替主要管理器或与主要管理器一起）来管理网络设备的行为。例如，CA Spectrum 可通过直接与虚拟网络设备联系或使用虚拟技术应用程序与设备联系来管理这些虚拟网络设备。当 Hyper-V 虚拟化技术与虚拟网络设备失去联系时，Virtual Host Manager 将为每个设备生成一个“失去代理管理”警报。这些警报具有唯一性，因为它们提醒您通过*代理*对设备执行的*管理*（而不是设备或直接 (SNMP) 管理的状态）受到影响。

丢失设备联系时故障隔离的工作方式

为了帮助您排除设备中的网络问题，CA Spectrum 使用故障隔离来缩小警报根本原因的范围。对于虚拟网络，Virtual Host Manager 将使用通过与设备直接联系获取的信息，以及由 Hyper-V 虚拟化技术通过 Hyper-V AIM 提供的信息。在许多情况下，标准 CA Spectrum 故障管理可以查明根本原因。但是在一些特殊情况下，无法使用标准方法来隔离虚拟网络中的问题。

Virtual Host Manager 用于发现根本原因的故障隔离类型取决于生成警报的设备，以及设备生成的事件类型。下列方案介绍了两种独特的故障管理情况，以及 CA Spectrum 如何确定虚拟网络中的网络错误。

方案 1：Hyper-V 虚拟机未运行

在虚拟环境中，与 CA Spectrum 通过标准设备监控发现的信息相比，虚拟管理应用程序可以提供更多的详细信息。例如，Hyper-V 虚拟化技术可发现 Hyper-V 虚拟机何时从“正在运行”状态更改为其他状态（如“未运行”）。

如果 Hyper-V 虚拟机不再运行，并且 CA Spectrum 与其失去了联系，但是 Hyper-V Manager 的代理管理 (请参阅本页中的定义 255)未中断，则 CA Spectrum 将按如下所示确定根本原因：

1. 当 CA Spectrum 与 Hyper-V 虚拟机失去联系时，将生成“失去联系”警报。
2. 在其下一个轮询周期内，Hyper-V Manager 模型将轮询 Hyper-V AIM 以收集有关虚拟机的信息。由于 Hyper-V 技术管理虚拟机，因此它可提供导致 Hyper-V 虚拟机所生成警报的可能原因的相关信息。
3. 如果 Hyper-V 虚拟化技术发现虚拟机处于未运行模式，它将生成“虚拟机未运行”警报。

   注意：在虚拟机重新运行后的第一个 Hyper-V AIM 轮询周期内，将清除此警报。
4. Virtual Host Manager 将“失去联系”警报与 CA Spectrum 所创建的相应“虚拟机未运行”警报关联。Virtual Host Manager 使“失去联系”警报显示为“虚拟机未运行”警报的症状。

方案 2：Hyper-V 主机关闭

如果 CA Spectrum 与已建模的 Hyper-V Manager 以及该主机上运行的所有 Hyper-V 虚拟机失去联系，它将检查上游路由器和交换机的状态。根据它们的状态，CA Spectrum 将按如下所示确定根本原因：

- 一个或多个虚拟机或 Hyper-V Manager 的所有上游设备都不可用 - 标准 CA Spectrum 故障隔离技术将按如下所示确定根本原因：
  - “设备已停止响应轮询”警报 - 当任何虚拟机或 Hyper-V Manager 的至少一个上游连接设备启动时在 Hyper-V 主机上生成。
  - “网关不可访问”警报 - 当*所有*上游连接设备都关闭时在 Hyper-V 主机上生成。
- 至少一个上游设备可用于连接到 Hyper-V 主机的每个虚拟机和 Hyper-V Manager - CA Spectrum 推断 Hyper-V 主机是根本原因，并按如下所示进行响应：

  a. 直接连接到 Hyper-V Manager 模型或虚拟机模型的 Hyper-V Manager 模型和所有 Hyper-V 虚拟机、端口及扇出将生成标准故障隔离警报。

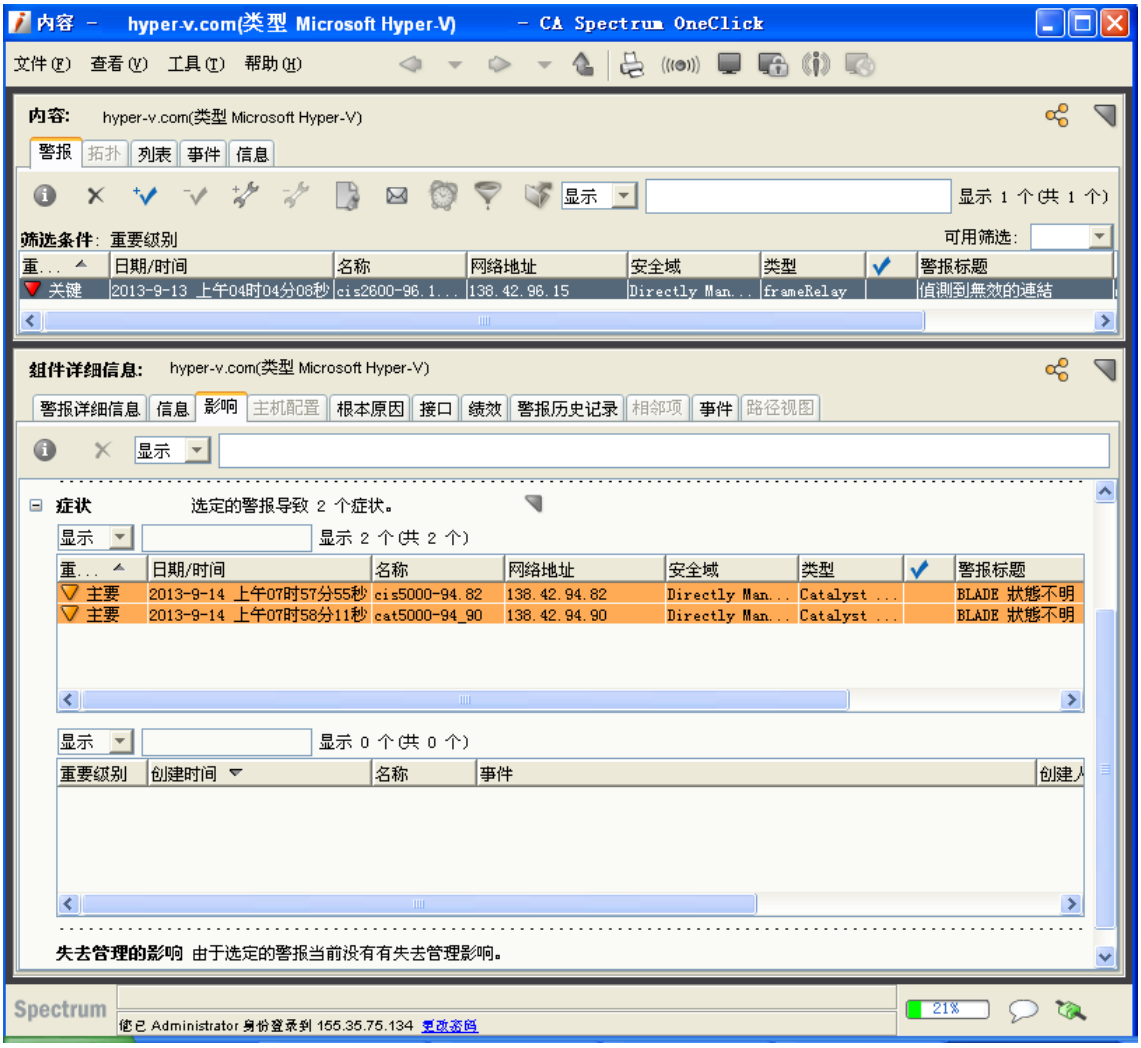
  b. Virtual Host Manager 为 Hyper-V 主机模型创建“物理主机关闭”警报。

  c. 为受影响设备（如虚拟机、端口和扇出）创建的所有故障隔离相关警报将关联到“物理主机关闭”警报，从而使它们成为“物理主机关闭”警报的症状。这些症状警报显示在“物理主机关闭”警报的“影响”选项卡上的“症状”表中。

     注意：对于每个 Hyper-V 主机模型，Virtual Host Manager 将创建一个“虚拟故障域”。此域中包括 Hyper-V 主机、Hyper-V Manager 和虚拟机，以及直接连接到 Hyper-V Manager 模型或虚拟机的所有端口和扇出。当 Hyper-V 主机生成“物理主机关闭”警报时，域中的所有标准故障隔离警报将与其关联。将这些警报作为症状关联可表明 Hyper-V 主机上的“物理主机关闭”警报是根本原因。

  d. “影响”选项卡上针对“物理主机关闭”警报的“失去管理的影响”表中列出了所有受影响设备。

注意：被抑制的设备在“症状”表中没有对应的警报。



e. 如果一个或多个虚拟机或 Hyper-V Manager 的所有上游设备都已关闭，则 CA Spectrum 无法再可靠地指出故障出自 Hyper-V 主机。因此，CA Spectrum 将清除“物理主机关闭”警报，并应用标准 CA Spectrum 故障隔离技术。

详细信息：

丢失代理管理时故障隔离的工作方式 (p. 166)
确定受 Hyper-V 主机停机影响的 Hyper-V 虚拟机 (p. 167)

丢失代理管理时故障隔离的工作方式

用于创建虚拟网络的 Microsoft Hyper-V 虚拟化技术为 CA Spectrum 提供了独特的管理机会。CA Spectrum 可以使用标准方法来直接联系您的虚拟设备，此外，CA Spectrum 可以同时从 Hyper-V 技术收集虚拟设备信息。从这个意义上讲，Hyper-V 技术是 CA Spectrum 可从其收集虚拟设备信息的“代理”。如果 CA Spectrum 与设备失去直接联系，则将生成警报。同样，如果 Hyper-V 技术与虚拟设备失去联系，或者如果 Virtual Host Manager 与 Hyper-V Manager 失去联系，Virtual Host Manager 将生成警报 -“失去代理管理”警报 (请参阅本页中的定义 255)。

作为响应，CA Spectrum 将尝试隔离导致代理管理故障的原因。代理故障隔离类似于标准 CA Spectrum 故障隔离，不过，这些警报将提醒您虚拟设备的*代理*管理会受到影响。代理管理故障隔离无法指明虚拟设备是已启动还是已关闭。但是，了解何时失去通过代理进行的联系非常重要，因为您可能会丢失设备的重要虚拟信息。

Virtual Host Manager 用于发现根本原因的代理故障隔离类型取决于生成警报的设备，以及设备生成的事件类型。下列方案介绍了一种独特的代理故障管理情况，以及 Virtual Host Manager 如何确定虚拟网络中的网络错误。

方案：CA Spectrum 与 Hyper-V Manager 之间失去联系

如果 CA Spectrum 与 Hyper-V Manager 模型失去联系或停止轮询该模型，则将丢失该 Hyper-V Manager 管理的所有虚拟模型的 Hyper-V 虚拟化技术数据。为了隔离该问题，Virtual Host Manager 将按如下所示确定根本原因：

1. CA Spectrum 将为该 Hyper-V Manager 管理的所有虚拟模型（包括虚拟机和 Hyper-V 主机）生成“代理已丢失”警报。CA Spectrum 还将在 Hyper-V Manager 模型上生成单独的“代理不可用”警报。
2. 虚拟机警报将与其相应的 Hyper-V 主机模型警报关联。
3. Hyper-V 主机模型警报将与 Hyper-V Manager 模型的“代理不可用”警报关联。
4. 然后，此“代理不可用”警报将与正关闭的 Hyper-V Manager 的根本原因关联。根本原因通常是由标准 CA Spectrum 故障管理生成的警报，例如为下列情况创建的警报：
   - 失去 Hyper-V Manager 的管理（即，Hyper-V Manager 主机上的 CA SystemEDGE 代理发生问题）
   - 失去计算机联系
   - Hyper-V Manager 模型处于维护模式

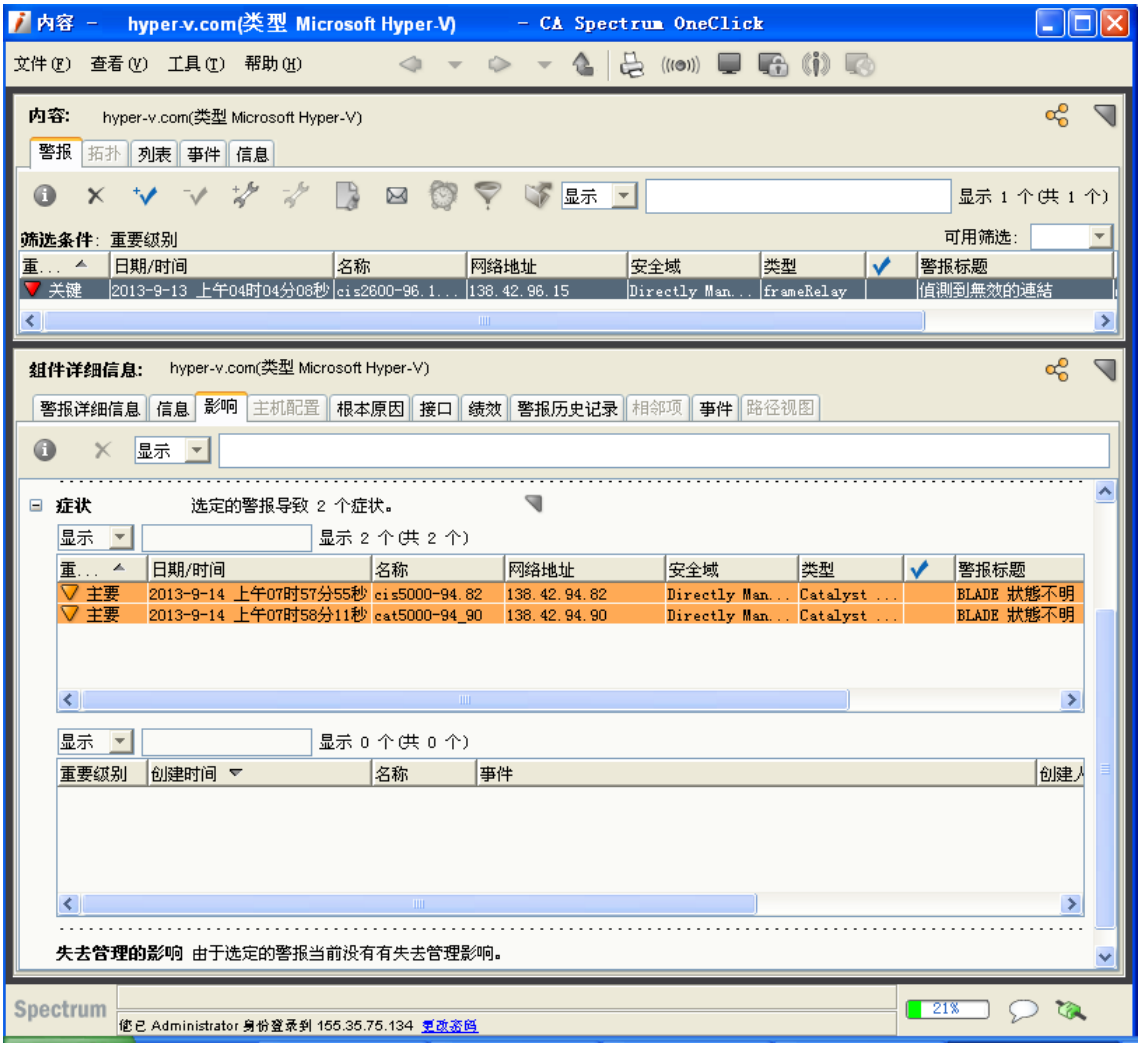
详细信息：

丢失设备联系时故障隔离的工作方式 (p. 162)

确定受 Hyper-V 主机停机影响的 Hyper-V 虚拟机

当与 Hyper-V 主机的联系中断或者 Hyper-V 主机关闭时，该 Hyper-V 主机承载的所有 Hyper-V 虚拟机都将受到影响。由于 Hyper-V 技术无法与 Hyper-V 主机进行通信以获取使用情况信息，因此您可能不会接收到该 Hyper-V 主机上关键虚拟机的警报。要确定关键虚拟机是否受到影响，可以在警报的“影响”选项卡上查看受影响虚拟机的列表，如下所示：

- “症状”子视图 - 显示受影响的 Hyper-V 虚拟机生成的所有症状警报
- “失去管理的影响”子视图 - 列出受警报影响的 Hyper-V 虚拟机



详细信息：

丢失设备联系时故障隔离的工作方式 (p. 162)

第 6 章： IBM LPAR

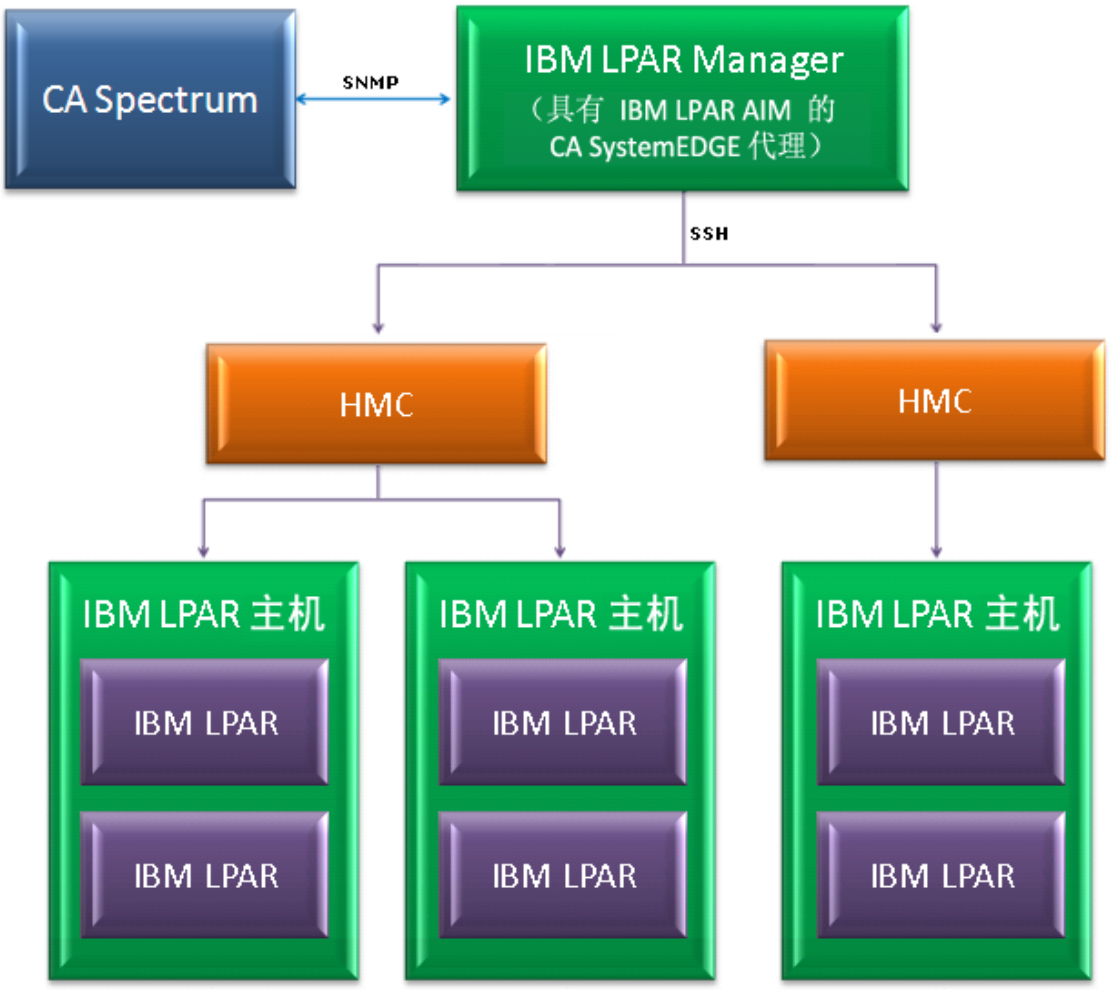
本节适用于 IBM LPAR 虚拟化技术用户，将介绍如何使用 Virtual Host Manager 来管理通过 IBM LPAR 技术创建的虚拟实体。

此部分包含以下主题：

Virtual Host Manager 如何使用 IBM LPAR

Virtual Host Manager 可以无缝监控您的虚拟网络实体和物理网络实体。您可以全面了解网络情况，并在网络中排除这两类实体的网络问题。虽然虚拟网络实体的行为与物理组件的行为类似，但是对这些实体的监控过程不同于一般 CA Spectrum 监控过程。了解此过程的工作原理可帮助您找到并解决与虚拟网络相关的网络问题。

Virtual Host Manager 中的 *IBM LPAR Manager* 是启用了 IBM LPAR AIM 的 CA SystemEDGE 代理。IBM LPAR Manager 负责报告所有已配置的 IBM LPAR。Virtual Host Manager 与 IBM LPAR Manager 进行通信，以收集有关 IBM LPAR 虚拟环境的详细信息。下图显示了 CA Spectrum 如何使用 IBM LPAR Manager 收集有关 IBM LPAR 虚拟环境的信息：



如图所示，收集有关 IBM LPAR 虚拟环境的信息的过程如下：

1. HMC (请参阅本页中的定义 256) 与其管理的每个 IBM LPAR 主机进行通信。
2. IBM LPAR Manager 使用 SSH 与其管理的每个 HMC 进行通信，以收集有关虚拟环境的详细信息。

   注意：仅监控具有 IBM LPAR AIM 的一个 IBM LPAR 主机实例。不要采用多个 HMC 来管理单个 IBM LPAR 主机。监控多个实例可能会导致 CA Spectrum 中出现重复模型。
3. CA Spectrum 定期与 IBM LPAR Manager 进行通信以检索这些详细信息。IBM LPAR Manager 已安装启用了 IBM LPAR AIM 的 CA SystemEDGE 代理。CA Spectrum 使用 SNMP 与 CA SystemEDGE 代理进行通信，并使用此信息在 CA Spectrum 中建模和监控虚拟环境。

详细信息：

Virtual Host Manager 的工作原理 (p. 11)
查看 IBM LPAR 虚拟网络 (p. 187)
Virtual Host Manager 中的 IBM LPAR 数据更新方式 (p. 189)

为 IBM LPARs 创建的模型

Virtual Host Manager 提供了多个模型来表示 IBM LPAR 虚拟技术网络的组件。通过了解以下基本模型，可以帮助您更好地了解发现以及虚拟环境与物理环境的连接方式。

Virtual Host Manager 包括用于 IBM LPAR 设备的以下模型和图标：

IBM LPAR Manager

表示包含已加载 IBM LPAR AIM 的 CA SystemEDGE 代理的服务器。

图标： 

IBM LPAR 主机

表示在 HMC (请参阅本页中的定义 256) 中配置的 IBM LPAR 主机。*IBM LPAR 主机*是使用 IBM LPAR 虚拟化软件承载 IBM LPAR 实例的物理计算机。IBM LPAR 主机可提供 IBM LPAR 使用的 CPU 和内存资源。它们还为这些 IBM LPAR 提供存储访问和网络连接。这些模型充当 Universe 拓扑中的容器模型，以帮助将虚拟实体分组到单独的视图中，同时显示虚拟环境与物理网络的连接情况。不能直接联系 IBM LPAR 主机以获取状态信息。而是将通过模型中所含项目的状态来推断这些模型的状态。

图标： 

IBM LPAR

表示在 HMC 中配置的 IBM LPAR。*IBM LPAR* 是在 IBM LPAR 主机上配置的逻辑分区实例，它能像物理计算机那样运行操作系统和应用程序。IBM LPAR 根据其工作负荷与配置动态消耗物理主机上的资源。

图标： 

详细信息：

查看 IBM LPAR 虚拟环境 (p. 187)

发现 IBM LPAR 网络

本节介绍 Virtual Host Manager 的发现和建模过程。这些任务通常由 Virtual Host Manager 管理员执行。

如何配置发现选项

在安装 Virtual Host Manager 后，可以配置 Virtual Host Manager 以执行 IBM LPAR 发现。通过配置首选项，可帮助确保 Virtual Host Manager 正确地为虚拟设备建模。

要为 IBM LPAR 发现配置 Virtual Host Manager 安装，请从下列选项中选择首选项：

- 新 IBM LPAR 的维护模式 (p. 173) - 允许您决定在可使用 CA Spectrum 来管理新发现的 IBM LPAR 实例之前将其中哪些实例置于维护模式。
- 允许在运行 IBM LPAR 发现期间删除设备模型 (p. 174) - 控制当 IBM LPAR 虚拟化技术模型不再受 Virtual Host Manager 管理时，CA Spectrum 如何处理它们。
- 搜索现有模型 (p. 175) - 确定在 IBM LPAR 发现期间 Virtual Host Manager 搜索的安全域。
- 发现支持 SNMP 的设备 (p. 177) - 控制如何在 IBM LPAR 发现期间为支持 SNMP 的设备建模。默认情况下，最初仅会将新模型创建为 VHM 模型。但是，此选项允许您覆盖默认设置，并为符合必要标准的设备立即创建 SNMP 模型。
- 执行 IBM LPAR Manager 删除期间保留启用了 SNMP 的 LPAR (p. 178) - 控制在删除 IBM LPAR Manager 模型时，CA Spectrum 如何处理启用了 SNMP 的 LPAR 模型。

为新 IBM LPAR 配置维护模式

Virtual Host Manager 会在 IBM LPAR 虚拟环境中自动为 IBM LPAR 实例建模。CA Spectrum 将尝试管理所有已发现的模型。但是，在最初建模某些新 IBM LPAR 时，它们尚未准备好由 CA Spectrum 管理。例如，未运行的 IBM LPAR 将导致 CA Spectrum 生成“失去联系”警报。为阻止在新 IBM LPAR 模型上生成不需要的警报，您可以决定将哪些新模型立即置于维护模式。之后，可以在准备好由 CA Spectrum 管理这些设备时手动禁用维护模式。

遵循这些步骤:

1. 在“导航”面板中打开 Virtual Host Manager (p. 109)。

   将在选定 Virtual Host Manager 的“内容”面板中打开详细信息页面。
2. 单击“信息”选项卡。
3. 展开“配置”、“IBM LPAR”、“IBM LPAR 发现”子视图。

4. 在“新 IBM LPAR 的维护模式”字段中单击“设置”，然后选择下列选项之一：

   将未启用的 LPAR 置于维护模式

   （默认）在初始 IBM LPAR 发现期间，仅向未启用的 IBM LPAR 模型应用维护模式。

   将所有 LPAR 置于维护模式

   在初始 IBM LPAR 发现期间，向所有新 IBM LPAR 模型应用维护模式。

   将保存您的设置，并且会根据您的选择将 Virtual Host Manager 创建的新 IBM LPAR 实例置于维护模式。

详细信息：

如何配置发现选项 (p. 173)
状态监控选项 (p. 193)

管理已从 IBM LPAR Manager 删除的设备的设备模型

虚拟环境中的设备及设备间的关联关系会频繁地发生更改。在 CA Spectrum 中维护有关虚拟环境的准确且及时的数据很具挑战性。例如，删除 IBM LPAR 主机或 IBM LPAR 实例时，CA Spectrum 知道要在“导航”面板中从 Virtual Host Manager 删除相应的设备模型。但是，CA Spectrum 是应保留还是删除模型？您可以选择设置以控制是否删除模型。

重要说明！删除模型时，这些模型上的所有注释或其他自定义也将丢失。如果以后可能会在 IBM LPAR 环境中重新创建模型，则可以禁用此选项。

遵循这些步骤:

1. 在“导航”面板中打开 Virtual Host Manager (p. 109)。

   将在选定 Virtual Host Manager 的“内容”面板中打开主详细信息页面。

2. 单击“信息”选项卡。
3. 展开“配置”、“IBM LPAR”、“IBM LPAR 发现”子视图。

4. 在“允许在运行 IBM LPAR 发现期间删除设备模型”字段中单击“设置”，然后选择下列选项之一：

   是

   （默认）删除不再受 IBM LPAR 环境管理的实体的对应 Virtual Host Manager 模型。

   否

   如果 Virtual Host Manager 模型的对应实体不再受 IBM LPAR 环境管理，则将这些模型放置在 LostFound 容器中。

   注意：将以不同的方式处理具有更多关联的模型（如全局集合中包括的模型）。将从 Universe 中删除这些模型，但是不会将其移动到 LostFound 容器中。

   将保存您的设置，并且会在从 IBM LPAR 环境中删除设备之后相应地处理设备模型。

详细信息：

如何配置发现选项 (p. 173)
删除 Virtual Host Manager 模型 (p. 200)
针对 IBM LPAR 的 Virtual Host Manager 警报 (p. 201)
Virtual Host Manager 中支持的陷阱 (p. 203)
删除 IBM LPAR Manager 后管理启用了 SNMP 的 LPAR 模型 (p. 178)

跨安全域配置模型搜索

IBM LPAR 发现将尝试查找 SpectroSERVER 中存在的模型，而不是创建新模型。在已部署 Secure Domain Manager 的环境中，IBM LPAR 发现将搜索与 IBM LPAR Manager 位于同一个安全域中的模型。此域是“本地”域。但是，某些虚拟环境设备可存在于不同的安全域中。在这种情况下，可以配置 IBM LPAR 发现以搜索所有安全域中的现有模型。

遵循这些步骤:

1. 在“导航”面板中打开 Virtual Host Manager (p. 46)。

   将在选定 Virtual Host Manager 的“内容”面板中打开主详细信息页面。

2. 单击“信息”选项卡。
3. 展开“配置”、“IBM LPAR”、“IBM LPAR 发现”子视图。

4. 在“搜索现有模型”字段中单击“设置”，然后从下列选项中进行选择：

   在 IBM LPAR Manager 的安全域中

   （默认）搜索与 IBM LPAR Manager 服务器位于同一个安全域中的现有模型。

   在所有安全域中

   搜索由 SpectroSERVER 管理的所有安全域中的现有模型。仅在下列情况下选择此选项：

   - 所有设备具有唯一的 IP 地址
   - 当安全域用于安全目的或用于隔离网络通信时

   注意：不要为 NAT 环境选择此选项。

   将保存您的设置，并且 IBM LPAR 发现会根据您的选择在 CA Spectrum 中搜索现有模型。当多个安全域中存在重复的模型（即共享相同 IP 地址的模型）时，Virtual Host Manager 将执行以下操作：

   - 在本地安全域中选择模型（如果有）。
   - 如果本地域中不存在重复的模型，Virtual Host Manager 将随机地从其他安全域中选择模型。
   - 在这两种情况下，Virtual Host Manager 将在 IBM LPAR Manager 模型上为重复的 IP 地址生成次要警报。

详细信息：

如何配置发现选项 (p. 173)

配置 SNMP 建模首选项

支持 SNMP 的设备可支持丰富的设备监控功能，如进程和文件系统监控功能。但是，部署 SNMP 代理可能会花费较高的经济和时间成本。默认情况下，IBM LPAR 发现将 IBM LPAR 实例创建为 VHM 模型 (请参阅本页中的定义 255)。可在以后将它们升级为 SNMP 模型。不过，也可以将 IBM LPAR 发现配置为将所有支持 SNMP 的新设备建模为 SNMP 模型。虽然完成 IBM LPAR 发现可能需要更长的时间，但是初始建模为 SNMP 模型可避免以后手动升级这些模型。

重要说明！在为 IBM LPAR 主机建模*之前*，请启用 SNMP 建模。如果首先为 IBM LPAR 主机建模，则会将所有子模型创建为 VHM 模型，并且必须手动将其升级为 SNMP 模型。

遵循这些步骤:

1. 在“导航”面板中打开 Virtual Host Manager (p. 46)。

   将在选定 Virtual Host Manager 的“内容”面板中打开主详细信息页面。

2. 单击“信息”选项卡。

3. 展开“配置”、“IBM LPAR”、“IBM LPAR 发现”、“SNMP 发现”子视图。

   重要说明！要准备设备和 CA Spectrum 以执行 SNMP 发现，请按照子视图中的步骤操作。如果在执行 IBM LPAR 发现之前未正确准备设备，Virtual Host Manager 将无法创建 SNMP 模型。

4. 在“发现支持 SNMP 的设备”字段中单击“设置”，然后从下列选项中进行选择：

   是

   在 IBM LPAR 发现期间启用 SNMP 建模。仅会将符合“SNMP 发现”子视图文本中指定标准的设备建模为 SNMP 设备。仅适用于*新*模型。

   否

   （默认）将 IBM LPAR 发现期间找到的所有新设备建模为 VHM 模型。可在以后手动将这些模型升级为 SNMP 模型。

   将保存您的设置，并且会根据您的选择在 Virtual Host Manager 中为新设备建模。

详细信息：

vCenter 发现的工作方式 (p. 41)
如何发现和建模虚拟环境 (p. 179)
向 VHM 模型中添加 SNMP 功能 (p. 183)
删除 IBM LPAR Manager 后管理启用了 SNMP 的 LPAR 模型 (p. 178)

删除 IBM LPAR Manager 后管理启用了 SNMP 的 LPAR 模型

默认情况下，删除以下项时，将从 CA Spectrum 中删除启用了 SNMP 的设备：

- 设备的 IBM LPAR Manager 模型
- “导航”面板中的 IBM LPAR 文件夹

启用了 SNMP 的设备模型可包括要保留的重要自定义。可以调整设置以避免删除这些模型。将它们放置在 LostFound 容器中供以后使用。

遵循这些步骤:

1. 在“导航”面板中打开 Virtual Host Manager (p. 46)。

   将在选定 Virtual Host Manager 的“内容”面板中打开主详细信息页面。

2. 单击“信息”选项卡。
3. 展开“配置”、“IBM LPAR”、“IBM LPAR 发现”子视图。
4. 在“在执行 IBM LPAR Manager 删除期间保留启用了 SNMP 的 LPAR”字段中单击“设置”，然后选择下列选项之一：

   是

   删除其 IBM LPAR Manager 或 IBM LPAR 文件夹时，将启用了 SNMP 的 LPAR 模型保留在 LostFound 容器中。

   注意：将以不同的方式处理具有更多关联的模型（如全局集合中包括的模型）。将从 Universe 中删除这些模型，但是不会将其移动到 LostFound 容器中。

   否

   （默认）删除其 IBM LPAR Manager 或 IBM LPAR 文件夹时，将删除所有 LPAR 模型。

   将保存您的设置，并且会在删除 IBM LPAR Manager 模型或 IBM LPAR 文件夹时相应地处理启用了 SNMP 的设备模型。

详细信息：

如何配置发现选项 (p. 173)
管理已从 IBM LPAR Manager 删除的设备的设备模型 (p. 174)
删除 Virtual Host Manager 模型 (p. 200)

如何发现和建模虚拟环境

要监控虚拟环境，必须发现并建模虚拟实体 - IBM LPAR 主机和 IBM LPAR 实例。通过在 Virtual Host Manager 中为这些实体建模，可以在一个工具中查看完整的网络拓扑，其中显示了物理组件和虚拟组件之间的关联关系。

为虚拟环境建模的主要步骤如下所示：

1. 运行标准的 CA Spectrum 发现 (p. 180)。

   此发现的目的是帮助确保在运行 IBM LPAR 发现之前为上游路由器和交换机建模。或者，如果已禁用“SNMP 建模”选项，则此步骤也可以为支持 SNMP 的 IBM LPAR Manager 建模。在为这些实体建模时，请确保正确设置建模选项以支持 Virtual Host Manager。

2. 升级 CA SystemEDGE 模型 (p. 181)。

   只有已在早于 CA Spectrum r9.2.1 的版本中为 IBM LPAR Manager 主机上的 CA SystemEDGE 代理建模后，才需要执行此步骤。

3. 允许运行 IBM LPAR 发现 (p. 182)。

   在 IBM LPAR Manager 主机上为带有 IBM LPAR AIM 的 CA SystemEDGE 代理建模时，将自动启动 IBM LPAR 发现。其中每个 IBM LPAR Manager 模型都具有自己的 IBM LPAR 发现进程。IBM LPAR 发现的目的是找到 IBM LPAR 环境中的虚拟实体，为不存在的实体建模，以及将它们放置在“导航”面板的 Virtual Host Manager 视图中。

详细信息：

向 VHM 模型中添加 SNMP 功能 (p. 183)
将 IBM LPAR 移至其他主机 (p. 186)
如何配置管理选项 (p. 194)
配置 SNMP 建模首选项 (p. 177)

运行 CA Spectrum 发现

要发现您的 IBM LPAR 环境，请运行标准 CA Spectrum 发现。此发现可确保为上游路由器和交换机建模，以便将来可以从虚拟实体建立连接。您还可以在 CA Spectrum 发现期间为支持 SNMP 的 IBM LPAR 主机和 IBM LPAR 实例建模。

注意：仅当在 IBM LPAR 发现期间禁用了“SNMP 建模”选项时，才需要在 CA Spectrum 发现期间为支持 SNMP 的 IBM LPAR 主机和 IBM LPAR 实例建模。

注意：只有管理员才可以执行此任务。

遵循这些步骤:

1. 打开发现控制台。

   注意：在建模之前，请确保您知道在非标准端口上运行的任何 SNMP 代理的正确团体字符串、IP 地址和端口号。

2. 在“导航”面板中单击  （新建配置）按钮。

3. 配置选项以支持虚拟网络建模，如下所示：

   a. 在“建模选项”组中单击“建模选项”按钮。

      此时将打开“建模配置”对话框。

   b. 单击“协议选项”按钮。

      此时将打开“协议选项”对话框。

   c. 选择“Pingable 项的 ARP 表”选项，然后单击“确定”。

      此时将打开“建模配置”对话框。

   d. （可选）在“高级选项”组中单击“高级选项”按钮，添加非标准 SNMP 端口（如 CA SystemEDGE 代理端口），然后单击“确定”。

4. 输入各个 IP 地址，或在“IP 边界列表”字段中输入开始 IP 地址和结束 IP 地址，然后单击“添加”。

   注意：确保 IP 地址范围中包括所有已安装 CA SystemEDGE 和 IBM LPAR AIM 的服务器以及互连交换机和路由器。或者，也可以包括需要 SNMP 模型的支持 SNMP 的 IBM LPAR 主机和 IBM LPAR 实例。

5. 在发现控制台中输入任何其他值，然后单击“发现”按钮。

   将创建以下模型，并会将其添加到 CA Spectrum 的网络拓扑中：

   - IBM LPAR Manager 以及用于将其连接到网络的交换机和路由器 - 有关虚拟环境的信息来自 IBM LPAR Manager。当 CA Spectrum 中存在这些 IBM LPAR Manager 模型时，IBM LPAR 发现即可启动。
   - IBM LPAR 实例 - 如果您决定不使用 CA Spectrum 发现为这些实体建模，则 IBM LPAR 发现会将它们创建为 VHM 模型 (请参阅本页中的定义 255)。

   注意：也可以通过 IP 地址手动为虚拟网络建模。在这种情况下，建议首先为上游设备建模。按正确顺序建模可确保在拓扑中正确生成这些实体之间的关联关系。有关如何执行发现的详细信息，请参阅《*IT 基础架构建模与管理 - 管理员指南*》。

详细信息：

向 VHM 模型中添加 SNMP 功能 (p. 183)
将 IBM LPAR 移至其他主机 (p. 186)
如何配置管理选项 (p. 194)
配置 SNMP 建模首选项 (p. 177)

升级 CA SystemEDGE 模型

在安装 Virtual Host Manager 之前或者在代理上加载 IBM LPAR AIM 之前，可能已在 CA Spectrum 中为 CA SystemEDGE 代理建模。在这种情况下，现有的 CA SystemEDGE 模型与 Virtual Host Manager 不兼容。升级该模型，以便 Virtual Host Manager 可以访问 CA SystemEDGE 中的 IBM LPAR AIM 功能。*如果在安装 CA Spectrum 之后加载并建模带有 IBM LPAR AIM 的 CA SystemEDGE 代理，则不需要执行此过程。*

要升级 CA SystemEDGE 模型，请右键单击该模型并依次选择“重新配置”、“重新配置模型”。

CA SystemEDGE 模型将升级，以支持 IBM LPAR AIM。

注意：也可以使用 CLI 向 CA SystemEDGE 发送重新配置模型操作。有关详细信息，请参阅《*IT 基础架构建模与管理 - 管理员指南*》。

详细信息：

向 VHM 模型中添加 SNMP 功能 (p. 183)
将 IBM LPAR 移至其他主机 (p. 186)
如何配置管理选项 (p. 194)

IBM LPAR 发现的工作方式

IBM LPAR 发现是专门用于收集有关虚拟环境的详细信息的发现进程。IBM LPAR 发现的目的是获取由 HMC (请参阅本页中的定义 256) 管理的虚拟实体，为 CA Spectrum 中不存在的实体建模，以及将它们放置在“导航”面板中的 Virtual Host Manager 下。

IBM LPAR 发现的主要优点是，它在后台自动运行，可使 CA Spectrum 中的虚拟环境数据保持更新。通过了解 IBM LPAR 发现的工作方式，可更有力地说明正确安装和建模各个 Virtual Host Manager 组件的重要性。

IBM LPAR 发现进程的工作方式如下：

1. 在配置 IBM LPAR Manager（已安装启用了 IBM LPAR AIM 的 CA SystemEDGE 代理）之后，IBM LPAR Manager 立即使用 SSH 来联系它监控的每个 HMC。IBM LPAR Manager 从 HMC 收集有关虚拟环境的信息并进行存储。

   注意：仅监控具有 IBM LPAR AIM 的一个 IBM LPAR 主机实例。不要采用多个 HMC 来管理单个 IBM LPAR 主机。监控多个实例可能会导致 CA Spectrum 中出现重复模型。

   重要说明！必须安装 CA SystemEDGE 代理和 IBM LPAR AIM，CA SystemEDGE、HMC 和 CA Spectrum 才能进行通信。如果它们无法通信，IBM LPAR 发现将无法运行。

2. 在 CA Spectrum 发现期间，CA Spectrum 将为步骤 1 中的每个 IBM LPAR Manager 创建一个模型，并允许 CA Spectrum 处理 CA Spectrum 和 CA SystemEDGE 代理之间的通信。

3. CA Spectrum 将轮询 IBM LPAR AIM，以收集在步骤 1 中存储的 IBM LPAR Manager 信息。

4. CA Spectrum 将启动 IBM LPAR 发现，并使用来自 AIM 的此信息在 CA Spectrum“拓扑”选项卡和“导航”面板的 Virtual Host Manager 层次结构中更新建模，如下所示：

   a. 如果在步骤 2 之前启用 SNMP 发现，则 Virtual Host Manager 发现将为符合 SNMP 发现标准的所有支持 SNMP 的新模型创建 SNMP 模型。

      注意：默认情况下，将在 IBM LPAR 发现期间禁用 SNMP 发现。

   b. 将为其余非 SNMP IBM LPAR 主机和 IBM LPAR 实例创建 VHM 模型 (请参阅本页中的定义 255)，如下所示：

      - 以前存在的 IBM LPAR 模型将更改为 VHM 模型。
      - 将为 CA Spectrum 中以前*不*存在的 IBM LPAR 实例创建 VHM 模型。

- 将为 IBM LPAR 主机模型创建 VHM 模型，这些模型将在“导航”面板的 Virtual Host Manager 下以及 Universe 拓扑中对其关联的 IBM LPAR 实例模型进行分组。

c. 虚拟网络的所有模型将添加到“导航”面板的 Virtual Host Manager 部分中。

注意：在虚拟环境中，不同 IBM LPAR 主机上的设备可具有相同的 IP 地址或 MAC 地址。在这种情况下，CA Spectrum 将为每个 IP 地址或 MAC 地址创建重复的模型。

5. IBM LPAR 发现将自动按每个定期排定的 IBM LPAR 技术轮询时间间隔重复该过程。

注意：默认情况下，通过在 IBM LPAR Manager 模型上设置轮询时间间隔来控制 IBM LPAR 轮询时间间隔。或者，也可以使用 IBM LPAR 虚拟化技术应用程序模型单独控制 IBM LPAR 轮询。

详细信息：

向 VHM 模型中添加 SNMP 功能 (p. 183)
将 IBM LPAR 移至其他主机 (p. 186)
如何配置管理选项 (p. 194)
控制 IBM LPAR AIM 轮询 (p. 198)
跨安全域配置模型搜索 (p. 175)

向 VHM 模型中添加 SNMP 功能

支持 SNMP 的设备可支持丰富的设备监控功能，如进程和文件系统监控功能。但是，部署 SNMP 代理可能会花费较高的经济和时间成本。当 SNMP 代理不可用或禁用了 SNMP 发现时，Virtual Host Manager 会将 IBM LPAR 创建为 VHM 模型 (请参阅本页中的定义 255)。

之后，您可以在任何 IBM LPAR 主机或 IBM LPAR 上安装 SNMP 代理，并在 CA Spectrum 中升级其建模。用于升级到 SNMP 模型的选项如下所示：

- **仅升级选定设备** - 当需要升级少量选定模型时，此方法可快速完成工作。将首先删除 VHM 模型。此方法的一个缺点是，在 CA Spectrum 删除模型之后，必须等待下一个 IBM LPAR 发现进程以创建 SNMP 模型，并将它们放置在 Virtual Host Manager 中。必须知道模型的 IP 地址才能进行升级。
- **升级所有支持 SNMP 的 VHM 模型** - 此方法可批量升级模型。在将 Virtual Host Manager 升级为新版本时，最好使用此方法。不必知道各个模型的 IP 地址。另一个优点是，在 CA Spectrum 删除 VHM 模型之后，会立即将升级后的 SNMP 模型放置在 Virtual Host Manager 层次结构中，而不必等待下一个轮询周期。因此，Virtual Host Manager 可更快地管理模型。此方法的缺点是可能需要很长时间才能完成。完成此升级所需的时间取决于在查找支持 SNMP 的设备时，Virtual Host Manager 必须搜索的团体字符串和 SNMP 端口的数量。

  注意： Virtual Host Manager 仅会尝试识别已启动的可 Ping 设备上的 SNMP 代理。

重要说明！删除模型时，这些模型上的所有注释或其他自定义也将丢失。

详细信息：

如何发现和建模虚拟环境 (p. 179)
删除 Virtual Host Manager 模型 (p. 200)
配置 SNMP 建模首选项 (p. 177)

将选定 VHM 模型升级为 SNMP 模型

当 SNMP 代理不可用或在 IBM LPAR 发现期间禁用了 SNMP 发现时，Virtual Host Manager 会将 IBM LPAR 实例创建为 VHM 模型 (请参阅本页中的定义 255)。之后，您可以在这些设备上安装 SNMP 代理，并在 CA Spectrum 中升级其建模。您必须知道 IP 地址才能升级设备模型。手动选择要升级的模型可快速完成，但这些模型上的所有说明或自定义将会在升级期间丢失。

遵循这些步骤:

1. 根据需要在设备上部署或启用 SNMP 代理。
2. 使用下列方法之一重新建模设备：
   - CA Spectrum 发现
   - 按 IP 地址为设备逐个建模

在创建支持 SNMP 的新模型时，CA Spectrum 将从 Virtual Host Manager 中移除以前的模型并将其删除。在下一个 IBM LPAR AIM 轮询周期中，CA Spectrum 将支持 SNMP 的模型添加到“导航”面板的 Virtual Host Manager 中。

重要说明！删除模型时，这些模型上的所有注释或其他自定义也将丢失。

详细信息：

管理已从 IBM LPAR Manager 删除的设备的设备模型 (p. 174)
如何发现和建模虚拟环境 (p. 179)
删除 Virtual Host Manager 模型 (p. 200)

将所有 VHM 模型升级为 SNMP 模型

当 SNMP 代理不可用或在 IBM LPAR 发现期间禁用了 SNMP 发现时，Virtual Host Manager 会将 IBM LPAR 实例创建为 VHM 模型 (请参阅本页中的定义 255)。之后，您可以在任何 IBM LPAR 上安装 SNMP 代理，并在 CA Spectrum 中升级其建模。在执行批量升级时，CA Spectrum 将搜索 VHM 模型，并查找现在作为支持 SNMP 的设备的模型。然后，CA Spectrum 将它们转换为 SNMP 模型。此方法可能需要很长的时间才能完成，具体取决于 Virtual Host Manager 必须搜索的团体字符串和端口的数量。

遵循这些步骤:

1. 根据需要在设备上部署或启用 SNMP 代理。
2. 在“导航”面板中打开 Virtual Host Manager (p. 46)。

   将在选定 Virtual Host Manager 的“内容”面板中打开主详细信息页面。
3. 在“导航”面板中选择用于管理要升级的模型的 IBM LPAR Manager 模型。
4. 单击“信息”选项卡。
5. 展开“IBM LPAR Manager”、“CA Spectrum 建模控制”子视图。
6. 单击“升级 ICMP 专用设备”按钮。

   重要说明！删除模型时，这些模型上的所有注释或其他自定义也将丢失。

   Virtual Host Manager 将搜索由选定 IBM LPAR Manager 设备上的 IBM LPAR AIM 管理的 VHM 模型。Virtual Host Manager 升级符合 SNMP 设备标准的 ICMP 专用设备，并将它们放置在 Virtual Host Manager 层次结构中。

将 IBM LPAR 移至其他主机

将 IBM LPAR 从一个 IBM LPAR 主机移至另一个 IBM LPAR 主机可能会导致数据丢失，具体取决于 Virtual Host Manager 和 HMC (请参阅本页中的定义 256) 中的配置设置。IBM LPAR AIM 不支持 IBM LPAR 迁移。对于 Virtual Host Manager，会将移动过程视为两个事件 - 在 HMC 中删除 IBM LPAR 以及创建新的 IBM LPAR。基于 Virtual Host Manager 配置，CA Spectrum 可以删除原始 IBM LPAR 模型并创建新模型。如果您已自定义原始模型，则删除它可能会导致数据丢失。如果在 HMC 中移动 IBM LPAR 之前正确配置 Virtual Host Manager 设置，则可以避免此数据丢失。

遵循这些步骤:

1. 将“允许在运行 IBM LPAR 发现期间删除设备模型”选项更改为“否” (p. 174)。

   注意：如果禁用此选项，则 CA Spectrum 不会从 CA Spectrum 中删除 IBM LPAR 模型，即使该模型已从 Virtual Host Manager 管理中移除。

2. 使用 HMC，从原始 IBM LPAR 主机中删除 IBM LPAR。
3. 等待 Virtual Host Manager 在“导航”面板中反映这些更改。

   CA Spectrum 会将 IBM LPAR 模型放置在 LostFound 容器中。

   重要说明！为了使 Virtual Host Manager 协调新的 IBM LPAR 与 LostFound 容器中的现有模型，在 HMC 中迁移 IBM LPAR 之后，IBM LPAR 名称、MAC 地址*和* IP 地址必须保持不变。如果其中任一值发生更改，则 Virtual Host Manager 无法使用现有模型。

4. 使用 HMC，将 IBM LPAR 添加到其他 IBM LPAR 主机。

   IBM LPAR 发现找到新的 IBM LPAR 时，Virtual Host Manager 将它与现有的模型进行协调，从 LostFound 容器中删除它，并将该模型置于 Virtual Host Manager 管理中。

5. （可选）在原始 IBM LPAR Manager 模型上将“允许在运行 IBM LPAR 发现期间删除设备模型”选项更改回“是”。

   IBM LPAR 将从一个 IBM LPAR 主机移至另一个 IBM LPAR 主机。

详细信息：

如何发现和建模虚拟环境 (p. 179)
运行 CA Spectrum 发现 (p. 180)
升级 CA SystemEDGE 模型 (p. 181)
IBM LPAR 发现的工作方式 (p. 182)
Virtual Host Manager 中的 IBM LPAR 数据更新方式 (p. 189)

查看 IBM LPAR 虚拟环境

本节介绍有关查看 IBM LPAR 虚拟环境和关联警报的概念。基本步骤与标准 CA Spectrum 步骤相同。但是，本节介绍仅适用于 IBM LPAR 虚拟技术的概念差异和详细信息。

查看 IBM LPAR 虚拟网络

在“资源管理器”选项卡上，Virtual Host Manager 节点显示了分层树结构，可帮助您可视化虚拟环境资源间的逻辑关联关系。

使用此信息，可以查看如何在 IBM LPAR Manager 中共享资源，从而帮助您发现机会以重新组织和优化虚拟环境。通过此层次结构，还可以快速监控资源性能以及排除其警报。

由于 Virtual Host Manager 无法识别 DSS 环境 (请参阅本页中的定义 255)，因此它位于格局层次结构中。以下示例显示了 Virtual Host Manager 在“导航”面板中“资源管理器”选项卡上的位置，并演示了虚拟环境的层次结构：

```
[-] SpectroSERVER 主机
    [+] Universe
    [-] Virtual Host Manager
        [-] IBM LPAR
            [+] IBM LPAR Manager 1
            [-] IBM LPAR Manager 2
                [-] IBM LPAR 主机 1
                     .  IBM LPAR 1
                     .  IBM LPAR 2
                [+] IBM LPAR 主机 2
                [+] IBM LPAR 主机 3
```

Virtual Host Manager 是由此 SpectroSERVER 管理的整个虚拟环境的根节点。在“导航”面板中选择此节点后，将在“内容”面板中显示 Virtual Host Manager 详细信息。您可以查看与虚拟环境相关的事件和警报等详细信息。

虚拟环境将直接在 Virtual Host Manager 下表示关联技术的文件夹中进行组织。在上面的示例层次结构中，IBM LPAR 文件夹包含使用 IBM LPAR 虚拟化技术创建的虚拟环境部分。在此文件夹中，Virtual Host Manager 列出了由此 SpectroSERVER 管理的所有 IBM LPAR Manager 主机。

每个 IBM LPAR Manager 仅包含它管理的虚拟环境部分。在“导航”面板中选择某个 IBM LPAR Manager 后，将在“内容”面板中显示相关详细信息，例如由选定 IBM LPAR Manager 管理的 IBM LPAR 主机或 IBM LPAR 实例。您还可以查看常规统计信息，以及有关未在 CA Spectrum 中建模的其他组件的相关详细信息，例如以下信息：

- 系统配置文件
- 配置文件
- 插槽
- 虚拟以太网设备
- 虚拟 SCSI 设备
- 虚拟串行设备
- 物理磁盘

在每个 IBM LPAR Manager 下，层次结构表示下列实体之间的逻辑关联关系：

- **IBM LPAR 主机**

  IBM LPAR 主机包含它管理的 IBM LPAR 实例。在“导航”面板中选择 IBM LPAR 主机后，将在“内容”面板中显示相关详细信息，例如与 IBM LPAR 主机相关的事件和警报以及 CPU 使用率。

- **IBM LPAR 实例**

  IBM LPAR 实例始终为 Virtual Host Manager 层次结构树中的叶节点。在“导航”面板中选择某个 IBM LPAR 后，将在“内容”面板中显示相关详细信息，包括事件和警报、内存使用率以及状态。

详细信息：

Virtual Host Manager 如何使用 IBM LPAR (p. 169)
为 IBM LPARs 创建的模型 (p. 171)
运行 CA Spectrum 发现 (p. 180)
虚拟实体类型的自定义子视图 (p. 191)
用于 IBM LPAR 搜索的定位器选项卡 (p. 192)

了解 IBM LPAR 虚拟拓扑

为虚拟环境创建的 IBM LPAR Manager、IBM LPAR 主机和 IBM LPAR 实例模型将集成到拓扑视图中。IBM LPAR 主机模型会自动分组其关联的 IBM LPAR 实例。拓扑将显示这些 IBM LPAR 如何连接到物理网络实体。

下列示例显示了这些模型在“导航”面板的“资源管理器”选项卡中 Universe 组下的显示方式：

```
[-] Universe
     .  物理交换机 1
     .  物理交换机 2
     .  IBM LPAR Manager
   [-] IBM LPAR 主机
        .  扇出 A
        .  扇出 B
        .  IBM LPAR A
        .  IBM LPAR B
        .  IBM LPAR C
```

选择这些模型之一后，将在“内容”面板的“拓扑”选项卡上以图形方式显示这些关联关系。

详细信息：

为 IBM LPARs 创建的模型 (p. 171)
Virtual Host Manager 中的 IBM LPAR 数据更新方式 (p. 189)
用于 IBM LPAR 搜索的定位器选项卡 (p. 192)

Virtual Host Manager 中的 IBM LPAR 数据更新方式

在初始 IBM LPAR 发现期间，CA Spectrum 将使用您的虚拟设备模型填充“导航”面板中的 Virtual Host Manager 层次结构。在 CA Spectrum 构建此初始层次结构后，您的虚拟网络配置可能会发生更改，Virtual Host Manager 必须持续工作以保持此信息在 CA Spectrum 中的准确性。例如，以下事件可能会更改虚拟网络配置：

- 在 IBM LPAR 主机上创建或删除 IBM LPAR
- 将 IBM LPAR 从一个 IBM LPAR 主机移至另一个 IBM LPAR 主机

为了保持信息准确，Virtual Host Manager 通过轮询 IBM LPAR AIM 来检测这些更改。因此，将于每个轮询周期在 CA Spectrum 中更新您的虚拟网络配置。CA Spectrum 还会从 AIM 接收陷阱，并生成相应的事件。通过查看事件日志，可以查明配置发生更改的时间（例如创建新 IBM LPAR 的时间）。

在删除 IBM LPAR 时，CA Spectrum 将从“导航”面板的 Virtual Host Manager 层次结构中删除模型。当 AIM 检测到向您的虚拟网络配置中添加了内容时（如配置新 IBM LPAR 或将某个 IBM LPAR 置于管理中时），CA Spectrum 将执行以下任务：

- 在“导航”面板的 Virtual Host Manager 层次结构中，更新虚拟设备模型的放置
- *自动*重新发现与受影响的 IBM LPAR 模型的连接，并将它们与 Universe 拓扑中的正确 IBM LPAR 主机关联。

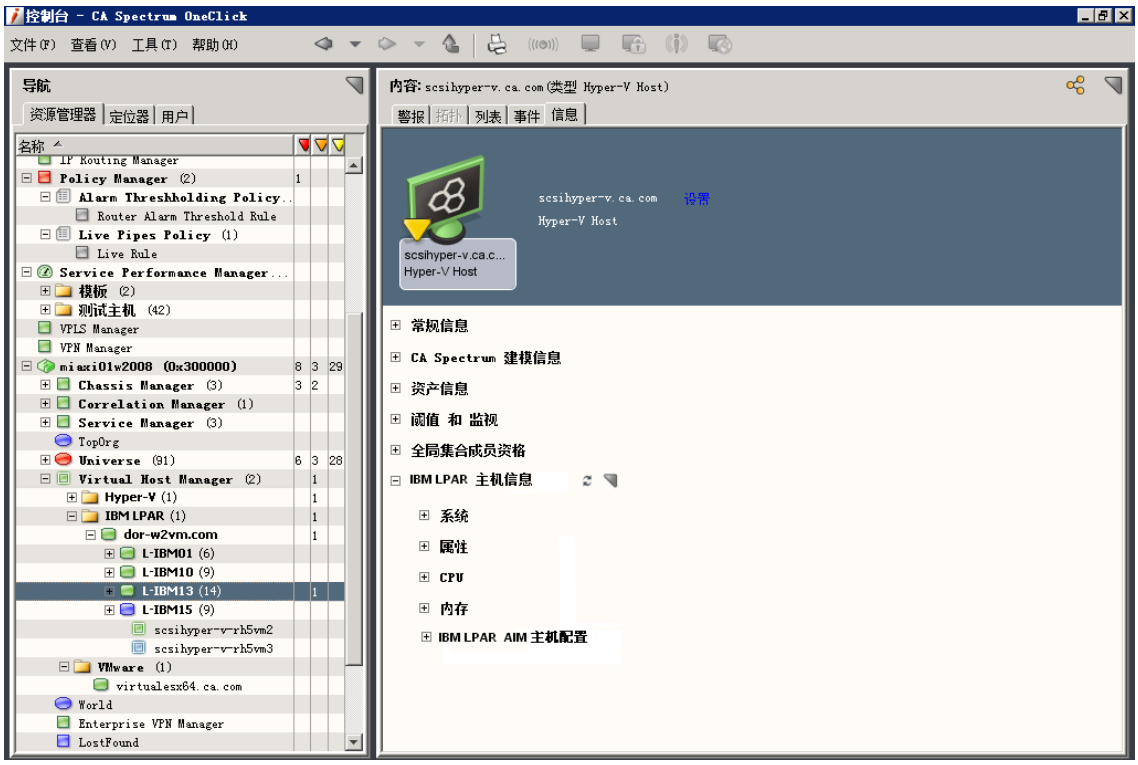
  重要说明！要正确重建与虚拟模型的连接，必须为物理网络中的所有互连路由器和交换机建模。如果在重新发现与虚拟设备的连接之前这些模型不存在，则 CA Spectrum 无法在 Universe 拓扑视图中解析这些连接并正确显示相关信息。IBM LPAR 主机将与 CA SystemEDGE 模型放置在同一个 LAN 容器中。

详细信息：

Virtual Host Manager 的工作原理 (p. 11)
为 IBM LPARs 创建的模型 (p. 171)
管理已从 IBM LPAR Manager 删除的设备的设备模型 (p. 174)
将 IBM LPAR 移至其他主机 (p. 186)
查看 IBM LPAR 虚拟网络 (p. 187)
配置和监控资源状态 (p. 197)

虚拟实体类型的自定义子视图

您的各个 Virtual Host Manager 模型将共同提供有关虚拟环境的信息。每个模型将单独提供特定的信息或配置设置，具体取决于其表示的虚拟实体类型。此自定义子视图显示在“内容”面板的“信息”选项卡上。这些子视图可包含实时数据（如 CPU 状态或内存利用率），并提供了对阈值设置的访问。例如，针对 IBM LPAR 主机的自定义子视图是“IBM LPAR 主机信息”子视图，如下所示：



注意：IBM LPAR Manager 模型提供由 IBM LPAR Manager 管理的所有虚拟设备的组合信息。也就是说，在“导航”面板中选择 IBM LPAR Manager 模型，可显示有关选定 IBM LPAR Manager 主机的信息，*以及*有关所有 IBM LPAR 主机、IBM LPAR 实例、系统配置文件、虚拟以太网设备等的组合信息。此信息包含在每个单独实体模型的“信息”选项卡上显示的相同数据。IBM LPAR Manager 模型中的组合视图可以很好地概述它管理的所有虚拟实体。

详细信息：

查看 IBM LPAR 虚拟网络 (p. 187)
配置和监控资源状态 (p. 197)

用于 IBM LPAR 搜索的定位器选项卡

除了在“资源管理器”选项卡上查看有关虚拟环境的详细信息外，还可以使用“定位器”选项卡运行预配置的 Virtual Host Manager 搜索。搜索选项在“定位器”选项卡中的“虚拟主机管理”->“IBM LPAR”文件夹下进行分组，如下所示：

这些详细搜索可以帮助您调查仅与虚拟实体相关的信息，例如查找格局中的所有 IBM LPAR 实例。

注意：虽然 Virtual Host Manager 无法识别 DSS (请参阅本页中的定义 255)，但是这些预配置搜索允许您在搜索参数中选择多个要搜索的格局。

“导航”面板的“定位器”选项卡中包含针对 Virtual Host Manager 信息的以下搜索：

所有 IBM LPAR 主机

在 CA Spectrum 数据库中查找已为虚拟网络建模的所有 IBM LPAR 主机。

所有 IBM LPAR

在 CA Spectrum 数据库中查找已为虚拟网络建模的所有 IBM LPAR 实例。

LPAR - 按 IBM LPAR 主机名

在 CA Spectrum 数据库中查找已为虚拟网络建模的所有 IBM LPAR 实例，仅限于由选定 IBM LPAR 主机管理的 IBM LPAR。

详细信息：

查看 IBM LPAR 虚拟网络 (p. 187)

状态监控选项

CA Spectrum 提供了多种用于监控虚拟网络资源状态的选项。为资源提供的状态信息将有所不同，具体取决于您监控的虚拟实体的类型。此外，您是否能够配置状态选项取决于其类型。例如，一些状态选项是只读选项，而另外一些状态选项则允许您配置阈值、启用行为或选择警报重要级别。通过提供此系列选项和自定义级别，CA Spectrum 允许您决定如何以最佳方式监控虚拟网络的性能。

状态字段位于 OneClick 子视图中。IBM LPAR Manager 模型上以表格格式提供了给定虚拟环境的所有状态信息。此外，在 CA Spectrum 中具有唯一模型的每个虚拟实体类型将提供相同状态信息的子集，以便于查看。可以从任一视图位置设置与状态相关的设置，包括报警类型、监控器和阈值。

下表概述了为每个虚拟实体类型提供的状态信息的类型。“子视图位置”列介绍了相应状态字段在 OneClick 中的位置。例如，在“信息”选项卡上的以下两个位置中提供了 IBM LPAR 模型的“内存”信息：

- IBM LPAR 模型的“IBM LPAR 信息”->“内存”子视图
- IBM LPAR Manager 模型的“IBM LPAR Manager”->“管理的环境”->“LPAR”子视图

要浏览可用于每个状态信息类型的确切状态选项，请在 OneClick 中查找子视图。

IBM LPAR 主机

状态信息类型	子视图位置
总体状态	IBM LPAR 主机、IBM LPAR Manager
CPU	IBM LPAR 主机、IBM LPAR Manager

IBM LPAR

状态信息类型	子视图位置
系统	IBM LPAR、IBM LPAR Manager
CPU	IBM LPAR、IBM LPAR Manager
内存	IBM LPAR、IBM LPAR Manager

详细信息：

配置和监控资源状态 (p. 197)
针对 IBM LPAR 的 Virtual Host Manager 警报 (p. 201)
Virtual Host Manager 中支持的陷阱 (p. 203)

如何配置管理选项

在为虚拟网络建模之后，可以配置 Virtual Host Manager 选项以查看和管理设备模型。通过配置首选项，可帮助确保 Virtual Host Manager 正确处理虚拟设备模型，并仅监控您需要的重要信息。

要配置 Virtual Host Manager 安装，请在发现并建模虚拟网络之后执行以下过程：

- 配置 IBM LPAR AIM 选项 (p. 195) - 这些选项允许您选择 CA SystemEDGE IBM LPAR AIM 的各种设置，如 AIM 轮询时间间隔和各种陷阱。
- 配置阈值和其他状态监控选项 (p. 197)- 这些选项允许您确定要监控的信息，以及 CA Spectrum 如何管理虚拟环境中发生的各种事件。

详细信息：

升级 CA SystemEDGE 模型 (p. 181)
Virtual Host Manager 中的 IBM LPAR 数据更新方式 (p. 189)

配置 IBM LPAR AIM

IBM LPAR AIM 与 IBM LPAR Manager 进行通信，以管理和收集有关虚拟环境的信息。在 Virtual Host Manager 中，可以配置 AIM 以确定它对轮询、陷阱和事件的处理方式。IBM LPAR AIM 配置设置可以帮助您正确平衡要收集的信息与所需的资源量。

遵循这些步骤:

1. 在“导航”面板中打开 Virtual Host Manager (p. 109)。

   将在选定 Virtual Host Manager 的“内容”面板中打开主详细信息页面。

2. 在“导航”面板的“资源管理器”选项卡上找到并单击 IBM LPAR Manager。

   “内容”面板上的各个选项卡中将填充有 IBM LPAR Manager 的相关详细信息。

3. 单击“信息”选项卡。

4. 展开“IBM LPAR Manager”、“IBM LPAR AIM”、“配置”子视图。

5. 根据需要，单击“设置”更改以下字段的设置：

   轮询时间间隔(秒)

   指定 IBM LPAR AIM 在已配置的 IBM LPAR 主机中轮询和缓存状态与建模信息的时间间隔（以秒为单位）。此轮询将检索状态和建模更新，如 IBM LPAR 未运行状态、IBM LPAR 主机已断开连接、新的 IBM LPAR 可用、新的 IBM LPAR 主机等。

   默认值： 300

   限制： 值大于或等于 300。

   注意： 为获得最佳结果，建议将此时间间隔设置为低于 CA Spectrum 轮询周期时间间隔。

   日志级别

   指定写入 IBM LPAR AIM 日志文件的信息的级别。这些级别可累积（例如，日志级别 4 将写入从级别 0 到 4 的所有消息）。日志级别如下所示：

   - 0：致命
   - 1：关键
   - 2：警告
   - 3：信息
   - 4：调试

- 5：调试（低）
- 6：调试（更低）
- 7：调试（最低）

默认值：2

注意：建议不要将调试级别指定为大于 4。

最大事件数

指定要在“事件”表中存储的最大事件数。达到最大行数时，CA Spectrum 从最早的已记录事件开始覆盖事件行。

默认值：500

限制：1–2147483647

历史记录(天)

指定在“事件”表中提供的历史记录信息量（以天为单位）。超过指定天数的事件将从“事件”表中清除。

注意：“最大事件数”字段中的值也影响此设置。达到最大数时，“事件”表无法始终存储跨越在“历史记录(天)”字段中指定的天数的事件。例如，在过去 30 天内发生了 800 个事件。在过去 10 天内发生了最近的 500 个事件。如果“最大事件数”字段指定 500，则在“事件”表中仅提供 10 天的历史记录。

默认值：30

限制：1–365

清除事件

确定是否从“事件”表中清除事件。从以下选项中进行选择：

不清除

（默认）在达到“最大事件数”或“历史记录(天)”值之前，保留“事件”表中的所有事件。

清除

启动 IBM LPAR AIM 时，从“事件”表中清除所有事件。

将使用您的选择配置 IBM LPAR AIM。

详细信息：

如何配置管理选项 (p. 194)

配置和监控资源状态

可以在 OneClick 中监控虚拟资源的状态。例如，可以查看总内存、已用内存、CPU 使用率百分比等。此外，还可以设置监控选项，例如，启用警报以及设置陷阱阈值。此信息可以帮助您优化虚拟网络性能以及排除警报故障。

注意：将在 IBM LPAR AIM 上设置陷阱，并由其来管理它们，但是您可以从 OneClick 子视图中配置这些阈值。在更改任何阈值或设置时，需要使用读取/写入团体字符串。

可以在“信息”选项卡上查看或配置虚拟设备的资源状态选项和信息。

遵循这些步骤:

1. 在“导航”面板中打开 Virtual Host Manager (p. 109)。

   将在选定 Virtual Host Manager 的“内容”面板中打开主详细信息页面。

2. 在“导航”面板的“资源管理器”选项卡上找到并单击虚拟设备。

   将在“内容”面板中显示设备的详细信息。

3. 单击“信息”选项卡。

   可查看多个子视图。通常，该选项卡底部的子视图中包括选定模型的资源分配和利用率信息。例如，IBM LPAR 主机模型将显示一个名为“IBM LPAR 主机信息”的子视图，其中包括您在“导航”面板中选择的特定模型的详细信息。

4. 展开相应的子视图。

   将显示选定设备模型的所有可用资源状态详细信息和监控选项。

   注意：IBM LPAR Manager 模型提供由 IBM LPAR Manager 管理的所有虚拟设备的组合信息。也就是说，在“导航”面板中选择 IBM LPAR Manager 模型，可显示有关选定 IBM LPAR Manager 主机的信息，*以及*有关所有 IBM LPAR 主机、IBM LPAR 实例、系统配置文件、虚拟以太网设备等的组合信息。此信息包含在每个单独实体模型的“信息”选项卡上显示的相同数据。IBM LPAR Manager 模型中的组合视图可以很好地概述它管理的所有虚拟实体。

详细信息：

虚拟实体类型的自定义子视图 (p. 191)
状态监控选项 (p. 193)
如何配置管理选项 (p. 194)
针对 IBM LPAR 的 Virtual Host Manager 警报 (p. 201)

控制 IBM LPAR AIM 轮询

在调整 Virtual Host Manager 性能时，可以更改 IBM LPAR Manager 轮询速率，或禁用 IBM LPAR 技术轮询。默认情况下，IBM LPAR Manager 模型上的轮询属性用于控制 IBM LPAR 相关的轮询行为。或者，也可以单独更改此 IBM LPAR 相关的轮询行为。IBM LPAR 虚拟技术应用程序模型 IBMLPARAIMApp 用于控制 IBM LPAR 相关轮询。

此应用程序上的以下两个属性值专门用于控制 IBM LPAR 技术轮询逻辑：

- PollingStatus
- Polling_Interval

IBM LPAR Manager 设备模型和 IBMLPARAIMApp 应用程序模型都包含这些属性。PollingStatus 用于禁用和启用轮询，而 Polling_Interval 用于控制轮询频率。如果这些模型的值不同，则优先考虑 IBMLPARAIMApp 应用程序模型属性值。

通过为设备模型和应用程序模型设置值，您可以微调 IBM LPAR 的相关轮询。对于 PollingStatus 和 Polling_Interval，修改 IBM LPAR Manager 设备模型上的属性时还将更改相应的应用程序模型属性（如果它们的值相同）。

详细信息：

IBM LPAR 发现的工作方式 (p. 182)

配置 IBM LPAR 轮询时间间隔

您可以更改 IBM LPAR AIM 轮询速率。可通过设置 IBM LPAR 虚拟技术应用程序模型上的 Polling_Interval 属性来配置轮询时间间隔。

遵循这些步骤:

1. 打开 OneClick，并单击“导航”面板中的“定位器”选项卡。
2. 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。
3. 在“设备 IP 地址”字段中输入 IBM LPAR Manager 的 IP 地址，然后单击“确定”。

   将在“内容”面板中显示 IBM LPAR Manager 的应用程序模型的列表。

4. 选择 IBMLPARAIMApp 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. 单击“组件详细信息”面板中的“信息”选项卡。

6. 单击“建模信息”子视图。

7. 在“轮询时间间隔(秒)”字段中单击“设置”，然后输入新值。

   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 IBM LPAR AIM 轮询。但是，如果将“轮询时间间隔(秒)”设置为 0，并将“轮询”字段设置为“打开”，IBM LPAR AIM 轮询将按照为 IBM LPAR Manager 设备设置的轮询时间间隔继续运行。

   IBM LPAR AIM 轮询时间间隔设置即已配置。

禁用 IBM LPAR 轮询

可以禁用 IBM LPAR AIM 轮询。禁用 IBM LPAR 轮询的过程与禁用 Virtual Host Manager 的过程相同。可以通过在 IBM LPAR 虚拟技术应用程序模型上设置 PollingStatus 属性来禁用轮询。

遵循这些步骤:

1. 打开 OneClick，并单击“导航”面板中的“定位器”选项卡。

2. 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。

3. 在“设备 IP 地址”字段中输入 IBM LPAR Manager 的 IP 地址，然后单击“确定”。

   将在“内容”面板中显示 IBM LPAR Manager 的应用程序模型的列表。

4. 选择 IBMLPARAIMApp 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. 单击“组件详细信息”面板中的“信息”选项卡。

6. 单击 CA Spectrum 的“建模信息”子视图。

7. 单击“轮询”字段中的“设置”，然后选择“关闭”。

   将在选定的 IBM LPAR Manager 上为 IBM LPAR AIM 禁用轮询。

删除 Virtual Host Manager 模型

可以随时出于各种原因从 OneClick 中删除模型。但是，Virtual Host Manager 会限制您在“导航”面板的 Virtual Host Manager 层次结构中删除模型的能力。要手动删除模型，有以下两个选项可用：

- 在 Virtual Host Manager 中删除 IBM LPAR 文件夹或 IBM LPAR Manager 模型
- 使用 HMC (请参阅本页中的定义 256) 删除虚拟实体

在 Virtual Host Manager 中，有时会自动删除模型。下列情况会导致 CA Spectrum 自动删除 Virtual Host Manager 模型：

- **已删除 IBM LPAR 文件夹，或者已从 Virtual Host Manager 中删除 IBM LPAR Manager 模型**

  如果删除 IBM LPAR Manager 模型，或从“导航”面板中删除 IBM LPAR 文件夹，CA Spectrum 将会删除所有相关的子模型。

- **已从 IBM LPAR 虚拟环境中删除实体**

  使用 HMC 删除 IBM LPAR 主机和 IBM LPAR 实例时，CA Spectrum 还会从 Virtual Host Manager 中删除这些模型及其子模型。

- **存在已升级模型** - 在某些情况下，会首先为无 SNMP 功能的 Virtual Host Manager 建模 IBM LPAR 实例。如果以后向 VHM 模型 (请参阅本页中的定义 255)添加 SNMP 功能，则之前的模型将被删除，并替换为支持 SNMP 的新模型。

注意：虽然默认设置是删除模型，但是您可以配置 Virtual Host Manager，以便在从 Virtual Host Manager 中删除 IBM LPAR 主机和 IBM LPAR 实例时将它们放置在 LostFound 容器中。仅当使用 HMC 删除设备时，才会应用此配置设置。但是，在删除 IBM LPAR 文件夹、删除 IBM LPAR Manager 模型或升级 VHM 模型时，不会应用此设置。

详细信息：

管理已从 IBM LPAR Manager 删除的设备的设备模型 (p. 174)
向 VHM 模型中添加 SNMP 功能 (p. 183)
删除 IBM LPAR Manager 后管理启用了 SNMP 的 LPAR 模型 (p. 178)

IBM LPAR 的警报和故障隔离

本节介绍 Virtual Host Manager 所使用的陷阱以及生成的警报。本节还说明 Virtual Host Manager 故障隔离与基础 CA Spectrum 故障隔离有何差异。

针对 IBM LPAR 的 Virtual Host Manager 警报

为了就虚拟网络中出现的问题向您报警，CA Spectrum 将生成警报。将以两种方式创建警报：

- 从 CA SystemEDGE 代理发送的陷阱
- 轮询

通过轮询可生成四个警报：“IBM LPAR 代理已丢失”、“IBM LPAR 主机代理已丢失”、“IBM LPAR Manager 不可用”和“IBM LPAR 未运行”。但是，有几个陷阱可以在虚拟设备上生成警报。CA Spectrum 支持 IBM LPAR AIM 从 CA SystemEDGE 代理发送的所有陷阱。要在监控设备时从这些陷阱获取最大价值，可以单独为每个虚拟设备配置阈值。

如果某个陷阱违反阈值并生成警报，CA Spectrum 将使用通过陷阱传递的“状态”varbind 的值来确定警报重要级别。所有状态 varbind 具有以下可能的值（CA Spectrum 以相同的方式发出警报）：

- 0：未知
- 1：正常
- 2：警告
- 3：关键

“未知”状态没有关联的警报重要级别，且不会更改设备的警报重要级别。CA Spectrum 将其他 IBM LPAR 技术状态映射到 CA Spectrum 警报重要级别：

IBM LPAR 状态	CA Spectrum 警报重要级别
1：正常	正常（绿色）
2：警告	次要（黄色）
3：关键	主要（橙色）

详细信息：

管理已从 IBM LPAR Manager 删除的设备的设备模型 (p. 174)
状态监控选项 (p. 193)
配置和监控资源状态 (p. 197)
删除 IBM LPAR Manager 后管理启用了 SNMP 的 LPAR 模型 (p. 178)

CA Spectrum 如何从 CA SystemEDGE 转发陷阱

CA Spectrum 支持由 IBM LPAR AIM 发送的所有陷阱。最初会将这些陷阱发送给 IBM LPAR CA SystemEDGE 模型。如果陷阱的目标不是此模型，则 CA Spectrum 会将陷阱转发给正确的虚拟模型。

注意：对于与陷阱相关的特定事件代码，请使用事件配置应用程序并针对“0x056e”进行筛选。或者，可以启动 MIB 工具以便在“EMPIRE-CALPARA-MIB”MIB 的“陷阱支持”表中查看陷阱。有关使用事件配置应用程序的详细信息，请参阅《*事件配置用户指南*》。有关使用 MIB 工具的详细信息，请参阅《*IT 基础架构建模与管理 - 管理员指南*》。

CA Spectrum 使用以下过程确定要将陷阱转发到的位置：

1. CA Spectrum 在接收到陷阱时会使用陷阱中的 varbind 信息来查找正确的虚拟实体，如下所示：
   - 对于转发到 IBM LPAR 主机的陷阱，CA Spectrum 将使用 UID 来查找正确的主机。
   - 对于转发到 IBM LPAR 实例的陷阱，CA Spectrum 将使用 UID 来首先确定正确的 IBM LPAR 主机。基于 UID 或 IBM LPAR 名称，CA Spectrum 在此 IBM LPAR 主机管理的 IBM LPAR 列表中查找正确的 IBM LPAR 实例。
2. CA Spectrum 使用此 UID 来查找并定位与给定 UID 相关的 CA Spectrum 模型。将预先确定所有陷阱的实体类型。CA Spectrum 将根据查找结果按如下所示转发陷阱：
   - 如果它使用给定 UID 和（在某些情况下）IBM LPAR 名称找到特定类型的 CA Spectrum 模型，CA Spectrum 会将事件和相应警报转发给目标模型。
   - 如果对于给定 UID 和（在某些情况下）IBM LPAR 名称它找不到 CA Spectrum 模型，CA Spectrum 将在 IBM LPAR Manager 模型上生成新的常规事件。此新事件包括有关陷阱的详细信息。

     注意：如果在 HMC (请参阅本页中的定义 256) 中更改虚拟网络实体之后立即发送陷阱，CA Spectrum 通常会找不到相关模型。IBM LPAR 发现尚未在 CA Spectrum 中标识和创建相应的模型。

详细信息：

Virtual Host Manager 中支持的陷阱 (p. 203)

Virtual Host Manager 中支持的陷阱

CA Spectrum 中支持由 IBM LPAR AIM 生成的所有陷阱。这些陷阱最初会发送给 IBM LPAR Manager 模型。然后，根据陷阱类型，陷阱会被转发到相应的虚拟实体类型（即“目标”实体）。通过使用这些陷阱，您可以监控虚拟网络的性能，解决生成的所有警报或触发事件。

注意：有关 IBM LPAR AIM 生成的陷阱的详细信息，请参阅《*CA Virtual Assurance for Infrastructure Managers 实施指南*》。

下表列出了特定目标实体类型的陷阱，并指定陷阱是否生成警报。

IBM LPAR Manager 陷阱

陷阱名称	陷阱 OID	生成警报？
lparAimSysAdded	1.3.6.1.4.1.546.1.1.0.165317	否
lparAimSysRemove	1.3.6.1.4.1.546.1.1.0.165316	否

IBM LPAR 主机陷阱

陷阱名称	陷阱 OID	生成警报？
lparAimLPAdded	1.3.6.1.4.1.546.1.1.0.165321	否
lparAimLPDeleted	1.3.6.1.4.1.546.1.1.0.165322	否
lparAimSlotAdd	1.3.6.1.4.1.546.1.1.0.165340	否
lparAimSlotDelete	1.3.6.1.4.1.546.1.1.0.165341	否
lparAimSlotLPChange	1.3.6.1.4.1.546.1.1.0.165342	否
lparAimSlotMonitorChange	1.3.6.1.4.1.546.1.1.0.165343	否
lparAimSysCfgAlertChange	1.3.6.1.4.1.546.1.1.0.165312	否
lparAimSysCfgMonitorChange	1.3.6.1.4.1.546.1.1.0.165311	否
lparAimSysCPUThresholdChange	1.3.6.1.4.1.546.1.1.0.165313	否
lparAimSysDown	1.3.6.1.4.1.546.1.1.0.165315	否
lparAimSysMEMThresholdChange	1.3.6.1.4.1.546.1.1.0.165314	否
lparAimSysProfAdd	1.3.6.1.4.1.546.1.1.0.165360	否
lparAimSysProfChange	1.3.6.1.4.1.546.1.1.0.165362	否
lparAimSysProfDelete	1.3.6.1.4.1.546.1.1.0.165361	否
lparAimSysStateChangeTrap	1.3.6.1.4.1.546.1.1.0.165310	是
lparAimSysCpuStateChange	1.3.6.1.4.1.546.1.1.0.165318	是

IBM LPAR 陷阱

陷阱名称	陷阱 OID	生成警报？
lparAimLPAlert	1.3.6.1.4.1.546.1.1.0.165324	否
lparAimLPCPUCritThreshold	1.3.6.1.4.1.546.1.1.0.165329	否
lparAimLPCPULagSetting	1.3.6.1.4.1.546.1.1.0.165327	否
lparAimLPCPUMonitor	1.3.6.1.4.1.546.1.1.0.165325	否
lparAimLPCPUState	1.3.6.1.4.1.546.1.1.0.165333	是
lparAimLPCPUWarnThreshold	1.3.6.1.4.1.546.1.1.0.165328	否
lparAimLPMemoryCritThreshold	1.3.6.1.4.1.546.1.1.0.165331	否
lparAimLPMemoryMonitor	1.3.6.1.4.1.546.1.1.0.165326	否
lparAimLPMemoryState	1.3.6.1.4.1.546.1.1.0.165332	是
lparAimLPMemoryWarnThreshold	1.3.6.1.4.1.546.1.1.0.165330	否
lparAimLPMonitor	1.3.6.1.4.1.546.1.1.0.165323	否
lparAimLPStateChange	1.3.6.1.4.1.546.1.1.0.165320	是
lparAimProfAdd	1.3.6.1.4.1.546.1.1.0.165350	否
lparAimProfDelete	1.3.6.1.4.1.546.1.1.0.165351	否
lparAimVIOvEthernetAdd	1.3.6.1.4.1.546.1.1.0.165373	否
lparAimVIOvEthernetRemoved	1.3.6.1.4.1.546.1.1.0.165374	否
lparAimVIOvSCSIAdd	1.3.6.1.4.1.546.1.1.0.165370	否
lparAimVIOvSCSIRemoved	1.3.6.1.4.1.546.1.1.0.165371	否
lparAimVIOvSerialAdd	1.3.6.1.4.1.546.1.1.0.165375	否
lparAimVIOvSerialRemoved	1.3.6.1.4.1.546.1.1.0.165376	否

详细信息：

Virtual Host Manager 中的 IBM LPAR 数据更新方式 (p. 189)
状态监控选项 (p. 193)
如何配置管理选项 (p. 194)
配置和监控资源状态 (p. 197)
CA Spectrum 如何从 CA SystemEDGE 转发陷阱 (p. 202)

用于虚拟网络的故障管理

故障隔离旨在缩小导致网络问题的根本原因的范围。通过查找根本原因，可以帮助您排除故障并快速更正问题，或使用自动化脚本以编程方式更正问题。确定哪些设备是导致警报的根本原因可能非常困难，因为单个设备中的问题会导致网络中的多个设备生成事件。

例如，与 IBM LPAR 主机失去联系通常意味着也会与其管理的 IBM LPAR 实例失去联系。因此，IBM LPAR 主机设备模型和所有受影响的 IBM LPAR 实例都将生成警报。通过使用故障隔离技术，Virtual Host Manager 将关联这些警报以尝试确定单个根本原因。

虚拟网络可提供独特的管理机会，因为它们针对 CA Spectrum 提供了备用管理视角。也就是说，CA Spectrum 可通过直接与您的虚拟设备联系或通过虚拟网络管理技术 IBM LPAR 来收集信息。这种备用管理视角可通过两种方式来增强标准 CA Spectrum 故障管理：

- **增强失去联系警报** - 两个设备信息源可帮助 Virtual Host Manager 查明原因，并更轻松地将事件与单个根本原因关联。
- **代理故障警报** - *代理管理*是指使用备用管理源（代替主要管理器或与主要管理器一起）来管理网络设备的行为。例如，CA Spectrum 可通过直接与虚拟网络设备联系或使用虚拟技术应用程序与设备联系来管理这些虚拟网络设备。当 IBM LPAR 虚拟化技术与虚拟网络设备失去联系时，Virtual Host Manager 将为每个设备生成一个“失去代理管理”警报。这些警报具有唯一性，因为它们提醒您通过*代理*对设备执行的*管理*（而不是设备或直接 (SNMP) 管理的状态）受到影响。

丢失设备联系时故障隔离的工作方式

为了帮助您排除设备中的网络问题，CA Spectrum 使用故障隔离来缩小警报根本原因的范围。对于虚拟网络，Virtual Host Manager 将使用通过与设备直接联系获取的信息，以及由 IBM LPAR 技术通过 IBM LPAR AIM 提供的信息。在许多情况下，标准 CA Spectrum 故障管理可以查明根本原因。但是在一些特殊情况下，无法使用标准方法来隔离虚拟网络中的问题。

Virtual Host Manager 用于发现根本原因的故障隔离类型取决于生成警报的设备，以及设备生成的事件类型。下列方案介绍了两种独特的故障管理情况，以及 CA Spectrum 如何确定虚拟网络中的网络错误。

方案 1：IBM LPAR 实例未运行

在虚拟环境中，与 CA Spectrum 通过标准设备监控发现的信息相比，虚拟管理应用程序可以提供更多的详细信息。例如，IBM LPAR 虚拟化技术可发现 IBM LPAR 何时从“正在运行”状态更改为其他状态（如“打开固件”）。

如果 IBM LPAR 不再运行，并且 CA Spectrum 与其失去联系，但是 IBM LPAR Manager 的代理管理 (请参阅本页中的定义 255)未中断，则 CA Spectrum 将按如下所示确定根本原因：

1. 当 CA Spectrum 与 IBM LPAR 失去联系时，将生成“失去联系”警报。
2. 在其下一个轮询周期内，IBM LPAR Manager 模型将轮询 IBM LPAR AIM 以收集有关 IBM LPAR 实例的信息。由于 IBM LPAR 技术管理 IBM LPAR 实例，因此它可提供导致 IBM LPAR 所生成警报的可能原因的相关信息。
3. 如果 IBM LPAR 技术发现 IBM LPAR 处于未运行模式，它将生成“IBM LPAR 未运行”警报。

   注意：在 IBM LPAR 重新运行后的第一个 IBM LPAR AIM 轮询周期内，将清除此警报。
4. Virtual Host Manager 将“失去联系”警报与 CA Spectrum 所创建的相应“IBM LPAR 未运行”警报关联。Virtual Host Manager 使“失去联系”警报显示为“IBM LPAR 未运行”警报的症状。

方案 2：IBM LPAR 主机关闭

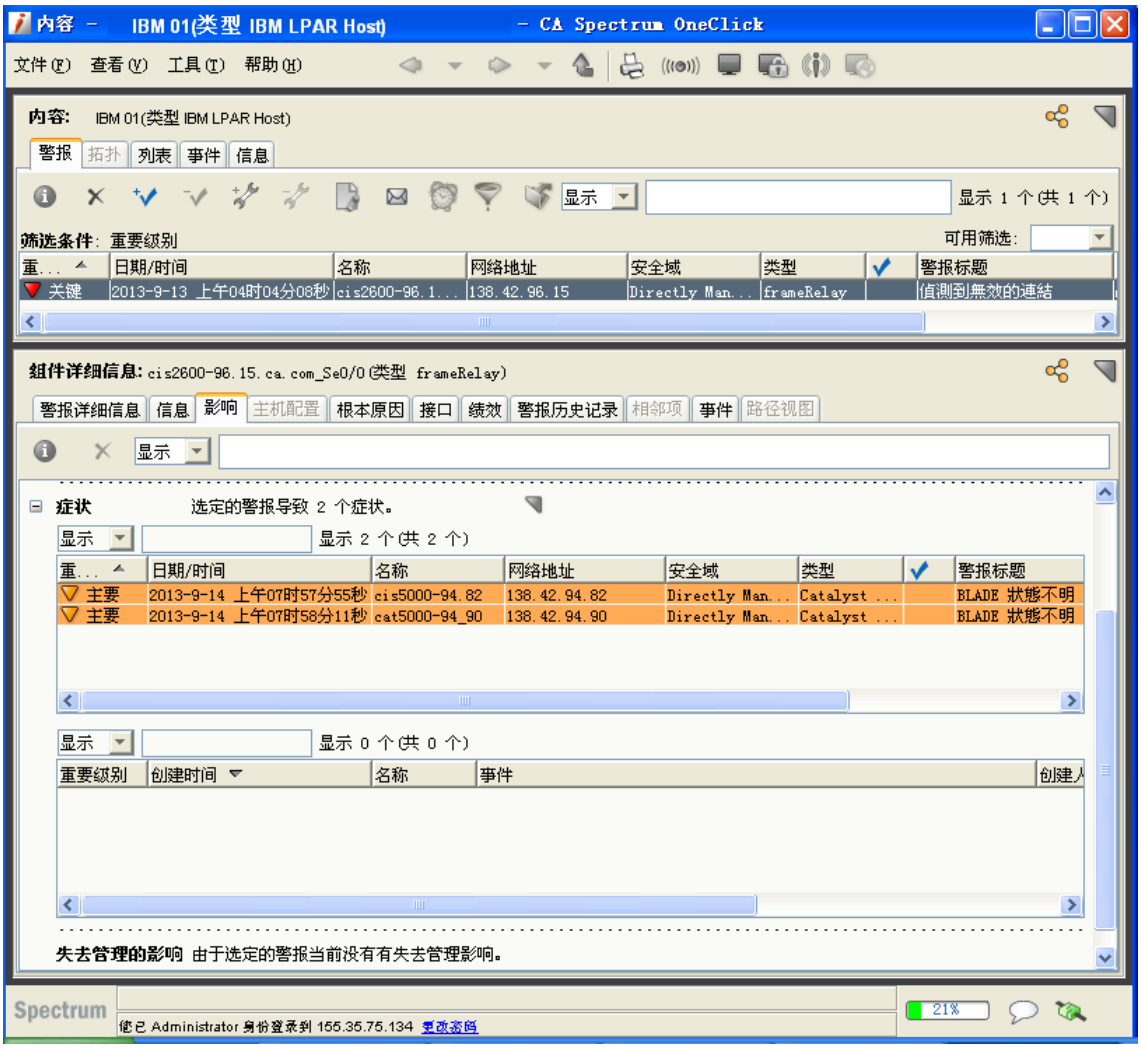
如果 CA Spectrum 与 IBM LPAR 主机上运行的所有 IBM LPAR 失去联系，它将检查上游路由器和交换机的状态。根据它们的状态，CA Spectrum 将按如下所示确定根本原因：

- 一个或多个 IBM LPAR 实例的所有上游设备都不可用 - 标准 CA Spectrum 故障隔离技术将按如下所示确定根本原因：
  - “设备已停止响应轮询”警报 - 当任何 IBM LPAR 的至少一个上游连接设备启动时在 IBM LPAR 主机上生成。
  - “网关不可访问”警报 - 当*所有*上游连接设备都关闭时在 IBM LPAR 主机上生成。
- 至少一个上游设备可用于连接到 IBM LPAR 主机的每个 IBM LPAR 实例 - CA Spectrum 推断 IBM LPAR 主机是根本原因，并按如下所示进行响应：
  a. 直接连接到 IBM LPAR 模型的所有 IBM LPAR、端口和扇出将生成标准故障隔离警报。
  b. Virtual Host Manager 为 IBM LPAR 主机模型创建“物理主机关闭”警报。
  c. 为受影响设备（如 IBM LPAR、端口和扇出）创建的所有故障隔离相关警报将关联到“物理主机关闭”警报，从而使它们成为“物理主机关闭”警报的症状。这些症状警报显示在“物理主机关闭”警报的“影响”选项卡上的“症状”表中。

注意：对于每个 IBM LPAR 主机模型，Virtual Host Manager 将创建一个“虚拟故障域”。此域中包括 IBM LPAR 主机和 IBM LPAR 实例，以及直接连接到 IBM LPAR 的所有端口和扇出。当 IBM LPAR 主机生成“物理主机关闭”警报时，域中的所有标准故障隔离警报将与其关联。将这些警报作为症状关联可表明 IBM LPAR 主机上的“物理主机关闭”警报是根本原因。

d. “影响”选项卡上针对“物理主机关闭”警报的“失去管理的影响”表中列出了所有受影响设备。

注意：被抑制的设备在“症状”表中没有对应的警报。



e. 如果一个或多个 IBM LPAR 实例的所有上游设备都已关闭，则 CA Spectrum 无法再可靠地指出故障出自 IBM LPAR 主机。因此，CA Spectrum 将清除“物理主机关闭”警报，并应用标准 CA Spectrum 故障隔离技术。

详细信息：

丢失代理管理时故障隔离的工作方式 (p. 208)
确定受主机停机影响的 IBM LPAR (p. 210)

丢失代理管理时故障隔离的工作方式

用于创建虚拟网络的 IBM LPAR 虚拟化技术为 CA Spectrum 提供了独特的管理机会。CA Spectrum 可以使用标准方法来直接联系您的虚拟设备，此外，CA Spectrum 可以同时从 IBM LPAR 技术收集虚拟设备信息。从这个意义上讲，IBM LPAR 技术是 CA Spectrum 可从其收集虚拟设备信息的“代理”。如果 CA Spectrum 与设备失去直接联系，则将生成警报。同样，如果 IBM LPAR 技术与虚拟设备失去联系，或者如果 Virtual Host Manager 与 IBM LPAR Manager 失去联系，Virtual Host Manager 将生成警报 -“失去代理管理”警报 (请参阅本页中的定义 255)。

作为响应，CA Spectrum 将尝试隔离导致代理管理故障的原因。代理故障隔离类似于标准 CA Spectrum 故障隔离，不过，这些警报将提醒您虚拟设备的*代理*管理会受到影响。代理管理故障隔离无法指明虚拟设备是已启动还是已关闭。但是，了解何时失去通过代理进行的联系非常重要，因为您可能会丢失设备的重要虚拟信息。

Virtual Host Manager 用于发现根本原因的代理故障隔离类型取决于生成警报的设备，以及设备生成的事件类型。下列方案介绍了两种独特的代理故障管理情况，以及 Virtual Host Manager 如何确定虚拟网络中的网络错误。

方案 1：IBM LPAR Manager 与 HMC 之间失去联系

如果 IBM LPAR Manager 与 HMC 以及该 HMC 管理的所有 IBM LPAR 主机和 IBM LPAR 失去联系，则有关该 IBM LPAR 主机和承载的所有 IBM LPAR 实例的 IBM LPAR Manager 数据将丢失。为了隔离该问题，Virtual Host Manager 将按如下所示确定根本原因：

1. 将在 IBM LPAR 主机和承载的所有 IBM LPAR 上生成“代理已丢失”警报。
2. IBM LPAR 警报将与 IBM LPAR 主机的“代理已丢失”警报关联，使这些 IBM LPAR 警报成为 IBM LPAR 主机警报的症状。将这些警报作为症状关联可表明 IBM LPAR 主机警报是根本原因。
3. 如果 CA Spectrum 也与 IBM LPAR 主机失去联系并生成“物理主机关闭”警报，则为 IBM LPAR 主机生成的“代理已丢失”警报将与“物理主机关闭”警报关联。在这种情况下，“代理已丢失”警报成为“物理主机关闭”警报的症状。将此警报关联为症状表明 Solaris Zones 主机上的“物理主机关闭”警报是根本原因。

方案 2：CA Spectrum 与 IBM LPAR Manager 之间失去联系

如果 CA Spectrum 与 IBM LPAR Manager 模型失去联系或停止轮询该模型，则将丢失该 IBM LPAR Manager 管理的所有虚拟模型的 IBM LPAR 技术数据。为了隔离该问题，Virtual Host Manager 将按如下所示确定根本原因：

1. CA Spectrum 将为该 IBM LPAR Manager 管理的所有虚拟模型（包括 IBM LPAR 实例和 IBM LPAR 主机）生成“代理已丢失”警报。CA Spectrum 还将在 IBM LPAR Manager 模型上生成单独的“代理不可用”警报。
2. IBM LPAR 警报将与其相应的 IBM LPAR 主机模型警报关联。
3. IBM LPAR 主机模型警报将与 IBM LPAR Manager 模型的“代理不可用”警报关联。
4. 然后，此“代理不可用”警报将与正关闭的 IBM LPAR Manager 的根本原因关联。根本原因通常是由标准 CA Spectrum 故障管理生成的警报，例如为下列情况创建的警报：
   - 失去 IBM LPAR Manager 的管理（即，IBM LPAR Manager 主机上的 CA SystemEDGE 代理发生问题）
   - 失去计算机联系
   - IBM LPAR Manager 模型处于维护模式

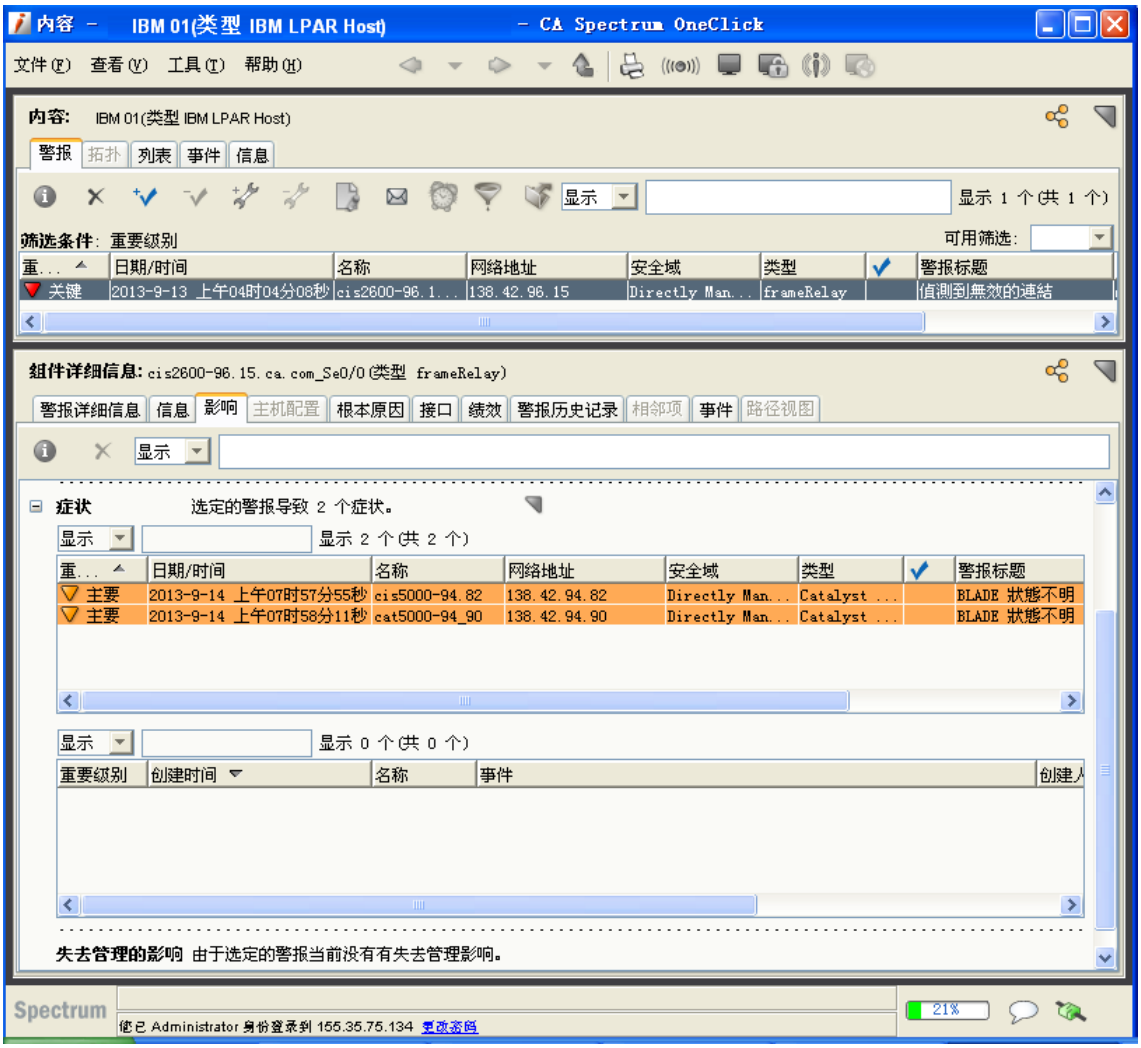
详细信息：

丢失设备联系时故障隔离的工作方式 (p. 205)

确定受主机停机影响的 IBM LPAR

当与 IBM LPAR 主机的联系中断或者 IBM LPAR 主机关闭时，IBM LPAR 主机承载的所有 IBM LPAR 实例都将受到影响。由于 IBM LPAR 技术无法与 IBM LPAR 主机进行通信以获取使用情况信息，因此您可能不会接收到该 IBM LPAR 主机上承载的关键 IBM LPAR 的警报。要确定关键 IBM LPAR 是否受到影响，可以在警报的“影响”选项卡上查看受影响 IBM LPAR 实例的列表，如下所示：

- “症状”子视图 - 显示受影响的 IBM LPAR 实例生成的所有症状警报
- “失去管理的影响”视图 - 列出受警报影响的 IBM LPAR 实例



详细信息：

丢失设备联系时故障隔离的工作方式 (p. 205)

第 7 章： Huawei SingleCLOUD

本节适用于 Huawei SingleCLOUD 虚拟化技术用户，将介绍如何使用 Virtual Host Manager 管理 Huawei SingleCLOUD 平台中的虚拟实体。

此部分包含以下主题：

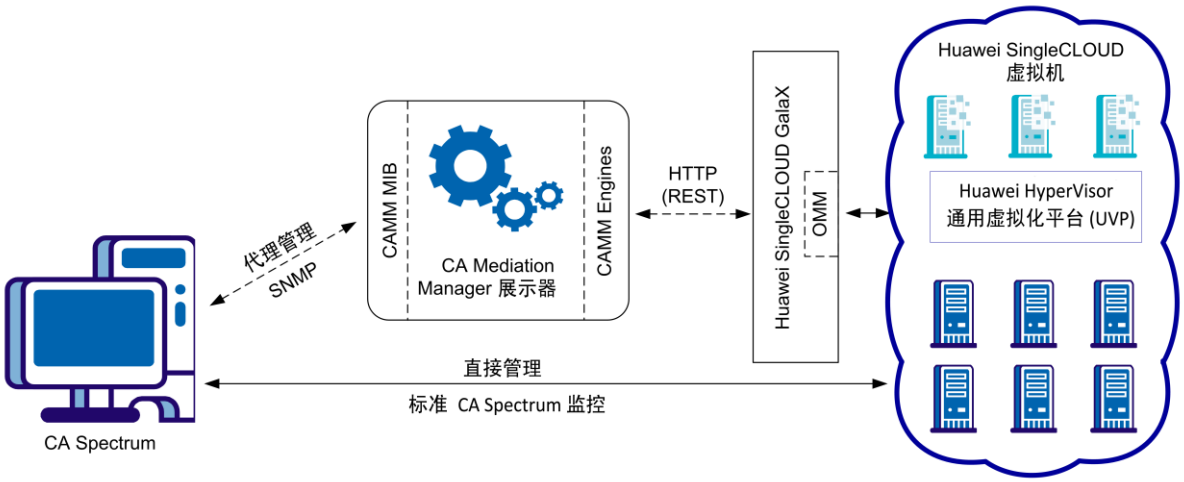
Virtual Host Manager 如何使用 Huawei SingleCLOUD

Virtual Host Manager 可以无缝监控您的虚拟网络实体和物理网络实体。您可以全面了解网络情况，并在网络中排除这两类实体的网络问题。虽然虚拟网络实体的行为与物理组件的行为类似，但是对这些实体的监控过程不同于一般 CA Spectrum 监控过程。了解此过程的工作原理可帮助您找到并解决与虚拟网络相关的网络问题。

Huawei SingleCLOUD 平台由完整的网络系统、存储、服务器和软件组成，用于创建专用或公共云。Virtual Host Manager 可帮助您管理和监控 Huawei SingleCLOUD 虚拟环境。

CA Spectrum 通过两种不同的方法收集有关 Huawei SingleCLOUD 虚拟环境的信息。与 CA Spectrum 管理的其他设备一样，Virtual Host Manager 使用标准 CA Spectrum 监控方法。此外，用于 Huawei SingleCLOUD 的 Virtual Host Manager 还从备用（代理）管理器 CA Mediation Manager (CAMM) 检索专用信息。

下图显示了 CA Spectrum 如何收集有关 Huawei SingleCLOUD 环境的信息：



CA Mediation Manager 驻留在它自己的主机上，并通过使用 HTTP (REST) 服务与 Huawei SingleCLOUD GalaX（统一管理 Huawei SingleCLOUD 的软件套件）进行通信，从 Huawei SingleCLOUD 环境获取信息。

CAMM 使用以下组件：

- 引擎。引擎是 CAMM 的轮询引擎，用于从 Huawei SingleCLOUD 平台中收集信息。CAMM 引擎直接与 Huawei SingleCLOUD GalaX 操作和管理模块 (OMM) 进行通信，以获取有关 Huawei HyperVisor 通用虚拟化平台 (UVP) 的信息。
- 展示器。展示器从引擎接收信息，并使用此信息填充 CA 开发的 MIB (CAMEDIATIONMANAGER-ENTERPRISES-HUAWEI-SINGLECLOUD-MIB)。

CA Spectrum 使用 SNMP 从 CAMM MIB 检索数据，并使用此信息在 OneClick 中对 Huawei SingleCLOUD 环境进行建模和监控。

为 Huawei SingleCLOUD 创建的模型

Virtual Host Manager 提供了多个模型来表示 Huawei SingleCLOUD 虚拟网络的组件。通过了解以下基本模型，可以帮助您更好地了解发现以及虚拟环境与物理环境的连接方式。

Virtual Host Manager 包括用于 Huawei SingleCLOUD 实体的以下模型和图标：

Huawei SingleCLOUD CAMM 展示器

表示 CA Mediation Manager (CAMM) 展示器。CAMM 展示器模型允许配置 CAMM 引擎用来与 Huawei SingleCLOUD GalaX 进行通信的虚拟 IP 地址。每个 CAMM 展示器可以支持多个虚拟 IP 地址。

图标： 

Huawei SingleCLOUD Manager

表示 CAMM 展示器上的虚拟 IP 地址。CAMM 与 Huawei SingleCLOUD GalaX 进行通信，后者负责管理 Huawei SingleCLOUD 虚拟平台。由 CAMM 监控的每个 Huawei SingleCLOUD GalaX 的信息通过 CAMM 展示器上的虚拟 IP 地址来提供，并由 Huawei SingleCLOUD Manager 模型表示。

图标： 

Huawei SingleCLOUD 云

表示构成专用或公共云网络的物理和虚拟主机的集合。

图标： 

Huawei SingleCLOUD 主机

表示承载虚拟机的计算节点代理 (CNA)。在 Universe 拓扑中，这些模型会将虚拟实体分组到单独的视图中，同时显示虚拟环境与物理网络的连接情况。不能直接联系 Huawei SingleCLOUD 主机以获取状态信息。而是将通过模型中所含项目的状态来推断此模型的状态。

图标： 

Huawei SingleCLOUD CNA FIP

表示正在承载虚拟机的 CNA 的管理接口。此模型分配有 CNA FIP 的 IP 地址，并存在于主机容器内。

图标： 

Huawei SingleCLOUD 虚拟机

表示在 Huawei SingleCLOUD 平台中配置的虚拟机。

图标： 

发现 Huawei SingleCLOUD 网络

必须先发现并建模要管理的任何网络元素，才能使用 Virtual Host Manager 监控 Huawei SingleCLOUD 虚拟环境。本节介绍用于 Huawei SingleCLOUD 的 Virtual Host Manager 的发现和建模过程。这些任务通常由 Virtual Host Manager 管理员执行。

遵循这些步骤:

1. 执行以下发现前步骤：
   a. 定义 CA Mediation Manager 展示器。 (p. 215)
   b. 配置发现选项。 (p. 216)
2. 发现并建模 Huawei SingleCLOUD 网络。 (p. 221)

定义 CA Mediation Manager 展示器

安装 Virtual Host Manager 后，可以为 CA Spectrum 定义 CA Mediation Manager 展示器。Huawei SingleCLOUD CAMM 展示器模型允许配置与 Huawei SingleCLOUD GalaX 关联的虚拟 IP 地址。定义 CAMM 展示器将创建一个容器模型，该模型之后将用于组织和包含 Huawei SingleCLOUD Manager 模型。

注意：创建 Huawei SingleCLOUD CAMM 展示器模型不会触发发现。

遵循这些步骤:

1. 在“导航”面板的“资源管理器”选项卡中，选择 Virtual Host Manager 节点。

   “内容”面板将显示有关 Virtual Host Manager 功能的信息。
2. 选择“信息”选项卡。
3. 展开“配置”、“Huawei SingleCLOUD”、“CA Mediation Manager 展示器”子视图。

   将显示“CA Mediation Manager 展示器”表。
4. 单击“添加”。

   将显示“创建 HuaweiSCCAMMPresenter 类型的模型”对话框。
5. 输入名称和说明，然后单击“确定”。

   Huawei SingleCLOUD CAMM 展示器模型即已创建，并将显示在表中。

详细信息：

为 Huawei SingleCLOUD 创建的模型 (p. 212)

配置发现选项

在执行发现以为 Huawei SingleCLOUD 实体创建模型之前，指定用于控制发现进程各个方面的选项。配置首选项可帮助 Virtual Host Manager 按预期为虚拟设备建模。

要为 Huawei SingleCLOUD 发现配置 Virtual Host Manager 安装，请从下列选项中选择首选项：

- 新 Huawei SingleCLOUD 虚拟机的维护模式 (p. 216) - 允许您决定是否在可使用 CA Spectrum 来管理新发现的虚拟机之前将它们置于维护模式。
- 允许在运行 Huawei SingleCLOUD 发现期间删除设备模型 (p. 217) - 控制当 Huawei SingleCLOUD 模型不再受 Virtual Host Manager 管理时，CA Spectrum 如何处理它们。
- 搜索现有模型 (p. 218) - 确定在 Huawei SingleCLOUD 发现期间 Virtual Host Manager 搜索的安全域。
- 在执行 Huawei SingleCLOUD Manager 删除期间保留启用了 SNMP 的虚拟机 (p. 219) - 控制在删除 Huawei SingleCLOUD Manager 模型时，CA Spectrum 如何处理启用了 SNMP 的 Huawei SingleCLOUD 模型。
- 发现支持 SNMP 的设备 (p. 221) - 控制如何在 Huawei SingleCLOUD 发现期间为支持 SNMP 的设备建模。默认情况下，最初仅会将新模型创建为 VHM 模型 (请参阅本页中的定义 255)。但是，此选项允许您覆盖默认设置，并为符合标准的设备立即创建 SNMP 模型。

为新 Huawei SingleCLOUD 设备配置维护模式

Virtual Host Manager 会自动为构成 Huawei SingleCLOUD 虚拟环境的虚拟机建模。CA Spectrum 将尝试管理所有已发现的模型。但是，在最初建模某些新发现的 Huawei SingleCLOUD 虚拟机时，它们尚未准备好由 CA Spectrum 管理。为阻止在新 Huawei SingleCLOUD 虚拟机模型上生成不需要的警报，您可以决定将哪些新模型立即置于维护模式。之后，可以在准备好由 CA Spectrum 管理这些设备时手动禁用维护模式。

遵循这些步骤:

1. 在“导航”面板的“资源管理器”选项卡中，单击 Virtual Host Manager 节点。

   “内容”面板将显示有关 Virtual Host Manager 功能的信息。
2. 单击“信息”选项卡。
3. 展开“配置”、“Huawei SingleCLOUD”、“Huawei SingleCLOUD 发现”子视图。

   将显示可配置的发现选项。

4. 在“新 Huawei SingleCLOUD 虚拟机的维护模式”字段中单击“设置”，然后选择下列选项之一：

   将未启用的 VM 置于维护模式

   （默认）在初始 Huawei SingleCLOUD 发现期间，仅向未启用的 Huawei SingleCLOUD 虚拟机模型应用维护模式。

   将所有 VM 置于维护模式

   在初始 Huawei SingleCLOUD 发现期间，向所有新发现的 Huawei SingleCLOUD 虚拟机模型应用维护模式。

   将保存您的设置，并且会根据您的选择将新发现的由 Virtual Host Manager 创建的 Huawei SingleCLOUD 虚拟机模型置于维护模式。

管理已删除 Huawei SingleCLOUD 设备的设备模型

虚拟环境中的设备及设备间的关联关系会频繁地发生更改。在 CA Spectrum 中维护有关虚拟环境的准确且及时的数据很具挑战性。例如，删除 Huawei SingleCLOUD 虚拟机时，CA Spectrum 知道要在“导航”面板中从 Virtual Host Manager 删除相应的设备模型。但是，CA Spectrum 是应保留还是删除模型？您可以选择设置以控制是否删除模型。

重要说明！删除模型时，这些模型上的所有注释或其他自定义也将丢失。如果以后可能会在 Huawei SingleCLOUD 环境中重新创建模型，则可以禁用此选项。

遵循这些步骤:

1. 在“导航”面板的“资源管理器”选项卡中，单击 Virtual Host Manager 节点。

   “内容”面板将显示有关 Virtual Host Manager 功能的信息。

2. 单击“信息”选项卡。
3. 展开“配置”、“Huawei SingleCLOUD”、“Huawei SingleCLOUD 发现”子视图。

   将显示可配置的发现选项。

4. 在“允许在运行 Huawei SingleCLOUD 发现期间删除设备模型”字段中单击“设置”，然后选择下列选项之一：

   是

   （默认）删除不再受 Huawei SingleCLOUD 环境管理的实体的对应 Virtual Host Manager 模型。

   否

   当 Virtual Host Manager 模型的相应实体不再受 Huawei SingleCLOUD 环境管理，但是未从 CA Spectrum 删除这些模型时，将这些模型放置在 LostFound 容器中。

   注意：将以不同的方式处理具有更多关联的模型（如全局集合中包括的模型）。将从 Universe 中删除这些模型，但是不会将其移动到 LostFound 容器中。

   将保存您的设置，并且会在从 Huawei SingleCLOUD 环境中删除设备之后相应地处理设备模型。

跨安全域配置模型搜索

Huawei SingleCLOUD 发现将尝试查找 SpectroSERVER 中存在的模型，而不是创建新模型。在已部署 Secure Domain Manager 的环境中，Huawei SingleCLOUD 发现将搜索与 Huawei SingleCLOUD Manager 位于同一个安全域中的模型。此域是“本地”域。但是，某些设备可存在于不同的安全域中。在这种情况下，可以配置 Huawei SingleCLOUD 发现以搜索所有安全域中的现有模型。

遵循这些步骤:

1. 在“导航”面板的“资源管理器”选项卡中，单击 Virtual Host Manager 节点。

   “内容”面板将显示有关 Virtual Host Manager 功能的信息。

2. 单击“信息”选项卡。
3. 展开“配置”、“Huawei SingleCLOUD”、“Huawei SingleCLOUD 发现”子视图。

   将显示可配置的发现选项。

4. 在“搜索现有模型”字段中单击“设置”，然后从下列选项中进行选择：

   在 Huawei SingleCLOUD Manager 的安全域中

   （默认）搜索与 Huawei SingleCLOUD Manager 服务器位于同一个安全域中的模型。

   在所有安全域中

   搜索由 SpectroSERVER 管理的所有安全域中的模型。仅在下列情况下选择此选项：

   - 所有设备具有唯一的 IP 地址
   - 当安全域用于安全目的或用于隔离网络通信时

   注意：不要为 NAT 环境选择此选项。

   将保存您的设置，并且 Huawei SingleCLOUD 发现会根据您的选择在 CA Spectrum 中搜索现有模型。当多个安全域中存在重复的模型（即共享相同 IP 地址的模型）时，Virtual Host Manager 将执行以下操作：

   - 在本地安全域中选择模型（如果有）。
   - 如果本地域中不存在重复的模型，Virtual Host Manager 将随机地从其他安全域中选择模型。

   在这两种情况下，Virtual Host Manager 将在 Huawei SingleCLOUD Manager 模型上为重复的 IP 地址生成次要警报。

管理启用了 SNMP 的 Huawei SingleCLOUD 模型的删除

默认情况下，删除以下项时，将从 CA Spectrum 中删除启用了 SNMP 的设备：

- “资源管理器”选项卡中的 Huawei SingleCLOUD 文件夹
- Huawei SingleCLOUD CAMM 展示器模型
- Huawei SingleCLOUD Manager 模型

启用了 SNMP 的设备模型可包括要保留的重要自定义。可以调整设置以避免删除这些模型。可将它们放置在 LostFound 容器中供以后使用。

遵循这些步骤:

1. 在“导航”面板的“资源管理器”选项卡中，单击 Virtual Host Manager 节点。

   “内容”面板将显示有关 Virtual Host Manager 功能的信息。

2. 单击“信息”选项卡。

3. 展开“配置”、“Huawei SingleCLOUD”、“Huawei SingleCLOUD 发现”子视图。

   将显示可配置的发现选项。

4. 在“在执行 Huawei SingleCLOUD Manager 删除期间保留启用了 SNMP 的虚拟机”字段中单击“设置”，然后选择下列选项之一：

   是

   删除其 Huawei SingleCLOUD 文件夹、Huawei SingleCLOUD CAMM 展示器模型或 Huawei SingleCLOUD Manager 模型时，将启用了 SNMP 的虚拟机模型保留在 LostFound 容器中。

   注意：将以不同的方式处理具有更多关联的模型（如全局集合中包括的模型）。将从 Universe 中删除这些模型，但是不会将其移动到 LostFound 容器中。

   否

   （默认）删除其 Huawei SingleCLOUD 文件夹、Huawei SingleCLOUD CAMM 展示器模型或 Huawei SingleCLOUD Manager 模型时，将删除所有的 Huawei SingleCLOUD 模型。

   将保存您的设置，并且会在删除 Huawei SingleCLOUD 文件夹、Huawei SingleCLOUD CAMM 展示器模型或 Huawei SingleCLOUD Manager 模型时相应地处理启用了 SNMP 的设备模型。

配置 SNMP 建模首选项

支持 SNMP 的设备可支持丰富的设备监控功能，如进程和文件系统监控功能。但是，部署 SNMP 代理可能会花费较高的经济和时间成本。默认情况下，Huawei SingleCLOUD 发现将 Huawei SingleCLOUD 虚拟机创建为 VHM 模型 (请参阅本页中的定义 255)。可在以后将它们升级为 SNMP 模型。不过，也可以将 Huawei SingleCLOUD 发现配置为将所有支持 SNMP 的新设备建模为 SNMP 模型。虽然完成 Huawei SingleCLOUD 发现可能需要更长的时间，但是初始建模为 SNMP 模型可避免以后手动升级这些模型。

重要说明！在为 Huawei SingleCLOUD 组件建模*之前*，请启用 SNMP 建模。如果首先为 Huawei SingleCLOUD 组件建模，则会将所有子模型创建为 VHM 模型，并且必须手动将其升级为 SNMP 模型。

遵循这些步骤:

1. 在“导航”面板的“资源管理器”选项卡中，单击 Virtual Host Manager 节点。

   “内容”面板将显示有关 Virtual Host Manager 功能的信息。

2. 单击“信息”选项卡。
3. 展开“配置”、“Huawei SingleCLOUD”、“Huawei SingleCLOUD 发现”、“SNMP 发现”子视图。
4. 在“发现支持 SNMP 的设备”字段中单击“设置”，然后从下列选项中进行选择：

   是

   在 Huawei SingleCLOUD 发现期间启用 SNMP 建模。仅会将符合“SNMP 发现”子视图文本中标准的设备建模为 SNMP 设备。仅适用于*新*模型。

   否

   （默认）将 Huawei SingleCLOUD 发现期间找到的所有新设备建模为 VHM 模型 (请参阅本页中的定义 255)。可在以后手动将这些模型升级为 SNMP 模型。

   将保存您的设置，并且会根据您的选择在 Virtual Host Manager 中为新设备建模。

发现并建模 Huawei SingleCLOUD 环境

要监控虚拟环境，必须发现并建模虚拟实体 - Huawei SingleCLOUD Manager、云、主机和虚拟机。通过在 Virtual Host Manager 中为这些实体建模，可以在一个工具中查看完整的网络拓扑，其中显示了物理组件和虚拟组件之间的关联关系。

为虚拟环境建模的主要步骤如下所示：

1. 运行标准的 CA Spectrum 发现 (p. 222)。

   此发现的目的是在 Huawei SingleCLOUD 发现运行之前为上游路由器和交换机建模。在为这些实体建模时，请确保正确设置建模选项以支持 Virtual Host Manager。

2. 定义 Huawei SingleCLOUD Manager (p. 224)。

   此步骤将发现并建模 CAMM 用来与 Huawei SingleCLOUD GalaX（Huawei SingleCLOUD 虚拟平台的管理应用程序）进行通信的虚拟 IP 地址。CA Spectrum 使用这些模型检索有关 Huawei SingleCLOUD 体系结构及其虚拟机的信息。

3. 允许运行 Huawei SingleCLOUD 发现 (p. 224)。

   为 Huawei SingleCLOUD Manager 建模时，将自动启动 Huawei SingleCLOUD 发现，以发现并建模 Huawei SingleCLOUD 环境中的虚拟实体。

4. （可选）向 VHM 模型添加 SNMP 功能 (p. 226)。

   如果已将 Huawei SingleCLOUD 实体建模为 VHM 模型，则可在以后将它们升级为 SNMP 模型。

5. （可选）将 Huawei SingleCLOUD 主机移至其他 Huawei SingleCLOUD GalaX (p. 228)。

   将 Huawei SingleCLOUD 主机从一个 Huawei SingleCLOUD GalaX 的管理移至另一个相应管理时，应按特定顺序执行步骤以准确反映已建模 CA Spectrum 环境中的更改。

在以下各节中对其中每个步骤进行了详细介绍。

运行 CA Spectrum 发现

要准确反映完整的 Huawei SingleCLOUD 环境，请运行标准 CA Spectrum 发现以查找任何连接设备。将为上游路由器和交换机建模，以便将来可以从虚拟实体建立连接。

注意：只有管理员才可以执行此任务。

遵循这些步骤:

1. 打开发现控制台。

   注意：在建模之前，请确保您知道在非标准端口上运行的任何 SNMP 代理的正确团体字符串、IP 地址和端口号。

2. 在“导航”面板中单击  （新建配置）。

   此时将打开“配置”对话框。

3. 指定新配置的名称和位置，然后单击“确定”。

   此时将关闭“配置”对话框。

4. 输入各个 IP 地址，或在“IP/主机名边界列表”字段中输入开始 IP 地址和结束 IP 地址，然后单击“添加”。

   注意：请确保 IP 地址范围包括所有的互连交换机和路由器。

5. 配置建模选项，如下所示：

   a. 选择“发现并为 CA Spectrum 自动建模”选项。

   b. 单击“建模选项”按钮。

      此时将打开“建模配置”对话框。

   c. 单击“协议选项”按钮。

      此时将打开“协议选项”对话框。

   d. 选择“Pingable 项的 ARP 表”选项，然后单击“确定”。

      此时将关闭“协议选项”对话框。

   e. 单击“确定”关闭“建模配置”对话框。

6. （可选）在“高级选项”组中单击“高级选项”按钮，添加非标准 SNMP 端口（如 CAMM 端口），然后单击“确定”。

7. 在发现控制台中输入任何其他值，然后单击“发现”。

   将为可将 Huawei SingleCLOUD 实体连接到网络的交换机和路由器创建模型，并将这些模型添加到 CA Spectrum 的网络拓扑中。

定义 Huawei SingleCLOUD Manager

定义 Huawei SingleCLOUD CAMM 展示器 (请参阅本页中的定义 253)并为连接设备建模后，可以建模并发现 Huawei SingleCLOUD Manager (请参阅本页中的定义 253)。成功创建 Huawei SingleCLOUD Manager 模型后，将自动触发 Huawei SingleCLOUD 发现。

遵循这些步骤:

1. 在“导航”面板的“资源管理器”选项卡中，从 Virtual Host Manager 层次结构的 Huawei SingleCLOUD 文件夹中选择“Huawei SingleCLOUD CAMM 展示器”。

   “组件详细信息”面板将显示 CAMM 展示器的信息。

2. 在“组件详细信息”面板上的“信息”选项卡中，展开“Huawei SingleCLOUD Manager”子视图。

   将显示“Huawei SingleCLOUD Manager”表。

3. 单击“添加”。

   将显示“创建 HuaweiSCManager 类型的模型”对话框。

4. 输入 Huawei SingleCLOUD Manager 的信息，然后单击“确定”。请注意以下字段：

   网络地址

   输入 CAMM 展示器用来与 Huawei SingleCLOUD GalaX 进行通信的虚拟 IP 地址。

   重要说明！此值不应与安装了 CAMM 展示器的设备或虚拟机的主 IP 地址相同。

   Huawei SingleCLOUD Manager 模型即已创建，并将显示在表中。有关 Huawei SingleCLOUD 环境的信息来自 Huawei SingleCLOUD Manager。创建此模型时，Huawei SingleCLOUD 发现将启动。

详细信息：

为 Huawei SingleCLOUD 创建的模型 (p. 212)

Huawei SingleCLOUD 发现

Huawei SingleCLOUD 发现是专门用于收集有关虚拟环境的详细信息的发现进程。发现的目的是发现并建模 Huawei SingleCLOUD 平台中的虚拟实体。通过了解 how Huawei SingleCLOUD 发现的工作方式，可更有力地说明正确安装和建模各个 Virtual Host Manager 组件的重要性。

Huawei SingleCLOUD 发现的主要优点是，它在后台自动运行，可持续更新 CA Spectrum 中的虚拟环境数据。由于此自动功能，Huawei SingleCLOUD 发现的若干部分已在前面的步骤中发生。以下描述从总体上说明 Huawei SingleCLOUD 发现，仅供参考。无需执行任何操作。

Huawei SingleCLOUD 发现进程的工作方式如下：

1. 在正确安装 CAMM 和 Huawei SingleCLOUD 设备包之后，CAMM 引擎会立即开始与 Huawei SingleCLOUD GalaX 进行通信。信息将由 CAMM 展示器处理，并可供 CA Spectrum 使用。

   重要说明！必须安装并配置 CA Mediation Manager 和 Huawei SingleCLOUD 设备包，CA Spectrum、CAMM 和 Huawei SingleCLOUD GalaX 才能进行通信。如果它们无法通信，Huawei SingleCLOUD 发现将无法运行。

2. 在 CA Spectrum 发现期间，CA Spectrum 将创建用于连接设备的模型，以便将来可以从虚拟实体建立连接。

3. 将创建 Huawei SingleCLOUD CAMM 展示器和 Huawei SingleCLOUD Manager 模型。通过创建 Huawei SingleCLOUD Manager，CA Spectrum 可以处理 CA Spectrum 和 CAMM 之间的通信。

4. Huawei SingleCLOUD Manager 轮询 CAMM 以收集有关 Huawei SingleCLOUD 环境的信息（已在步骤 1 中收集）。

5. CA Spectrum 启动 Huawei SingleCLOUD 发现。CA Spectrum 使用此信息在 CA Spectrum“拓扑”选项卡和“导航”面板的 Virtual Host Manager 层次结构中更新建模，如下所示：

   a. 如果在步骤 2 之前启用 SNMP 发现，则 Virtual Host Manager 发现将为符合 SNMP 发现标准的所有支持 SNMP 的新模型创建 SNMP 模型。

      注意：默认情况下，将在 Huawei SingleCLOUD 发现期间禁用 SNMP 发现。

   b. 将为其余非 SNMP Huawei SingleCLOUD 实体创建 VHM 模型。

   注意：在虚拟环境中，不同 Huawei SingleCLOUD 主机上的设备可具有相同的 IP 地址或 MAC 地址。在这种情况下，CA Spectrum 将为每个 IP 地址或 MAC 地址创建重复的模型。

6. Huawei SingleCLOUD 发现将自动按每个定期排定的 Huawei SingleCLOUD Manager 轮询时间间隔重复该过程。

向 VHM 模型添加 SNMP 功能

支持 SNMP 的设备可支持丰富的设备监控功能，如进程和文件系统监控功能。但是，部署 SNMP 代理可能会花费较高的经济和时间成本。当 SNMP 代理不可用或禁用了 SNMP 发现时，Virtual Host Manager 会将 Huawei SingleCLOUD 实体创建为 VHM 模型 (请参阅本页中的定义 255)。

之后，您可以在任何 Huawei SingleCLOUD 主机或虚拟机上安装 SNMP 代理，并在 CA Spectrum 中升级其建模。用于升级到 SNMP 模型的选项如下所示：

- 仅升级选定设备 (p. 226)- 当需要升级少量选定模型时，此方法可快速完成工作。将首先删除 VHM 模型。此方法的一个缺点是，在 CA Spectrum 删除模型之后，必须等待下一个 Huawei SingleCLOUD 发现进程以创建新 SNMP 模型，并将它们放置在 Virtual Host Manager 中。必须知道模型的 IP 地址才能进行升级。
- 升级所有支持 SNMP 的 VHM 模型 (p. 227) - 此方法可批量升级模型，在将 Virtual Host Manager 升级为新版本时，最好使用此方法。不必知道各个模型的 IP 地址。另一个优点是，在 CA Spectrum 删除 VHM 模型之后，会立即将升级后的 SNMP 模型放置在 Virtual Host Manager 层次结构中，而不必等待下一个轮询周期。因此，Virtual Host Manager 可更快地管理模型。

  此方法的一个缺点是可能需要很长时间才能完成。完成此升级所需的时间取决于在查找支持 SNMP 的设备时，Virtual Host Manager 必须搜索的团体字符串和 SNMP 端口的数量。

  注意： Virtual Host Manager 仅会尝试识别已启动的可 Ping 设备上的 SNMP 代理。

重要说明！删除模型时，这些模型上的所有注释或其他自定义也将丢失。

将选定 VHM 模型升级为 SNMP 模型

当 SNMP 代理不可用或在 Huawei SingleCLOUD 发现期间禁用了 SNMP 发现时，Virtual Host Manager 会将 Huawei SingleCLOUD 主机和虚拟机创建为 VHM 模型 (请参阅本页中的定义 255)。之后，您可以在这些设备上安装 SNMP 代理，并在 CA Spectrum 中升级其建模。您必须知道 IP 地址才能升级设备模型。手动选择要升级的模型可快速完成，但这些模型上的所有说明或自定义将会在升级期间丢失。

遵循这些步骤:

1. 根据需要在设备上部署或启用 SNMP 代理。
2. 使用下列方法之一重新建模设备：
   - CA Spectrum 发现
   - 按 IP 地址为设备逐个建模

   在创建支持 SNMP 的新模型时，CA Spectrum 将从 Virtual Host Manager 中移除以前的模型并将其删除。在下一个 Huawei SingleCLOUD Manager 轮询周期中，CA Spectrum 将支持 SNMP 的模型添加到“导航”面板的 Virtual Host Manager 中。

   重要说明！删除模型时，这些模型上的所有注释或其他自定义也将丢失。

将所有 VHM 模型升级为 SNMP 模型

当 SNMP 代理不可用或在 Huawei SingleCLOUD 发现期间禁用了 SNMP 发现时，Virtual Host Manager 会将 Huawei SingleCLOUD 主机和虚拟机创建为 VHM 模型 (请参阅本页中的定义 255)。之后，您可以在这些设备上安装 SNMP 代理，并在 CA Spectrum 中升级其建模。在执行批量升级时，CA Spectrum 将搜索 VHM 模型，并查找支持 SNMP 的设备。然后，CA Spectrum 将它们转换为 SNMP 模型。此方法可能需要很长的时间才能完成，具体取决于 Virtual Host Manager 必须搜索的团体字符串和端口的数量。

遵循这些步骤:

1. 根据需要在设备上部署或启用 SNMP 代理。
2. 在“导航”面板中打开 Virtual Host Manager。

   将在选定 Virtual Host Manager 的“内容”面板中打开主详细信息页面。
3. 在“导航”面板中选择用于管理要升级的模型的 Huawei SingleCLOUD Manager 模型。
4. 单击“信息”选项卡。
5. 展开“Huawei SingleCLOUD Manager”、“CA Spectrum 建模控制”子视图。
6. 单击“升级 ICMP 专用设备”按钮。

   重要说明！删除模型时，这些模型上的所有注释或其他自定义也将丢失。

   Virtual Host Manager 将搜索由 Huawei SingleCLOUD Manager 管理的 VHM 模型。Virtual Host Manager 升级符合 SNMP 设备标准的 ICMP 专用设备，并将它们放置在 Virtual Host Manager 层次结构中。

将 Huawei SingleCLOUD 主机移至其他 Huawei SingleCLOUD GalaX

在将 Huawei SingleCLOUD 主机从一个 Huawei SingleCLOUD GalaX 的管理移至另一个相应管理时，如果这两个 Huawei SingleCLOUD Manager 是在同一个 SpectroSERVER 上建模的，则可能会导致 CA Spectrum 建模问题。

这些建模问题的一些可能症状如下：

- CA Spectrum 删除与主机关联的模型，并且不会在移动后重新创建它们。
- 创建并保留虚假“代理已丢失”警报，即使新的管理 Huawei SingleCLOUD GalaX 可联系主机和承载的所有虚拟机也是如此。

要避免这些问题，请按正确顺序执行相应步骤以移动主机并在建模的 CA Spectrum 环境中反映更改，如下所示：

遵循这些步骤:

1. （可选）将“允许在运行 Huawei SingleCLOUD 发现期间删除设备模型”选项更改为“否” (p. 217)。

   注意：仅当原始 Huawei SingleCLOUD Manager 和目标 Huawei SingleCLOUD Manager 在同一个 SpectroSERVER 中建模时，才需要执行此步骤。将此选项设置为“否”，可阻止在第一个 Huawei SingleCLOUD GalaX 取消管理现有的 Huawei SingleCLOUD 主机、CNA FIP 和虚拟机模型时将它们删除。因此，这些模型的自定义或历史详细信息将保留，并在移动后可用。

2. 使用 Huawei SingleCLOUD GalaX 删除对主机的管理。
3. 在“导航”面板中，等待 Virtual Host Manager 反映这些更改。
4. 使用目标 Huawei SingleCLOUD GalaX 添加对主机的管理。

   注意：Virtual Host Manager 无法识别 DSS (请参阅本页中的定义 255)。因此，将主机移至在其他 SpectroSERVER 上管理的 Huawei SingleCLOUD GalaX 时，将创建一组新模型以表示主机、CNA FIP 和虚拟机。

5. （可选）将“允许在运行 Huawei SingleCLOUD 发现期间删除设备模型”选项更改回“是” (p. 217)。

   该主机将成功从一个 Huawei SingleCLOUD GalaX 的管理移至另一个相应管理，并在 CA Spectrum 建模环境中得到准确反映。

查看 Huawei SingleCLOUD 虚拟环境

本节介绍用于查看 Huawei SingleCLOUD 虚拟环境的概念。基本步骤与标准 CA Spectrum 步骤相同。但是，本节介绍仅适用于 Huawei SingleCLOUD 平台的概念差异和详细信息。

详细信息：

查看 Huawei SingleCLOUD 虚拟网络

在“资源管理器”选项卡上的 Virtual Host Manager 节点下，展开的 Huawei SingleCLOUD 文件夹显示分层树结构，可帮助您可视化托管 Huawei SingleCLOUD 环境的逻辑组织。

使用此信息，可以查看如何在 Huawei SingleCLOUD Manager 中共享资源，从而帮助您发现机会以重新组织和优化虚拟环境。通过此层次结构，还可以快速验证云体系结构中已分配资源的相应状态，监控性能以及排除警报故障。

由于 Virtual Host Manager 无法识别 DSS 环境 (请参阅本页中的定义 255)，因此它位于格局层次结构中。下图显示了 Virtual Host Manager 在“导航”面板中“资源管理器”选项卡上的位置，并演示了 Huawei SingleCLOUD 的层次结构：

```
[-] SpectroSERVER 主机
    [+] Universe
    [-] Virtual Host Manager
        [-] Huawei SingleCLOUD
            [+] Huawei SingleCLOUD CAMM 展示器 1
            [-] Huawei SingleCLOUD CAMM 展示器 2
                [-] Huawei SingleCLOUD Manager 1
                     [+] Huawei SingleCLOUD 云 1
                     [-] Huawei SingleCLOUD 云 2
                         [+] Huawei SingleCLOUD 主机 1
                         [-] Huawei SingleCLOUD 主机 2
                             . Huawei SingleCLOUD CNA FIP
                             . Huawei SingleCLOUD 虚拟机 1
                             . Huawei SingleCLOUD 虚拟机 2
                [+] Huawei SingleCLOUD Manager 2
                [+] Huawei SingleCLOUD Manager 3
```

Virtual Host Manager 是由此 SpectroSERVER 管理的整个虚拟环境的根节点。在“导航”面板中选择此节点后，将在“内容”面板中显示 Virtual Host Manager 详细信息。您可以查看与整体虚拟环境相关的事件和警报等详细信息。

虚拟环境将直接在 Virtual Host Manager 下表示用于创建这些虚拟环境的技术的文件夹中进行组织。在上面的示例层次结构中，Huawei SingleCLOUD 文件夹包含由 Huawei SingleCLOUD 创建和管理的虚拟环境部分。在此文件夹中，Virtual Host Manager 列出了由此 SpectroSERVER 管理的所有 CAMM 展示器、Huawei SingleCLOUD Manager 和云。每个 Huawei SingleCLOUD Manager 仅包含它管理的虚拟环境部分。

层次结构表示下列虚拟实体之间的逻辑关联关系：

- **Huawei SingleCLOUD CAMM 展示器**

  Huawei SingleCLOUD CAMM 展示器节点将它管理的所有 Huawei SingleCLOUD Manager 分组在一起。选择 CAMM 展示器可提供对 Huawei SingleCLOUD Manager 子视图的访问，通过指定用来与 Huawei SingleCLOUD GalaX 进行通信的虚拟 IP 地址，可以在该子视图中定义由展示器管理的 Huawei SingleCLOUD Manager。选择 CAMM 展示器节点还将显示与其托管环境中的实体相关的事件和警报。在 Huawei SingleCLOUD CAMM 展示器模型上生成的“物理主机关闭”警报表示，它管理的所有 Huawei SingleCLOUD Manager（虚拟 IP 地址）都已关闭。

- **Huawei SingleCLOUD Manager**

  Huawei SingleCLOUD Manager 表示 CAMM 用来与 Huawei SingleCLOUD GalaX 进行通信的虚拟 IP 地址。CA Spectrum 使用虚拟 IP 地址从 Huawei SingleCLOUD GalaX 获取有关它管理的 Huawei SingleCLOUD 环境的信息。选择 Huawei SingleCLOUD Manager 将显示有关其托管环境的信息，如有关 GalaX OMM、托管云、主机和虚拟机的详细信息，包括上次更新 MIB 中数据的时间。将在 Huawei SingleCLOUD Manager 模型上生成从 Huawei SingleCLOUD 陷阱服务接收到的陷阱。

- **Huawei SingleCLOUD 云**

  Huawei SingleCLOUD 云是在 Huawei SingleCLOUD 平台中定义的托管云的名称。选择 Huawei SingleCLOUD 云将显示有关云的详细信息，包括：

  - 云类型（公共或专用）。
  - 与 MIB 相关的状态信息，包括上次更新云的数据的时间以及预期的更新间隔。

  在层次结构中，每个云的下面是与云关联的 Huawei SingleCLOUD 主机。

- **Huawei SingleCLOUD 主机**

  Huawei SingleCLOUD 主机是承载虚拟机的 CNA。在层次结构中，每个主机的下面是它管理的 CNA FIP 和虚拟机。Huawei SingleCLOUD 主机可以是公共或专用云的一部分。

  选择 Huawei SingleCLOUD 主机将显示详细的主机信息，包括：

  - 主机所属的云类型（公共或专用）。
  - CNA 进程占用的资源，如存储、CPU 和内存利用率。
  - 用于故障解决期间快速物理定位的主机的地理信息。
  - 与 MIB 相关的状态信息，包括上次更新主机的数据的时间以及预期的更新间隔。

  注意：根据主机属于公共云还是专用云，可用的主机信息有所不同。可在“主机信息”、“CNA”、“属性”子视图中确定云类型。

- **Huawei SingleCLOUD CNA FIP**

  Huawei SingleCLOUD CNA FIP 是所承载虚拟机的管理接口。该模型显示为其相应 Huawei SingleCLOUD 主机模型的子项，并且始终为 Virtual Host Manager 层次结构树中的叶节点。

  注意：Huawei SingleCLOUD CNA FIP 模型是“信息”选项卡上不提供 Virtual Host Manager 特定的子视图的唯一 Huawei SingleCLOUD 模型类型。

- **Huawei SingleCLOUD 虚拟机**

  虚拟机始终为 Virtual Host Manager 层次结构树中的叶节点。选择虚拟机将显示相关详细信息，包括：

  - 标识信息，如 IP 地址和 MAC 地址。
  - 资源信息，包括存储、CPU 和内存利用率。
  - 与 MIB 相关的状态信息，包括上次更新虚拟机的数据的时间以及预期的更新间隔。

详细信息：

为 Huawei SingleCLOUD 创建的模型 (p. 212)
CAMM MIB 更新 (p. 233)

了解 Huawei SingleCLOUD 虚拟拓扑

为虚拟环境创建的 Huawei SingleCLOUD 主机、CNA FIP 和虚拟机模型将集成到拓扑视图中。Huawei SingleCLOUD 主机模型会自动分组其关联的 CNA FIP 和虚拟机模型。拓扑将显示这些元素如何连接到物理网络实体。

下列示例显示了这些模型在“导航”面板的“资源管理器”选项卡中 Universe 组下的显示方式：

```
[-] Universe
    [-] Huawei SingleCLOUD 主机
          . Huawei SingleCLOUD CNA FIP
          . Huawei SingleCLOUD 虚拟机 1
          . Huawei SingleCLOUD 虚拟机 2
          . Huawei SingleCLOUD 虚拟机 3
```

选择这些模型之一后，将在“内容”面板的“拓扑”选项卡上以图形方式显示这些关联关系。

Virtual Host Manager 中的 Huawei SingleCLOUD 数据更新方式

在初始 Huawei SingleCLOUD 发现期间，CA Spectrum 将使用您的虚拟设备模型填充“导航”面板中的 Virtual Host Manager 层次结构。在 CA Spectrum 构建此初始层次结构后，您的虚拟网络配置可能会发生更改，Virtual Host Manager 必须持续工作以保持此信息在 CA Spectrum 中的准确性。例如，以下事件可能会更改虚拟网络配置：

- 创建或删除云、主机或虚拟机
- 手动将虚拟机从一个 Huawei SingleCLOUD 主机移至另一个 Huawei SingleCLOUD 主机

为了保持信息准确，Virtual Host Manager 通过轮询 CAMM 展示器以从 CAMM MIB 检索有关虚拟环境的信息来检测这些更改。因此，将于每个轮询周期在 CA Spectrum 中更新您的虚拟网络配置。由于与 Huawei SingleCLOUD GalaX 进行通信，CA Spectrum 可发现自发的网络配置更改（如迁移和主机停机），这些更改将快速反映到 OneClick 中，并用于分析根本原因。

在检测到虚拟网络配置中的更改时，CA Spectrum 将执行以下任务：

- 在“导航”面板的 Virtual Host Manager 层次结构中，更新虚拟设备模型的放置
- *自动*重新发现与受影响的模型的连接，并将它们与 Universe 拓扑中的正确 Huawei SingleCLOUD 主机关联。

  重要说明！要正确重建与虚拟模型的连接，必须为物理网络中的所有互连路由器和交换机建模。如果在重新发现与虚拟设备的连接之前这些模型不存在，则 CA Spectrum 无法在 Universe 拓扑视图中解析这些连接并正确显示相关信息。

除了基于轮询的事件外，CA Spectrum 还支持来自 Huawei SingleCLOUD 陷阱服务的陷阱并生成相应的事件。通过查看事件日志，可以查明配置发生更改的时间（例如创建或迁移虚拟机的时间）。

详细信息：

CAMM MIB 更新 (p. 233)

CAMM MIB 更新

CA Spectrum 从 CAMM MIB 检索有关 Huawei SingleCLOUD 环境的信息。为了保持 CA Spectrum 中的建模准确，MIB 中的数据必须是最新的。

CAMM 从 Huawei SingleCLOUD GalaX 获取数据，并根据 CAMM 引擎中已配置的轮询速率来更新 MIB。CA Spectrum 根据在 Huawei SingleCLOUD Manager 模型上指定的轮询时间间隔使用 SNMP 从 MIB 检索数据。

通过使用各种 Huawei SingleCLOUD 实体模型的自定义子视图，可以确定上次更新 CAMM 的时间和重新更新它的预期时间，这些子视图中提供了与 MIB 相关的以下状态信息字段：

上次更新时间

显示上次更新 MIB 的时间。从 Huawei SingleCLOUD GalaX 获取有关相应实体的信息时，CAMM 将更新此时间戳值。可以使用此值来确定实体的 MIB 信息的更新程度。

预期的更新增量

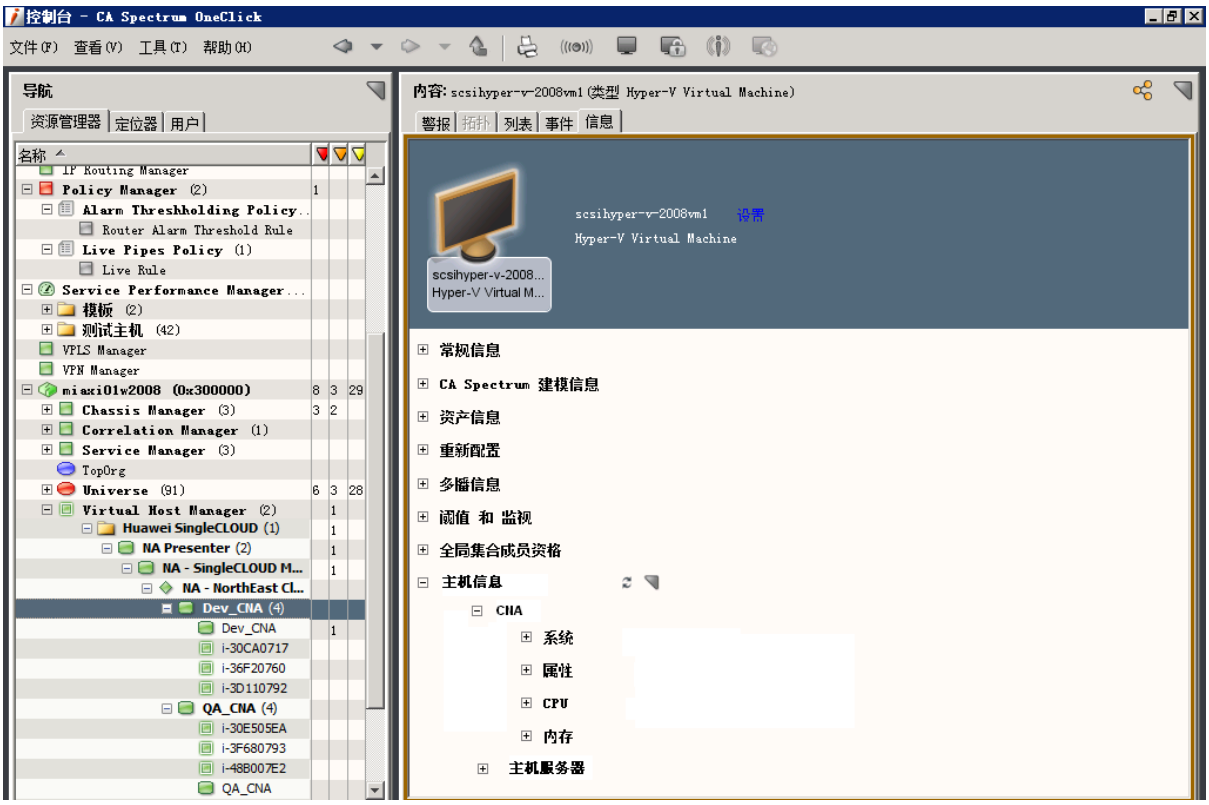
显示 MIB 更新之间的预期时长（以秒为单位）。如果在预期的时间内未更新主机或虚拟机，则将生成“代理已丢失”警报，以表示无法获取实体的已更新信息。

详细信息：

Virtual Host Manager 如何使用 Huawei SingleCLOUD (p. 211)
查看 Huawei SingleCLOUD 虚拟环境 (p. 229)
丢失代理管理时故障隔离的工作方式 (p. 243)

自定义子视图

您的各个 Virtual Host Manager 模型将共同提供有关虚拟环境的信息。每个模型将单独提供特定的信息或配置设置，具体取决于其表示的虚拟实体类型。自定义子视图显示在“内容”面板中的“信息”选项卡上。这些子视图可包含实时数据，例如 CPU 状态或内存利用率。例如，针对 Huawei SingleCLOUD 主机模型的自定义子视图是“主机信息”子视图，该子视图提供特定于主机的详细信息，如下所示：



注意：Huawei SingleCLOUD Manager 模型提供由 Huawei SingleCLOUD Manager 管理的所有虚拟设备的组合信息。在“导航”面板中选择 Huawei SingleCLOUD Manager 模型后，将显示有关 Huawei SingleCLOUD GalaX OMM 的唯一信息，以及有关它管理的所有 Huawei SingleCLOUD 云、主机和虚拟机的组合信息。此信息包含在每个单独实体模型的“信息”选项卡上显示的一些相同数据。Huawei SingleCLOUD Manager 模型中的组合视图可以很好地概述它管理的所有虚拟实体。

用于 Huawei SingleCLOUD 搜索的定位器选项卡

除了在“资源管理器”选项卡上查看有关虚拟环境的详细信息外，还可以使用“定位器”选项卡运行预配置的搜索。搜索选项在“定位器”选项卡中的“虚拟主机管理”->“Huawei SingleCLOUD”文件夹下进行分组，如下所示：

这些详细搜索可以帮助您调查与 CA Spectrum 数据库中已建模的 Huawei SingleCLOUD 实体相关的信息。

注意：虽然 Virtual Host Manager 无法识别 DSS (请参阅本页中的定义 255)，但是这些预配置搜索允许您在搜索参数中选择多个要搜索的格局。

为 Huawei SingleCLOUD 提供了以下类型的搜索：

Huawei SingleCLOUD

按模型类型查找 CA Spectrum 数据库中已建模的 Huawei SingleCLOUD 实体。这些模块包括：

- 所有云
- 所有 CNA FIP
- 所有主机
- 所有管理器
- 所有展示器
- 所有虚拟机

主机

按云名称或地理位置（机架、地区、房间和区域）查找 Huawei SingleCLOUD 主机。

虚拟机

查找驻留在特定 Huawei SingleCLOUD 主机上的所有虚拟机。

删除 Virtual Host Manager 模型

可以随时出于各种原因从 OneClick 中删除模型。但是，Virtual Host Manager 会限制您在“导航”面板的 Virtual Host Manager 层次结构中删除模型的能力。要手动删除模型，可使用以下选项：

- 在 Virtual Host Manager 中删除 Huawei SingleCLOUD 文件夹、Huawei SingleCLOUD 展示器模型或 Huawei SingleCLOUD Manager 模型
- 使用 Huawei SingleCLOUD GalaX 删除虚拟实体

在 Virtual Host Manager 中，有时会自动删除模型。下列情况会导致 CA Spectrum 自动删除 Virtual Host Manager 模型：

- **删除 Huawei SingleCLOUD 文件夹、Huawei SingleCLOUD CAMM 展示器模型或 Huawei SingleCLOUD Manager 模型**

  如果从“导航”面板中删除 Huawei SingleCLOUD 文件夹、Huawei SingleCLOUD CAMM 展示器模型或 Huawei SingleCLOUD Manager 模型，CA Spectrum 将会删除所有相关的子模型。对于 CAMM 展示器模型，这包括所有的虚拟 IP 地址。

- **从 Huawei SingleCLOUD 虚拟环境中删除实体**

  使用 Huawei SingleCLOUD GalaX 删除 Huawei SingleCLOUD 主机和虚拟机时，CA Spectrum 还会从 Virtual Host Manager 中删除这些模型及其子模型。

- **存在已升级模型。**

  在某些情况下，会首先为无 SNMP 功能的 Virtual Host Manager 建模虚拟机。如果以后向 VHM 模型 (请参阅本页中的定义 255)添加 SNMP 功能，则之前的模型将被删除，并替换为支持 SNMP 的新模型。

注意：虽然默认设置是删除模型，但是您可以配置 Virtual Host Manager，以便在从 Virtual Host Manager 中删除 Huawei SingleCLOUD 主机和 Huawei SingleCLOUD 虚拟机模型时将它们放置在 LostFound 容器中。仅当使用 Huawei SingleCLOUD GalaX 删除实体时，才会应用此配置设置。但是，在删除 Huawei SingleCLOUD 文件夹、删除 Huawei SingleCLOUD Manager 模型或升级 VHM 模型时，不会应用此设置。

Huawei SingleCLOUD 的警报和故障隔离

为了就虚拟网络中出现的问题向您报警，CA Spectrum 将生成警报。快速确认任何设备故障有助于最大限度地提高系统运行时间和云体系结构的可靠性。将通过以下方式创建警报：

- 从 Huawei SingleCLOUD 发送的陷阱 (p. 238)。
- 轮询。将针对以下条件生成警报：
  - Huawei SingleCLOUD Manager（代理）已关闭或者通信已丢失。
  - Huawei SingleCLOUD 虚拟机未运行。
  - 在定义的轮询速率内未更新 CAMM。
  - 虚拟机已移至新的 Huawei SingleCLOUD 主机。
  - 已遇到不支持的 Virtual Host Manager 配置。

  通过轮询生成的警报会在 Huawei SingleCLOUD 的故障管理 (p. 239)中进行介绍。

Huawei SingleCLOUD 的陷阱

陷阱由 Huawei SingleCLOUD 陷阱服务生成，标识与配置更改、进程状态、磁盘或内存使用率以及电源或风扇状态等相关的事件。陷阱在 Huawei SingleCLOUD Manager 模型上生成，并可以在 CA Spectrum 中生成警报。

本节包括以下主题：

Huawei SingleCLOUD 的陷阱和警报重要级别

如果接收到陷阱并生成警报，CA Spectrum 将使用通过陷阱传递的“状态”varbind 的值来确定警报重要级别。CA Spectrum 将这些 Huawei SingleCLOUD 状态映射到 CA Spectrum 警报重要级别，如下所示：

Huawei SingleCLOUD 状态	CA Spectrum 警报重要级别
0：警告	次要（黄色）
1：次要	次要（黄色）
2：主要	主要（橙色）
3：关键	关键（红色）

支持的 Huawei SingleCLOUD 陷阱

下表提供支持的 Huawei SingleCLOUD 陷阱及其各自的陷阱类型。OID 后缀（陷阱 OID 中的最低节点）的值表示陷阱类型。

Huawei SingleCLOUD 陷阱类型

OID 后缀	陷阱类型
.1	设置
.2	Update
.3	清除

Huawei SingleCLOUD 陷阱

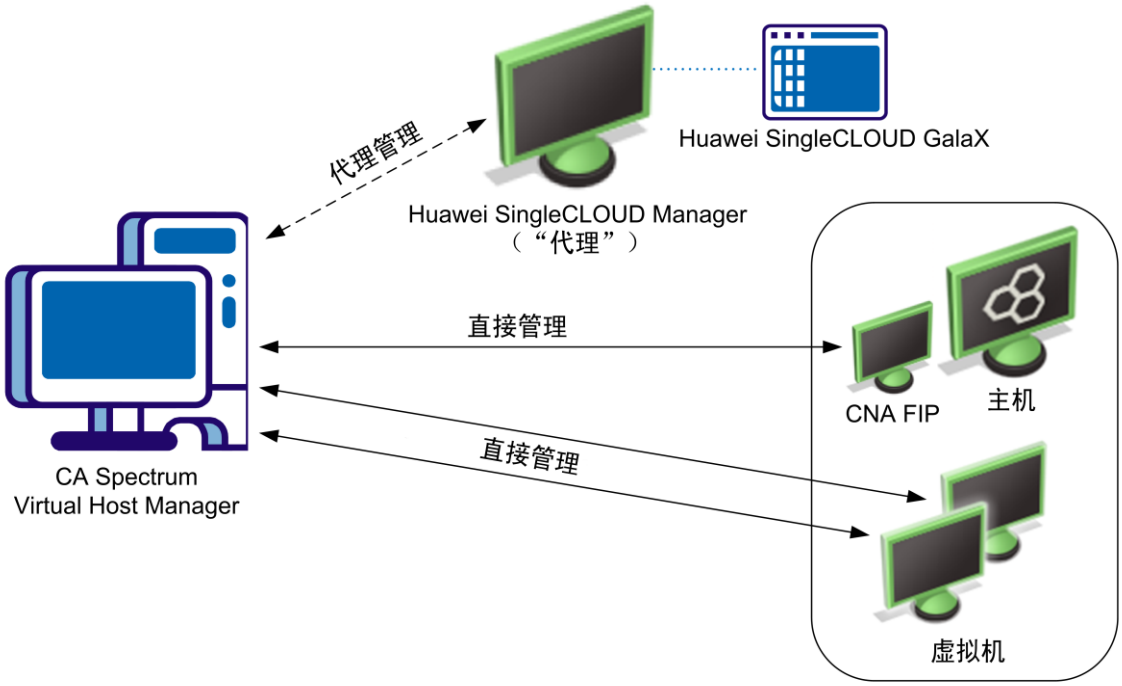
陷阱名称	陷阱 OID
配置管理代理进程异常	1.3.6.1.4.1.60001.10.1.10.1000001.6.1 1.3.6.1.4.1.60001.10.1.10.1000001.6.2 1.3.6.1.4.1.60001.10.1.10.1000001.6.3
目录中的已占用空间太大	1.3.6.1.4.1.60001.10.1.15.1000203.6.1 1.3.6.1.4.1.60001.10.1.15.1000203.6.2 1.3.6.1.4.1.60001.10.1.15.1000203.6.3
CNA 节点磁盘使用率已超过阈值	1.3.6.1.4.1.60001.10.1.15.1000036.6.1 1.3.6.1.4.1.60001.10.1.15.1000036.6.2 1.3.6.1.4.1.60001.10.1.15.1000036.6.3
硬盘丢失	1.3.6.1.4.1.60001.10.1.15.1000202.6.1 1.3.6.1.4.1.60001.10.1.15.1000202.6.2 1.3.6.1.4.1.60001.10.1.15.1000202.6.3
VM MEM 使用率已超过阈值	1.3.6.1.4.1.60001.10.1.15.1000102.6.1 1.3.6.1.4.1.60001.10.1.15.1000102.6.2 1.3.6.1.4.1.60001.10.1.15.1000102.6.3
风扇状态异常	1.3.6.1.4.1.60001.10.1.15.1000017.6.1 1.3.6.1.4.1.60001.10.1.15.1000017.6.2 1.3.6.1.4.1.60001.10.1.15.1000017.6.3
控制器节点硬盘使用率已超过阈值	1.3.6.1.4.1.60001.10.1.15.1000015.6.1 1.3.6.1.4.1.60001.10.1.15.1000015.6.2 1.3.6.1.4.1.60001.10.1.15.1000015.6.3
电源处于异常状态	1.3.6.1.4.1.60001.10.1.15.1000016.6.1 1.3.6.1.4.1.60001.10.1.15.1000016.6.2 1.3.6.1.4.1.60001.10.1.15.1000016.6.3

Huawei SingleCLOUD 的故障管理

故障隔离旨在缩小导致网络问题的根本原因的范围。通过查找根本原因，可以帮助您排除故障并快速更正问题，或使用自动化脚本以编程方式更正问题。确定哪些设备是导致警报的根本原因可能非常困难，因为单个设备中的问题会导致网络中的多个设备生成事件。

例如，与 Huawei SingleCLOUD 主机失去联系通常意味着也会与其管理的虚拟机失去联系。因此，Huawei SingleCLOUD 主机模型和所有受影响的虚拟机都将生成警报。通过使用故障隔离技术，Virtual Host Manager 将关联这些警报以尝试确定单个根本原因。

虚拟网络可提供独特的管理机会，因为它们针对 CA Spectrum 提供了备用管理视角。也就是说，CA Spectrum 可以通过与虚拟设备直接联系或者通过与 Huawei SingleCLOUD GalaX 进行通信的 CAMM 来收集信息。



这种备用管理视角可通过两种方式来增强标准 CA Spectrum 故障管理：

- **增强失去联系警报** - 两个设备信息源可帮助 Virtual Host Manager 查明原因，并更轻松地将事件与单个根本原因关联。
- **代理故障警报** - 代理管理是指使用备用管理源（代替主要管理器或与主要管理器一起）来管理网络设备的行为。例如，CA Spectrum 可通过直接与 Huawei SingleCLOUD 虚拟机联系或通过 CAMM（它从 Huawei SingleCLOUD GalaX 获取数据）来管理这些虚拟机。当 Huawei SingleCLOUD Manager 与 Huawei SingleCLOUD GalaX 失去联系时，或者 Huawei SingleCLOUD GalaX 与虚拟设备失去联系时，Virtual Host Manager 将为每个设备生成一个代理管理警报。这些警报提醒您通过 *代理*对设备执行的 *管理*（而不是设备或直接 (SNMP) 管理的状态）受到影响。

以下各节提供有关与设备或代理失去联系时可能出现的情况的其他信息。

详细信息：

丢失设备联系时故障隔离的工作方式 (p. 241)
丢失代理管理时故障隔离的工作方式 (p. 243)

丢失设备联系时故障隔离的工作方式

为了帮助您排除设备中的网络问题，CA Spectrum 使用故障隔离来缩小警报根本原因的范围。对于虚拟网络，Virtual Host Manager 将使用通过与设备直接联系获取的信息，以及由 Huawei SingleCLOUD GalaX 通过 CAMM 提供的信息。在许多情况下，标准 CA Spectrum 故障管理可以查明根本原因。但是在一些特殊情况下，无法使用标准方法来隔离虚拟网络中的问题。

Virtual Host Manager 用于发现根本原因的故障隔离类型取决于生成警报的设备，以及设备生成的事件类型。下列方案介绍了故障管理情况，以及 CA Spectrum 如何确定虚拟网络中的网络错误。

方案 1：Huawei SingleCLOUD 虚拟机未运行

在虚拟环境中，与 CA Spectrum 通过标准设备监控发现的信息相比，虚拟管理应用程序可以提供更多的详细信息。例如，Huawei SingleCLOUD GalaX 可发现虚拟机何时从“正在运行”状态更改为其他状态。

如果虚拟机不再运行，并且 CA Spectrum 与其失去联系，但是虚拟机的代理管理 (请参阅本页中的定义 255)未中断，则 CA Spectrum 将按如下所示确定根本原因：

1. 当 CA Spectrum 与虚拟机失去联系时，将生成“失去联系”警报。
2. 在其下一个轮询周期内，Huawei SingleCLOUD Manager 模型将轮询与 Huawei SingleCLOUD GalaX 进行通信的 CAMM 来收集有关虚拟机的信息。由于 Huawei SingleCLOUD GalaX 管理虚拟机，因此它可提供导致虚拟机所生成警报的可能原因的相关信息。
3. 如果 Huawei SingleCLOUD GalaX 指出虚拟机处于未运行模式，它将生成“Huawei SingleCLOUD 未运行”警报。

   注意：在 CAMM 于其后确定虚拟机重新运行的轮询周期内，将清除此警报。
4. Virtual Host Manager 将“失去联系”警报与 CA Spectrum 所创建的相应“Huawei SingleCLOUD 未运行”警报关联。Virtual Host Manager 使“失去联系”警报显示为“Huawei SingleCLOUD 未运行”警报的症状。

方案 2：Huawei SingleCLOUD 主机关闭

如果 CA Spectrum 与 Huawei SingleCLOUD 主机上运行的所有虚拟机失去联系，它将检查上游路由器和交换机的状态。根据它们的状态，CA Spectrum 将按如下所示确定根本原因：

- **一个或多个 Huawei SingleCLOUD 虚拟机的所有上游设备都不可用时**

  使用标准 CA Spectrum 故障隔离技术确定根本原因：

  - *当所有*上游连接设备都关闭时，在 Huawei SingleCLOUD 主机上生成“网关不可访问”警报。

- **至少一个上游设备可用于连接到 Huawei SingleCLOUD 主机的每个虚拟机时**

  CA Spectrum 推断 Huawei SingleCLOUD 主机是根本原因，并按如下所示进行响应：

  a. 直接连接到 Huawei SingleCLOUD 主机模型的所有 Huawei SingleCLOUD 虚拟机、端口和扇出将生成标准故障隔离警报。

  b. Virtual Host Manager 为 Huawei SingleCLOUD 主机模型创建“物理主机关闭”警报。

  c. 为受影响设备（如虚拟机、端口和扇出）创建的所有故障隔离相关警报将关联到“物理主机关闭”警报，从而使它们成为“物理主机关闭”警报的症状。这些症状警报显示在“物理主机关闭”警报的“影响”选项卡上的“症状”表中。

     注意：对于每个 Huawei SingleCLOUD 主机模型，Virtual Host Manager 将创建一个“虚拟故障域”。此域中包括 Huawei SingleCLOUD 主机、CNA FIP 和虚拟机，以及直接连接到 Huawei SingleCLOUD 主机的所有端口和扇出。当 Huawei SingleCLOUD 主机生成“物理主机关闭”警报时，域中的所有标准故障隔离警报将与其关联。将这些警报作为症状关联可表明 Huawei SingleCLOUD 主机上的“物理主机关闭”警报是根本原因。

  d. “影响”选项卡上针对“物理主机关闭”警报的“失去管理的影响”表中列出了所有受影响设备。

     注意：被抑制的设备在“症状”表中没有对应的警报。

     有关使用“影响”选项卡以了解警报信息的详细信息，请参阅确定受主机停机影响的虚拟机 (p. 245)。

  e. 如果一个或多个虚拟机的所有上游设备都已关闭，则 CA Spectrum 无法再可靠地指出故障出自 Huawei SingleCLOUD 主机。CA Spectrum 将清除“物理主机关闭”警报，并应用标准 CA Spectrum 故障隔离技术。

丢失代理管理时故障隔离的工作方式

用于创建虚拟网络的 Huawei SingleCLOUD GalaX 为 CA Spectrum 提供了独特的管理机会。CA Spectrum 可以使用标准方法来直接联系您的虚拟设备，此外，CA Spectrum 可以同时从与 Huawei SingleCLOUD GalaX 进行通信的具有 Huawei SingleCLOUD 设备包的 CAMM 中收集虚拟设备信息。从这个意义上讲，CAMM 是 CA Spectrum 可从其收集虚拟设备信息的“代理”。如果 CA Spectrum 与设备失去直接联系，则将生成警报。同样，如果 CAMM 与虚拟设备失去联系（经由 Huawei SingleCLOUD GalaX 联系），或者如果 Virtual Host Manager 与 CAMM 失去联系，Virtual Host Manager 将生成警报 - 代理管理警报 (请参阅本页中的定义 255)。

作为响应，CA Spectrum 将尝试隔离导致代理管理故障的原因。代理故障隔离类似于标准 CA Spectrum 故障隔离，不过，这些警报将提醒您虚拟设备的*代理*管理会受到影响。代理管理故障隔离无法指明虚拟设备是已启动还是已关闭。但是，了解何时失去通过代理进行的联系非常重要，因为您可能会丢失设备的重要虚拟信息。

Virtual Host Manager 用于发现根本原因的代理故障隔离类型取决于生成警报的设备，以及设备生成的事件类型。下列方案介绍了代理故障管理情况，以及 Virtual Host Manager 如何确定虚拟网络中的网络错误。

方案 1：CA Spectrum 与 CAMM (Huawei SingleCLOUD Manager) 之间失去联系

如果 CA Spectrum 与 Huawei SingleCLOUD Manager 模型失去联系或停止轮询该模型，则 CA Spectrum 无法获取该 Huawei SingleCLOUD Manager 管理的所有虚拟模型的已更新 Huawei SingleCLOUD GalaX 数据。为了隔离该问题，Virtual Host Manager 将按如下所示确定根本原因：

1. CA Spectrum 将为该 Huawei SingleCLOUD Manager 管理的所有虚拟模型（包括 Huawei SingleCLOUD 云、主机、CNA FIP 和虚拟机）生成“代理已丢失”警报。CA Spectrum 还将在 Huawei SingleCLOUD Manager 模型上生成单独的“代理不可用”警报。
2. Huawei SingleCLOUD 警报将与其相应的 Huawei SingleCLOUD 主机模型警报关联。

3. Huawei SingleCLOUD 云和主机模型警报将与 Huawei SingleCLOUD Manager 模型的“代理不可用”警报关联。
4. 然后，此“代理不可用”警报将与正关闭的 Huawei SingleCLOUD Manager 的根本原因关联。根本原因通常是由标准 CA Spectrum 故障管理生成的警报，例如为下列情况创建的警报：
   - 失去 Huawei SingleCLOUD Manager 的管理（即，CAMM 发生问题）
   - 失去计算机联系
   - Huawei SingleCLOUD Manager 模型处于维护模式

方案 2：CAMM 与 Huawei SingleCLOUD GalaX 之间失去联系

如果 CAMM 未在特定的时间内更新，则 CAMM 报告的 Huawei SingleCLOUD 平台数据可能不是最新的。使用检测信号指示器和已配置的轮询速率，CA Spectrum 可以确定托管 Huawei SingleCLOUD 实体上次更新的时间。

未在配置的时间内更新 Huawei SingleCLOUD 主机或虚拟机时，Virtual Host Manager 将确定 CAMM 无法联系 Huawei SingleCLOUD GalaX。将在此 Huawei SingleCLOUD Manager 管理的 Huawei SingleCLOUD 主机、CNA FIP 和虚拟机模型上生成“代理已丢失”警报。未更新多个元素时，CA Spectrum 会将这些警报与相应的根本原因关联（例如，与主机关联的多个虚拟机警报）。此外，无法联系与 CAMM 展示器关联的任何虚拟 IP 时，将在 Huawei SingleCLOUD CAMM 展示器模型上生成“物理主机关闭”警报。在警报文本中提供了故障 CAMM 引擎的标识信息和自上次成功通信以来的时间。

方案 3：Huawei SingleCLOUD GalaX 与 Huawei SingleCLOUD 主机之间失去联系

如果 Huawei SingleCLOUD GalaX 与其管理的一个 Huawei SingleCLOUD 主机失去联系，则有关该主机和承载的所有虚拟设备的代理数据将丢失。为了隔离该问题，Virtual Host Manager 将按如下所示确定根本原因：

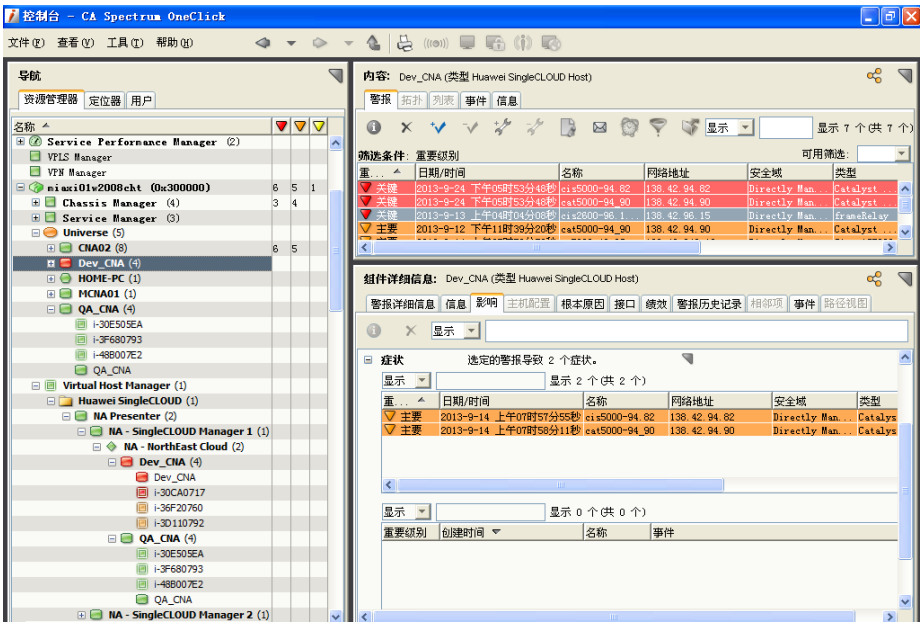
1. 将在 Huawei SingleCLOUD 主机、CNA FIP 和承载的所有虚拟机上生成“代理已丢失”警报。
2. CNA FIP 和虚拟机警报将与 Huawei SingleCLOUD 主机的“代理已丢失”警报关联，使这些警报成为 Huawei SingleCLOUD 主机警报的症状。将这些警报作为症状关联可表明 Huawei SingleCLOUD 主机警报是根本原因。
3. 如果 CA Spectrum 也与 Huawei SingleCLOUD 主机失去联系并生成“物理主机关闭”警报，则为 Huawei SingleCLOUD 主机生成的“代理已丢失”警报将与“物理主机关闭”警报关联。在这种情况下，“代理已丢失”警报成为“物理主机关闭”警报的症状。将此警报作为症状关联可表明 Huawei SingleCLOUD 主机上的“物理主机关闭”警报是根本原因。

确定受主机停机影响的虚拟机

当与 Huawei SingleCLOUD 主机的联系中断或者 Huawei SingleCLOUD 主机关闭时，该 Huawei SingleCLOUD 主机承载的所有虚拟机都将受到影响。由于 Huawei SingleCLOUD Manager 无法与 Huawei SingleCLOUD 主机进行通信以获取使用情况信息，因此您可能不会接收到该 Huawei SingleCLOUD 主机上承载的关键虚拟机的警报。

要确定关键虚拟机是否受到影响，可以在警报的“影响”选项卡上查看受影响虚拟机的列表，如下所示：

- “症状”子视图 - 显示受影响的虚拟机生成的所有症状警报
- “失去管理的影响”子视图 - 列出受警报影响的虚拟机



附录 A： 故障排除

本节介绍在使用 Virtual Host Manager 时可能发生的常见症状或问题，以及建议的解决方案。

在 SNMP 和 vCenter 发现进程后创建的重复模型

症状：

我在虚拟网络上运行标准 CA Spectrum 发现并让 Virtual Host Manager 运行 vCenter 发现之后，收到与某些虚拟机相关的“重复模型”警报。我应删除哪个模型，以及如何防止再次发生该问题？

解决方案：

在为虚拟环境建模时，如果虚拟机未安装 VMware 工具或 SNMP 代理，则可能会创建重复的模型。重复模型的创建过程如下所示：

1. 由于虚拟机未安装 SNMP 代理，CA Spectrum 发现将使用 Pingable 模型类型为虚拟机建模。此模型包含 IP 地址，但不包含 MAC 地址。由于尚未为通常负责查找设备 MAC 地址的上游路由器建模，因此虚拟机的 MAC 地址得不到解析。
2. Virtual Host Manager 运行 vCenter 发现并找到相同的虚拟机。由于虚拟机未安装 VMware 工具，所以发现进程可以识别 MAC 地址，但无法确定 IP 地址。因此，vCenter 发现无法将其识别为在步骤 1 中创建的现有模型，它会为该虚拟机创建第二个模型。此模型包含 MAC 地址，但不包含 IP 地址。
3. 当 CA Spectrum 找到没有 IP 地址的模型时，它将使用模型名称执行操作系统调用以获取 IP 地址。如果 vCenter 中的虚拟机名称与操作系统返回的名称匹配，操作系统就会把虚拟机设备的 IP 地址传递给 CA Spectrum。CA Spectrum 在 vCenter 发现所创建的模型中设置 IP 地址 - 现在此模型同时包含 MAC 地址和 IP 地址。
4. 将为每个模型触发“重复模型”警报，因为它们具有相同的 IP 地址。

要更正该问题，请删除 CA Spectrum 发现所创建的虚拟机设备模型（即，仅包含 IP 地址的模型）- *保留既有 IP 地址又有 MAC 地址的模型*。否则，将在下一个 vCenter 轮询周期中发生相同的问题。如果删除操作将影响 Virtual Host Manager 层次结构，请等待至下一次 vCenter Server 主机轮询周期，届时建模将被还原。

为避免在使用 CA Spectrum 发现为虚拟环境建模时发生此问题，请验证没有 VMware 工具的所有虚拟机的上游路由器是否满足下列标准之一：

- 已使用支持 SNMP 的模型类型为路由器建模
- 路由器连同适当的 SNMP 凭据一起包含在您的发现范围内

通过包括上游路由器，CA Spectrum 将尝试解析属于没有 SNMP 代理的每个主机的物理地址。

如果通过按 IP 地址为 VMware vCenter Server 建模来为您的虚拟环境建模，并且发现进程创建了没有 IP 地址的模型，则必须首先为这些设备手动指定 IP，然后再运行 CA Spectrum 发现。

在 Solaris Zones 发现后创建了重复模型

症状：

我在虚拟网络上运行标准 CA Spectrum 发现并使 Virtual Host Manager 运行 Solaris Zones 发现之后，得到针对某些设备模型的“重复模型”警报。我应删除哪个模型，以及如何防止再次发生该问题？

解决方案：

在建模 Solaris Zones 虚拟环境时，如果多个虚拟技术管理器实例在管理某个设备模型，则可能会创建重复的模型。例如，如果 vCenter Server 和 Solaris Zones Manager 都在管理某个设备，则 CA Spectrum 将创建重复的模型。

要更正此问题，请确认您的 SpectroSERVER 环境中只有一个虚拟技术管理器正在管理该设备。

详细信息：

删除 Virtual Host Manager 模型 (p. 108)

在 Solaris Zones 模型上生成了重复的 MAC、不同的 IP 地址警报

症状：

CA Spectrum 为我的一些 Solaris Zones 主机和 Solaris 区域实例生成“重复的 MAC、不同的 IP 地址”警报。我的 Solaris Zones 技术环境中的许多虚拟和物理 NIC 共享相同的 MAC 地址。为什么我仅收到其中一些设备的警报，我该如何禁用这些警报？

解决方案：

在 Solaris Zones 虚拟环境中，可能会经常发生共享 MAC 地址的情况。因此，CA Spectrum 智能将为 Virtual Host Manager 管理的设备抑制这些警报，但是仍然会记录事件。在下列情况下，CA Spectrum 会在 Solaris Zones 主机和 Solaris 区域设备上生成“重复的 MAC、不同的 IP 地址”警报：

- **Solaris Zones 发现未建模设备，并且 Virtual Host Manager 尚未对它们进行管理** 。
  在这种情况下，请验证是否已将 Solaris Zones 发现配置为对设备进行建模。还可以调整轮询周期以更快地进行建模。
- **已从 Virtual Host Manager 管理中删除设备模型，但是这些模型仍保留在 Universe 拓扑中。**
  要阻止这种情况下的警报，请将设备放回 Virtual Host Manager 中，或从 CA Spectrum 中删除这些设备模型。

详细信息：

管理从 Solaris 中删除的设备的设备模型 (p. 89)
如何发现和建模虚拟环境 (p. 94)
配置 Solaris Zones AIM (p. 103)
删除 Virtual Host Manager 模型 (p. 108)

Huawei SingleCLOUD 模型上的重复模型警报

症状：

对于我的一些 Huawei SingleCLOUD 模型，CA Spectrum 生成了“检测到重复模型”警报。为什么会生成这些警报，我该如何进行更正？

解决方案：

为 Huawei SingleCLOUD 环境建模时，可能会由于不同的原因而创建重复模型。下面提供了可能导致重复模型警报的情况，并说明如何更正它们：

- **虚拟技术管理器的多个实例正在管理设备模型。**

  要更正此问题，请确认您的 SpectroSERVER 环境中只有一个虚拟技术管理器正在管理该设备。
- **用于定义 Huawei SingleCLOUD Manager 的虚拟 IP 地址与安装了 CAMM 展示器的设备的主 IP 地址相同。**

  要更正此问题，请验证用于与 Huawei SingleCLOUD Galax 进行通信的虚拟 IP 地址是否与安装了 CAMM 展示器的设备的主 IP 地址不同。

详细信息：

定义 Huawei SingleCLOUD Manager (p. 224)

连接未显示在 Huawei SingleCLOUD 拓扑中

症状：

我在发现并建模 Huawei SingleCLOUD 环境后，在拓扑中看不到 Huawei SingleCLOUD 组件之间的所有连接。我已按照正确的过程安装并设置了用于 CAMM 的 Huawei SingleCLOUD 设备包，且还执行了 Huawei SingleCLOUD 发现的建议过程。为什么在拓扑中看不到 Huawei SingleCLOUD 组件的连接？

解决方案：

为了在拓扑视图中生成 Huawei SingleCLOUD 组件之间的连接，CA Spectrum 在建模过程中确定第 2 层连接时要求提供特定模型和信息，如下所示：

- **连接设备的模型**

  为了使 CA Spectrum 在已建模环境中 Huawei SingleCLOUD 组件之间建立连接，必须在为虚拟实体建模之前为任何连接设备建模。发现并建模 Huawei SingleCLOUD 环境时，应首先运行标准 CA Spectrum 发现以为上游路由器和交换机建模。然后，可以运行 Huawei SingleCLOUD 发现，为虚拟实体创建模型和连接。如果未首先为连接设备建模，则不会在虚拟元素之间建立连接。

- **有关托管网络元素的信息**

  CA Spectrum 需要有关托管网络元素的特定信息，才能确定网络内的第 2 层连接。如果未提供此信息，则无法生成拓扑中的连接。以下两个已知问题导致了确定 Huawei SingleCLOUD 组件的第 2 层连接时的限制：

  - 在 Huawei SingleCLOUD 平台中使用的 Huawei 交换机未正确支持 dot1d 网桥表。如果没有正确的网桥表信息，则 CA Spectrum 无法确定 Huawei SingleCLOUD 组件的第 2 层连接。
  - Huawei SingleCLOUD API 当前未提供 Huawei SingleCLOUD 虚拟机的 MAC 地址。MAC 地址是 CA Spectrum 确定与上游网络设备的连接所必需的。如果无法直接从 Huawei SingleCLOUD API 获取必要信息，则 CA Spectrum 会尝试从上游设备解析 MAC 地址。如果 CA Spectrum 无法解析 MAC 地址，则无法确定连接。

遵循这些步骤:

1. 在 Huawei SingleCLOUD 发现运行之前，验证是否已对上游路由器和交换机正确建模。
2. 如果未对连接设备正确建模，请执行以下操作：
   a. 在受影响的虚拟机上运行“发现连接”。

      注意：有关“发现连接”的详细信息，请参阅《*IT 基础架构建模与管理 - 管理员指南*》。

   b. 如果“发现连接”未创建连接，请删除相应的 Huawei SingleCLOUD 模型，并重复发现和建模过程 (p. 221)。
3. 如果连接设备已正确建模，请在上游路由器和交换机上检查“检测到 SNMP Get_Next 循环”警报。
   - 如果存在该警报，则拓扑中缺少第 2 层连接是由于 Huawei 设备填充网桥表的方式所致，没有相应的解决办法。
   - 如果不存在该警报，请验证 Huawei SingleCLOUD 虚拟机是否具有有效的 MAC 地址，如下所示：
     a. 对“Huawei SingleCLOUD”->“所有虚拟机”运行定位器搜索。
     b. 在“结果”选项卡中，查看“MAC 地址”列中的值。

     虽然 CA Spectrum 尝试在未提供 MAC 地址时解析该地址，但是必要信息并不始终可用。

词汇表

Application Insight Module (AIM)

CA SystemEDGE 代理提供了插件体系结构，代理可在初始化时通过该体系结构加载可选的 *application insight module (AIM)*。AIM 是 SystemEDGE 代理的功能扩展。例如，vCenter AIM 允许 CA SystemEDGE 通过 VMware vCenter 服务器管理 vSphere 环境。

CAMM 展示器 (Huawei SingleCLOUD)

*Huawei SingleCLOUD CAMM 展示器*模型表示 CA Mediation Manager (CAMM) 展示器。CAMM 展示器模型允许配置 CAMM 引擎用来与 Huawei SingleCLOUD GalaX 进行通信的虚拟 IP 地址。每个 CAMM 展示器模型可以支持多个 Huawei SingleCLOUD Manager。

CNA FIP (Huawei SingleCLOUD)

Huawei SingleCLOUD CNA FIP 表示正在承载虚拟机的 CNA 的管理接口。此模型分配有 CNA FIP 的 IP 地址，并存在于主机容器内。

ESX 主机 (VMware)

*ESX 主机*是使用 ESX 服务器虚拟化软件来运行虚拟机的物理计算机。主机可提供虚拟机使用的 CPU 和内存资源，并为虚拟机提供存储访问和网络连接。

ESX 服务控制台 (VMware)

*ESX 服务控制台*是在 ESX 主机上运行的 Linux 内核，可提供所承载虚拟机的管理接口。

Huawei SingleCLOUD

Huawei SingleCLOUD 平台是一种企业级成套产品，由用于创建专用或公共云的网络、存储、服务器和软件的完整系统组成。

Huawei SingleCLOUD GalaX

Huawei SingleCLOUD GalaX 是用于统一管理 Huawei SingleCLOUD 的软件套件。它包括负责管理通用虚拟化平台 (UVP) 的操作和管理模块 (OMM)。

Huawei SingleCLOUD Manager

Huawei SingleCLOUD Manager 表示 CAMM 展示器上的虚拟 IP 地址。CAMM 监控 Huawei SingleCLOUD GalaX，后者负责管理 Huawei SingleCLOUD 虚拟平台。由 CAMM 监控的每个 Huawei SingleCLOUD GalaX 的信息通过 CAMM 展示器上的虚拟 IP 地址来提供，并由 Huawei SingleCLOUD Manager 模型表示。

Hyper-V 主机

*Hyper-V 主机*是使用 Microsoft Hyper-V 虚拟化软件来运行虚拟机的物理计算机。主机提供 Hyper-V 虚拟机使用的 CPU 和内存资源。它们还为这些虚拟机提供存储访问和网络连接。

Hyper-V 管理操作系统

*Hyper-V 管理操作系统*是在 Hyper-V 主机上运行的原始操作系统。Microsoft Hyper-V 使用此操作系统来配置承载的 Hyper-V 虚拟机。

IBM LPAR

IBM LPAR 是在 IBM LPAR 主机上配置的逻辑分区实例，它能像物理计算机那样运行操作系统和应用程序。IBM LPAR 根据其工作负荷与配置动态消耗物理主机上的资源。

IBM LPAR Manager

Virtual Host Manager 中的 *IBM LPAR Manager* 是启用了 IBM LPAR AIM 的 CA SystemEDGE 代理。IBM LPAR Manager 负责报告所有已配置的 IBM LPAR。Virtual Host Manager 与 IBM LPAR Manager 进行通信，以收集有关 IBM LPAR 虚拟环境的详细信息。

IBM LPAR 主机

*IBM LPAR 主机*是使用 IBM LPAR 虚拟化软件承载 IBM LPAR 实例的物理计算机。IBM LPAR 主机可提供 IBM LPAR 使用的 CPU 和内存资源。它们还为这些 IBM LPAR 提供存储访问和网络连接。

Pingable 模型

*Pingable 模型*是在 CA Spectrum 中基于非 SNMP 模型类型创建的常规网络模型类型。CA Spectrum 可以轮询这些设备以提供基本模型管理功能，但不提供支持 SNMP 的监控功能。

Solaris Zones Manager

Virtual Host Manager 中的 *Solaris Zones Manager* 是已启用 Solaris Zones AIM 的 CA SystemEDGE 代理。Solaris Zones Manager 负责报告所有已配置的 Solaris 区域。Virtual Host Manager 与 Solaris Zones Manager 进行通信，以收集有关 Solaris Zones 虚拟环境的详细信息。

Solaris Zones 主机

*Solaris Zones 主机*表示由 Virtual Host Manager 管理的 Solaris 主机的物理硬件。

Solaris 区域

*Solaris 区域*是由在 Solaris Zones 主机上运行的 Virtual Host Manager 管理的非全局区域实例。

Solaris 全局区域

*Solaris 全局区域*是在 Solaris Zones 主机上运行的管理操作系统，Solaris Zones 使用它来配置所承载的 Solaris 区域实例。

vCenter

vCenter 是一个 VMware 应用程序，可以针对 ESX 环境实现集中管理、操作自动化和资源优化。

vCenter 服务器 (VMware)

VMware *vCenter Server* 为配置、开通和管理虚拟 vSphere 环境提供了一个中央控制点。vCenter 服务器作为 Microsoft Windows 服务器和 Linux 服务器上的一项服务来运行。

VHM 模型

CA Spectrum 中的 *VHM 模型*表示由 Virtual Host Manager 管理的虚拟实体。与一些传统的 CA Spectrum 模型不同（这些模型从 SNMP 检索状态和管理信息），VHM 模型与代理管理器进行通信以实现其故障及虚拟管理功能。如果已在建模的设备上安装和配置 SNMP 代理，VHM 模型还可以通过 SNMP 进行通信。

VMware Manager

Virtual Host Manager 中的 *VMware Manager* 是已加载 vCenter Server AIM 的 CA SystemEDGE 代理。VMware Manager 负责报告其管理的所有已配置的虚拟机。Virtual Host Manager 与 VMware Manager 进行通信，以收集有关 VMware 虚拟环境的详细信息。

分布式 SpectroSERVER (DSS)

分布式 SpectroSERVER (DSS) 是一项强大的建模功能，支持对大型网络的各个部分实施分布式管理（按地理位置或跨单个物理位置中的多个服务器）。

计算节点代理 (CNA) (Huawei SingleCLOUD)

计算节点代理 (CNA) 是在 Huawei SingleCLOUD 平台中使用的管理进程，驻留在承载虚拟机的服务器上。在 CA Spectrum 中，CNA 由 Huawei SingleCLOUD 主机模型表示。Huawei SingleCLOUD CNA FIP 模型分配有 CNA 的 IP 地址。

代理管理

*代理管理*是指使用备用管理源（代替主要管理器或与主要管理器一起）来管理网络设备的行为。例如，CA Spectrum 可通过直接与虚拟网络设备联系或使用虚拟技术应用程序与设备联系来管理这些虚拟网络设备。

全局区域 (Solaris)

*全局区域*是每个 Solaris 系统上均包含的区域。如果系统上存在非全局区域，则全局区域是系统和系统范围管理的默认区域。

非全局区域 (Solaris)

*非全局区域*在 Solaris 操作系统的单个实例中提供虚拟化的操作系统环境。Solaris Zones 软件分区技术虚拟化操作系统服务。

资源池 (Solaris)

*资源池*定义分区系统资源的配置机制。资源池是能够进行分区的资源组之间的关联。

资源池 (VMware)

*资源池*定义物理计算的分区和单个主机或群集的内存资源。您可以将任何资源池分割成更小的资源池，从而将资源分开并分配给具体的组或用于特殊目的。您也可以分层组织和嵌套资源池。

通用虚拟化平台 (UVP)

通用虚拟化平台 (UVP) 是 Huawei HyperVisor，为由构成其云体系结构的主机和虚拟机组成的 Huawei SingleCLOUD 解决方案的一部分。

虚拟 NIC (VMware)

虚拟 NIC 是虚拟机上的虚拟以太网适配器。来宾操作系统通过设备驱动程序与虚拟以太网适配器（将虚拟以太网适配器看作物理以太网适配器）进行通信。虚拟以太网适配器有其自己的 MAC 地址、一个或多个 IP 地址，并响应标准以太网协议（就像物理 NIC）。

虚拟机

虚拟机 (VM) 是一种软件计算机，它能像物理计算机那样运行操作系统和应用程序。虚拟机根据其工作负荷动态地消耗其物理主机上的资源。由于虚拟机是一种非常灵活的计算单元，因此其部署可以包括多种环境。示例包括数据中心、云计算、测试环境、台式机和笔记本电脑等环境。在数据中心实施中，可以利用它们来实现服务器整合、优化工作负荷或提高能效。

硬件管理控制台 (HMC)

硬件管理控制台 (HMC) 是用于配置 IBM LPAR 的 IBM LPAR 虚拟化技术应用程序。此控制台提供 IBM LPAR 环境的集中式管理。

数据中心 (VMware)

*数据中心*用作主机、虚拟机、资源池或群集的容器。根据其虚拟配置，数据中心可以表示组织结构，如地理区域或单独的业务功能。也可以使用数据中心创建隔离的虚拟环境，以用于测试目的或组织您的基础架构。

数据中心 (VMware)

*数据中心*用作主机、虚拟机、资源池或群集的容器。如果它们的虚拟配置符合特定部门的要求，则数据中心可以表示组织结构（如地理区域或单独的业务功能）。您也可以使用数据中心创建隔离的虚拟环境用于测试，或用于组织环境。

群集

*群集*是一组 ESX 主机及其关联的虚拟机。在将主机添加到群集时，该主机的资源将成为群集资源的一部分。群集将管理它包含的所有主机的资源。

操作和管理模块 (OMM)

操作和管理模块 (OMM) 是 Huawei SingleCLOUD GalaX 软件应用程序的一部分，负责管理 Huawei SingleCLOUD Hypervisor 通用虚拟化平台 (UVP)。