CA Spectrum®

Virtual Host Manager Solution Guide

Release 9.4

CA Technologies Product References

This document references the following CA Technologies products:

- 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)

Contact CA Technologies

Contact CA Support

For your convenience, CA Technologies provides one site where you can access the information that you need for your Home Office, Small Business, and Enterprise CA Technologies products. At http://ca.com/support, you can access the following resources:

- Online and telephone contact information for technical assistance and customer services
- Information about user communities and forums
- Product and documentation downloads
- CA Support policies and guidelines
- Other helpful resources appropriate for your product

Providing Feedback About Product Documentation

If you have comments or questions about CA Technologies product documentation, you can send a message to techpubs@ca.com.

To provide feedback about CA Technologies product documentation, complete our short customer survey which is available on the CA Support website at http://ca.com/docs.

Contents

Chapter 1: Virtual Host Manager

This section contains the following topics:

About Virtual Host Manager

Virtual Host Manager is an application that is provided with CA Spectrum that models and monitors the health of your virtual network environment. With this application, you can view details about your virtual networking components and the relationships between your physical and virtual components.

This broad view helps you better monitor the health of your network infrastructure, preventing service interruptions to your virtual components. Monitoring your virtual environment, such as monitoring resource utilization on hosts and virtual devices, can help you identify potential performance issues. Virtual Host Manager also helps you pinpoint and effectively troubleshoot problems within your entire network by applying CA Spectrum fault isolation techniques to virtual environments.

A key challenge when monitoring your virtual environment is keeping the data updated. Virtual environments are designed to optimize resource allocation as needed, so the relationship between the virtual and physical networks can change rapidly. Virtual Host Manager keeps up with these changes and continuously monitors the current state of your virtual network to detect any changes.

Who Should Use Virtual Host Manager

Multiple vendors provide virtual technology solutions. Virtual Host Manager is intended for CA Spectrum users who create and manage virtual environments. Virtual Host Manager allows the user to monitor the fault and performance of both their physical and virtual network entities.

Virtual Technologies Supported by Virtual Host Manager

Virtual Host Manager can model and manage virtual networks that are created with the following virtual network technologies:

- VMware vCenter Server (part of VMware Infrastructure and vSphere)
- Solaris Zones
- Microsoft Hyper-V
- IBM logical partitions (LPARs)
- Huawei SingleCLOUD

More information:

Overlapping Virtual Technologies (see page 13)

System Requirements

Virtual Host Manager is an application that works within CA Spectrum when all required components are configured properly. Virtual Host Manager requires the following components by solution.

VMware

- CA Spectrum r9.2.3 or later
- VMware vCenter Server
- Latest CA SystemEDGE agent with vCenter Server AIM

Solaris Zones

- CA Spectrum r9.2.3 or later
- CA SystemEDGE agent with Solaris Zones AIM installed on a computer running Windows 2003 Server (32-bit)

Hyper-V

- CA Spectrum Release 9.2.3 or later
- CA SystemEDGE agent with Hyper-V AIM installed on each physical Microsoft Hyper-V server

IBM LPAR

- CA Spectrum Release 9.2.3 or later
- CA SystemEDGE agent with IBM LPAR AIM installed on a Windows server separate from the HMC (see definition on page 268) managing the IBM LPARs

Huawei SingleCLOUD

- CA Spectrum Release 9.2.3 or later
- CA Mediation Manager with Huawei SingleCLOUD Device Pack

Note: For more information about the CA SystemEDGE agent and AIM system requirements, see the *CA Virtual Assurance for Infrastructure Managers Implementation Guide*. For more information about CA Mediation Manager, see the CA Mediation Manager documentation.

How Virtual Host Manager Works

Virtual Host Manager monitors your virtual network entities seamlessly beside your physical network entities within CA Spectrum. You get a full view of your network, which facilitates troubleshooting for both types of entities. Although your virtual network entities behave like physical components, the process for monitoring those entities differs from the general CA Spectrum monitoring process. Understanding how this process works can help you locate and resolve networking issues that are related to your virtual network.

CA Spectrum typically contacts an SNMP agent on your network devices to gather information. However, some network devices do not have an SNMP agent installed. Without an SNMP agent, it is difficult to gather information that is needed for monitoring status and pinpointing issues using fault isolation. Virtual Host Manager extends basic CA Spectrum functionality, using a proxy manager to gather the needed information, as shown in the following diagram:

The process to gather information about your virtual network environment is as follows:

1. The proxy manager communicates directly with entities in your virtual environment.

   Note: The proxy manager resides on a server in your network. The location of the server depends on the virtual technology.

2. Using SNMP, CA Spectrum retrieves this information from the proxy manager and uses it to model and monitor your virtual entities.

Depending on the solution, Virtual Host Manager uses either of the following proxy managers, which are described in the following sections:

- CA SystemEDGE agent with a CA Virtual Assurance for Infrastructure Managers AIM module (see page 12)
- CA Mediation Manager with a solution-specific device pack (see page 13)

CA SystemEDGE Agent with CA Virtual Assurance for Infrastructure Managers AIMs

The following CA Virtual Assurance for Infrastructure Managers AIMs work with Virtual Host Manager:

vCenter Server AIM

Provides the capabilities for managing and monitoring systems that are under VMware vCenter Server control. The AIM communicates directly with vCenter Server software to get an entire view of all ESX servers that the associated VMware vCenter Server manages.

Solaris Zones AIM

Provides the capabilities for managing and monitoring Oracle Solaris systems that are configured to run containers and zones. The Solaris Zones AIM requires the CA SystemEDGE agent running on a Windows server. The Solaris Zones AIM communicates with the managed Solaris Zones servers through SSH connections. Verify that SSH is enabled on the managed Solaris servers and on the server where the Solaris Zones AIM runs. Verify the supported platforms in the CA Virtual Assurance for Infrastructure Managers documentation set.

Hyper-V AIM

Provides the capabilities for monitoring VMs that are under Hyper-V Server control. The Microsoft Hyper-V AIM requires the CA SystemEDGE agent on the Microsoft Hyper-V server. The Microsoft Hyper-V AIM communicates with the Microsoft Hyper-V server through WMI. The Microsoft Hyper-V AIM must reside on the Microsoft Hyper-V server to monitor virtual machines.

IBM LPAR AIM

Provides the capabilities for monitoring IBM LPARs managed by the HMC (see definition on page 268). The IBM LPAR AIM requires the CA SystemEDGE agent running on a Windows server separate from the HMC. The IBM LPAR AIM uses SSH to communicate with the HMCs, gathering information from the HMC to monitor the IBM LPAR instances.

More information:

How Virtual Host Manager Works with Solaris Zones (see page 91)
How Virtual Host Manager Works with Hyper-V (see page 139)
How Virtual Host Manager Works with IBM LPARs (see page 179)

CA Mediation Manager

The following CA Mediation Manager Device Pack is used with Virtual Host Manager:

Huawei SingleCLOUD

Provides the capabilities for monitoring the Huawei SingleCLOUD platform. CA Mediation Manager communicates directly with Huawei SingleCLOUD GalaX to obtain information about the Huawei HyperVisor Universal Virtualization Platform (UVP).

More information:

How Virtual Host Manager Works with Huawei SingleCLOUD (see page 225)

Overlapping Virtual Technologies

Your virtual environment has "overlapping" technologies when either of the following conditions exist:

- When two or more virtual technologies are used together in your environment
- When the same virtual technology is nested together

Virtual Host Manager does *not* support overlapping technologies that are modeled within a single SpectroSERVER. The following configurations represent examples of overlapping virtual technologies:

- Solaris Zones AIM and vCenter Server AIM are enabled on the same CA SystemEDGE host
- vCenter Server AIM is enabled on a VMware virtual machine that a different vCenter Server AIM manages

- Solaris Zones AIM is installed on a VMware virtual machine
- Solaris Zones Host is installed on a VMware virtual machine
- Solaris Zones Manager is installed on a Hyper-V virtual machine
- IBM LPAR AIM running on a VMware virtual machine or Hyper-V virtual machine

When CA Spectrum discovers an unsupported configuration between virtual technologies, the following behavior occurs:

- During initial modeling of a virtual technology manager, CA Spectrum prevents the creation of the technology folder. A minor alarm is generated, alerting you to the unsupported configuration.
- When a virtual technology manager monitors the same device that another manager is managing currently, CA Spectrum creates duplicate models for that device.

If you model the overlapping virtual technology manager on a separate SpectroSERVER, then Virtual Host Manager *can* support the overlapping technology managers.

For example, assume that you host a Solaris zone instance on a VMware virtual machine. You cannot manage both of these virtual environments on a single SpectroSERVER. Instead, each virtual environment must be managed on separate SpectroSERVERs.

More information:

Virtual Technologies Supported by Virtual Host Manager (see page 10)

Virtual Device Management and Multiple CA Spectrum AIM Solutions

When managing a device by multiple CA Spectrum AIM solutions, a defined ranked order of management applies, as follows:

1. Virtual Host Manager
2. Cluster Manager
3. Other technologies (such as Active Directory and Exchange Server Manager)

When a host with a CA SystemEDGE agent is already modeled in CA Spectrum, Virtual Host Manager recognizes the model. A duplicate model is not created. Instead, Virtual Host Manager pulls the existing model into its own management, applying the rules for each solution using the ranked order.

For example, when both Virtual Host Manager and Cluster Manager are managing a device, model parameters that Virtual Host Manager assigns are used. Examples of these parameters include the model name, IP address, and MAC address.

When a solution no longer manages a device, the rules of the remaining solutions are reapplied in the ranked order. Typically, any changes are made at the next polling cycle.

The defined order of management also affects how models appear in the Universe topology. Because Virtual Host Manager is the highest in the management ranking, all virtual devices appear in the appropriate virtual host containers automatically.

Note: For more information, see the *Cluster Manager Solution Guide* and the *Active Directory and Exchange Server Manager Solution Guide*.

More information:

How to Model Your Environment When Using Multiple AIM Solutions (see page 18)
Deleting Models When Using Multiple AIM Solutions (see page 26)

Chapter 2: Getting Started

This section describes the basic information that is required to install and begin using Virtual Host Manager. The information in this section applies to all virtual technologies supported by Virtual Host Manager.

This section contains the following topics:

How to Install Virtual Host Manager

When you install CA Spectrum, the Virtual Host Manager components are automatically installed and available for use. However, Virtual Host Manager is operable only after you also install and configure the appropriate proxy manager for your solution. For Huawei SingleCLOUD, use CA Mediation Manager. For all other supported technologies, use the CA Virtual Assurance for Infrastructure Managers AIM of the CA SystemEDGE agent.

To manage your virtual devices, CA Spectrum must be able to contact the proxy manager. And the proxy manager must be able to communicate with your network devices.

To install Virtual Host Manager, complete these tasks:

1. Install the appropriate proxy manager:
   - For VMware, Solaris Zones, Hyper-V, and IBM LPAR solutions, install the CA SystemEDGE agent and load the appropriate CA Virtual Assurance for Infrastructure Managers AIM. Use the appropriate location for your virtual technology, as follows:
     - VMware: Install on a separate server that can contact vCenter remotely.
     - Solaris Zones: Install on a 32-bit Windows system with SSH access to each Solaris Zone Host.
     - Hyper-V: Install on each Hyper-V Host.
     - IBM LPAR: Install on a Windows server separate from the HMC (see definition on page 268) that manages the IBM LPARs.

       Note: Monitor only one instance of the IBM LPAR Host with the IBM LPAR AIM. Do not manage a single IBM LPAR Host with multiple HMCs. Monitoring more than one instance can result in duplicate models in CA Spectrum.

Note: For installation instructions and more information about the AIM for your virtual technology, see the *CA Virtual Assurance for Infrastructure Managers Implementation Guide*.

- For Huawei SingleCLOUD, install and configure CA Mediation Manager and the Huawei SingleCLOUD Device Pack. Do not install the CAMM components on the same server where CA Spectrum is installed.

  Important! When configuring the Huawei SingleCLOUD Device Pack, you set the virtual IP addresses. The primary IP address of the device or virtual machine where the CAMM Presenter is installed cannot be used as a virtual IP address.

  Note: For more information, see the CA Mediation Manager documentation.

2. Install CA Spectrum with Virtual Host Manager included.

   Important! Do not install the SpectroSERVER on a virtual machine that Virtual Host Manager will manage.

   Note: For specific installation instructions, see the *Installation Guide*.

   You can now model your virtual network in CA Spectrum.

More information:

Discovering VMware Networks (see page 33)
System Requirements (see page 10)
Getting Started with Solaris Zones (see page 94)
Discovering Hyper-V Networks (see page 142)
Discovering IBM LPAR Networks (see page 182)
Discovering Huawei SingleCLOUD Networks (see page 228)

How to Model Your Environment When Using Multiple AIM Solutions

Depending on your environment, you can use Virtual Host Manager with other CA Spectrum AIM solutions to manage your infrastructure. Some configurations, such as the following examples, require multiple solutions for comprehensive management:

- A cluster node is a virtual machine.
- An Active Directory or Exchange Server host is a virtual machine.

Each of the CA Spectrum AIM solutions provides information that is specific to the technology it supports. For example:

- Virtual Host Manager provides data that is specific to virtual technologies.
- Cluster Manager provides data that is specific to cluster technologies.
- Active Directory and Exchange Server (ADES) Manager data that is specific to the supported Active Directory and Exchange Server roles.

Combined, these features provide a complete monitoring solution. To set up your implementation of multiple AIM solutions, take the following recommended approach.

Important! When using multiple AIMs, only a single AIM can be installed on a CA SystemEDGE host.

Follow these steps:

1. Configure the AutoDiscovery settings on the VNM model.
2. Configure the Virtual Host Manager settings that are related to your virtual technology.
3. Set up Virtual Host Manager by modeling the virtual technology manager and all virtual technology components.
4. Set up Cluster Manager by modeling the cluster technology manager and all cluster components.
5. Set up ADES Manager by modeling the ADES Host Manager and all Active Directory and Exchange Server hosts.

Note: For more information, see the *Cluster Manager Solution Guide* and the *Active Directory and Exchange Server Manager Solution Guide*.

More information:

Virtual Device Management and Multiple CA Spectrum AIM Solutions (see page 14)
Deleting Models When Using Multiple AIM Solutions (see page 26)

Viewing the Virtual Environment

The purpose of Virtual Host Manager is to provide visibility into your virtual environment. This visibility lets you view the logical relationships between devices, view performance data for individual entities, and report on the data you discover. Your virtual environment inevitably connects with your physical environment. Virtual Host Manager can help you visualize where these connections are and how they are performing.

Virtual Host Manager provides several methods for viewing your virtual environment, as follows:

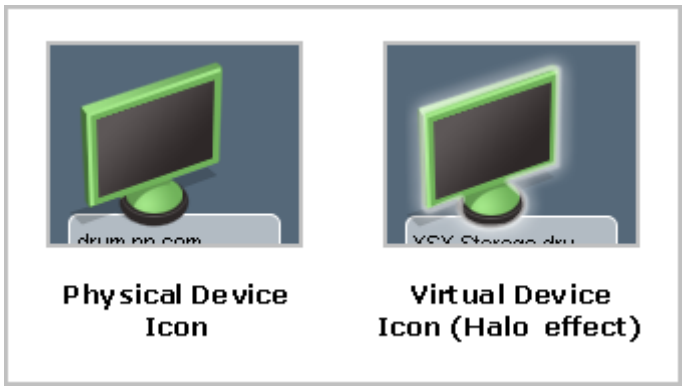
- The Explorer tab hierarchy in the Navigation panel shows logical relationships.
- Icons for individual models provide status and model type information at a glance.
- A graphical topology view helps you visualize connections between virtual and physical entities.
- Information views in the Contents and Component Detail panels provide detailed information about individual entities in your virtual environment.

Understanding each of these methods can help you monitor your virtual environment, letting you troubleshoot issues and optimize performance.

Note: For more information about using the OneClick interface, see the *Operator Guide*.

Icons for Virtual Devices

Virtual Host Manager provides icons that are designed specifically to distinguish devices in your virtual environment. To distinguish physical and virtual entities, the virtual device icons have a halo-like appearance around the outer edge. For example, a virtual device model icon displays a halo around the perimeter, as follows:



For physical servers that host virtual devices, Virtual Host Manager uses a distinctive honeycomb pattern on the device icon, as follows:

Locating Virtual Models in CA Spectrum

The models that are created for your virtual environment are integrated into CA Spectrum in the following three places:

Universe group

Appears in the Navigation panel and provides a hierarchical tree structure that displays the logical relationships between devices, both physical and virtual.

Virtual Host Manager group

Appears in the Navigation panel and provides a hierarchical tree structure. This structure helps you to visualize the relationships between your virtual devices, physical devices, and the logical entities that are configured in your virtual technology.

Topology tab

Appears in the Contents panel, providing a graphical view of your physical network, virtual network, and virtual machines. The topology provides a layer 2 view of the network, showing how your virtual and physical networks are connected. You can use this view to resolve alarms involving these virtual network models.

Note: This tab is available for only items in the Universe group.

All these views are available from the Explorer tab in the Navigation panel. Understanding how your virtual environment information appears in CA Spectrum is the key to deciding which view is best for viewing your virtual entities.

Note: For more information about using the OneClick interface, see the *Operator Guide*.

Locate Models on the Explorer tab

As you work with models in the OneClick Console, you can quickly locate a selected model on the Explorer tab. The location feature is provided for items in the Contents and Component Detail panels that reference a single model. These items include rows from the alarms or events tables. The feature is also available from the search results table.

View the same model in different Explorer tab groups to gain insight into its relationships within your physical and virtual networks.

To locate models on the Explorer tab, use the following procedure.

Follow these steps:

1. Locate an item in the Contents panel or Component Detail panel that references a single model.
2. Right-click the item and select from the following options:

   Location

   Changes the OneClick Console views to locate the selected model within the Explorer tab hierarchy in the Navigation panel. You can select from the following location options:

   Universe

   Locates the model in the Universe group hierarchy on the Explorer tab.

   Virtual Host Manager

   Locates the model in the Virtual Host Manager group hierarchy on the Explorer tab.

   The OneClick Console locates the related model in the Explorer tab. The Contents and Component Detail panels display details about the selected model.

Topology View

The CA Spectrum topology views provide a graphical depiction of your physical network, virtual network, and virtual machines. The topology views are available on the Topology tab in the Contents panel. Use the views on the Topology tab to resolve alarms involving these virtual network models. These views display the Layer 2 connectivity, showing how virtual and physical networks are connected.

CA Spectrum provides options for arranging the models in most topology views, such as the tree, radial, or manual layout. When selecting the tree layout, the Topology tab for the Universe group includes the following three *unlabeled* tiers of models:

Top tier

Displays the routers that are discovered with SNMP. These routers are the first level of routers within your virtual network environment that connect your virtual host devices to your physical network.

Middle tier

Contains any manageable switches that are discovered in your environment. These switches provide connectivity to the virtual host devices within the data center.

Bottom tier

Contains the virtual host device models and any unmanaged switches. The virtual host devices are the physical servers that run your virtualization technology.

When a server that hosts virtual machines is selected from the Explorer tab, only one layout option is available for the Topology tab. This automatic layout is organized into a tree structure and includes the following three *labeled* tiers:

Physical Network

Contains an off-page reference to any physical switches that detect traffic for a specific virtual machine. These entities are the components of your physical network that connect to your virtual network.

Virtual Network

Represents the internal or virtual switching that the virtual machine device provides. When a virtual switch has been configured with multiple virtual machines, CA Spectrum creates a model in the Virtual Network tier named a "repeater segment" or a "fanout." This fanout model represents the presence of a virtual switch.

Virtual Machines

Includes the virtual machines that are configured on the virtual host device that you selected in the Navigation panel.

Information Tab and Subviews

The tabs in the Contents and Component Details panels provide information that helps you monitor your virtual environment. The Information tab provides details about a single entity in your environment.

Expand the subviews to see detailed information. Most of the Information tabs include a General Information subview that lists general details about a selected model. Details include the IPv4 address, connection status, and other information.

Updating the Views

When you run the initial Discovery, Virtual Host Manager populates the Explorer tab with virtual device models. After Virtual Host Manager builds this initial hierarchy, your virtual network configuration can change frequently. Therefore, Virtual Host Manager continually updates this information. The information is useful for troubleshooting issues and optimizing performance only when it accurately reflects your virtual environment.

Understanding how and when the information is updated can help you evaluate the data and monitor your virtual environment.

More information:

How the Solaris Zones Data is Updated in Virtual Host Manager (see page 119)
How the Hyper-V Data is Updated in Virtual Host Manager (see page 158)
How the IBM LPAR Data is Updated in Virtual Host Manager (see page 199)
How the Huawei SingleCLOUD Data is Updated in Virtual Host Manager (see page 246)

Searches

Searching your virtual environment with CA Spectrum is a fundamental network management task. Virtual Host Manager does not provide a virtual-only topology view. Instead, CA Spectrum provides a collection of searches on the Locater tab that are designed specifically for your virtual network. These searches identify specific models or groups of models on your virtual network. Using these searches can help you locate details that you can use to monitor the performance of your virtual environment.

More information:

Locater Tab for Solaris Zones (see page 121)
Locater Tab for Hyper-V Searches (see page 161)
Locater Tab for IBM LPAR Searches (see page 202)
Locater Tab for Huawei SingleCLOUD Searches (see page 249)
Locater Tab for VMware Searches (see page 57)

Alarms and Fault Isolation

To alert you to problems within your virtual network, CA Spectrum generates alarms and uses advanced fault management techniques to isolate the root cause. Virtual networks provide a unique management opportunity because they provide an alternate management perspective in addition to standard device monitoring. While gathering information directly from a device, CA Spectrum also simultaneously gathers information from the proxy manager. With this extra monitoring capability, in addition to Contact Lost alarms, you can also incur Proxy Lost or Proxy Manager Unavailable alarms.

Alarms and fault isolation vary by virtual technology. The type of fault isolation that Virtual Host Manager uses depends on the devices that generate alarms and the type of events. CA Spectrum uses all available information to correlate the alarms to the appropriate root cause, avoiding multiple or false alarms.

Alarms on Initial Models

Until CA Spectrum contacts a model, the model remains in the Initial (blue) condition. Alarms are typically not visible on a model in the Initial condition; however, an exception applies when using Virtual Host Manager. If a virtual machine is brought into Virtual Host Manager management in the powered-down or suspended state, the critical Powered-Down or Suspended alarm overrides the Initial condition.

Creating Event Reports

Use event filters to create event reports in Report Manager. You can base these reports on any of the traps and events that are generated for your virtual entities in CA Spectrum.

To report on Virtual Host Manager events, the following event filter files are included with Report Manager:

- vhm.xml
- vhmtrap.xml

Note: For more information about using Report Manager to generate event reports from these codes, see the *Report Manager User Guide*. For information about using the predefined event filter files to generate reports, see the *Report Manager Installation and Administration Guide*.

Deleting Models When Using Multiple AIM Solutions

If you use Virtual Host Manager with other CA Spectrum AIM solutions, consider the following points when deleting models in your environment:

- If you plan to stop managing the device models using Virtual Host Manager, configure Virtual Host Manager delete settings to retain models. Otherwise, Virtual Host Manager deletes the model initially, losing any history or customization. Another AIM solution then recreates the model.

  Note: The Virtual Host Manager setting to retain models when the technology manager is deleted applies to SNMP-enabled device models only. For ICMP (Pingable) models, Virtual Host Manager deletes the model, and then another AIM solution recreates the model.

- When Virtual Host Manager unmanages a device and the model is retained, another AIM solution automatically pulls the model into its management.
- If a solution no longer manages a device, the rules of the remaining solutions are reapplied in the ranked order. Typically, any changes are made at the next polling cycle.
- The Explorer view hierarchy synchronizes after the Lost and Found (LostFound) is emptied.

More information:

Virtual Device Management and Multiple CA Spectrum AIM Solutions (see page 14)
How to Model Your Environment When Using Multiple AIM Solutions (see page 18)

Chapter 3: VMware

This section is for VMware users and describes how to use Virtual Host Manager to manage your virtual entities that are created with VMware vCenter.

This section contains the following topics:

How Virtual Host Manager Works with VMware

Virtual Host Manager monitors your virtual network entities seamlessly with your physical network entities within CA Spectrum. You get a full view of your network where you can troubleshoot networking issues for both types of entities. Although your virtual network entities behave like physical components, the process for monitoring those entities differs from the general CA Spectrum monitoring process. Understanding how this process works can help you locate and resolve networking issues that are related to your virtual network.

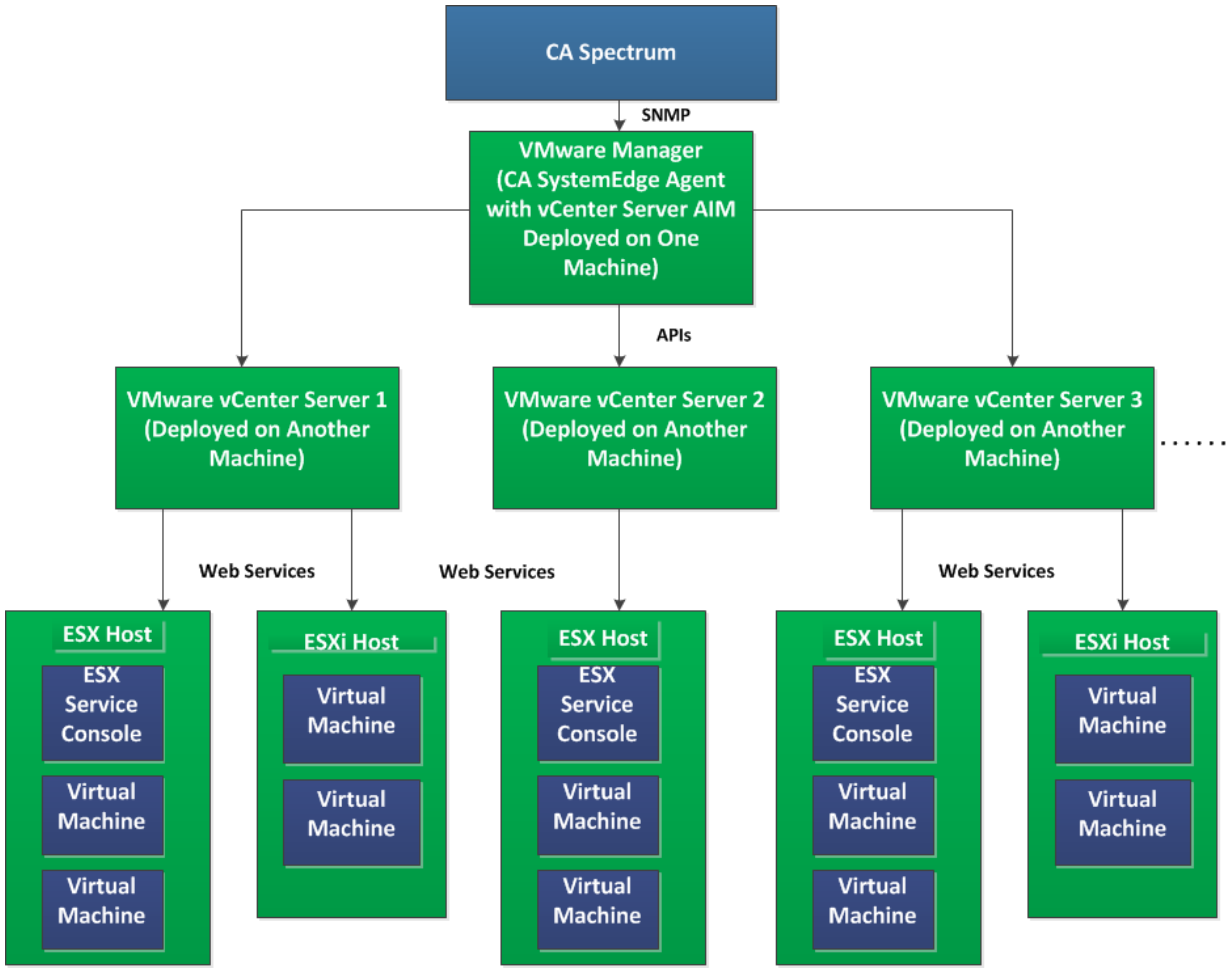
This release of CA Spectrum supports only the remote deployments of the latest CA SystemEDGE. The latest CA SystemEDGE comes with the latest vCenter server AIM capable of managing multiple vCenter server instances (multi-instance). As a result, you can have one or more remote CA SystemEDGE deployments for managing multiple VMware vCenter servers. We recommend not to manage the same VMware vCenter server using more than one remote CA SystemEDGE deployment.

As a result, before upgrading to this release of CA Spectrum, upgrade all the remote CA SystemEDGE deployments to the latest version, and remove all the local CA SystemEDGE deployments. If you do not remove all of the local CA SystemEDGE deployments, after the upgrade CA Spectrum generates "AGENT INSTALLED LOCALLY ON VCENTER SERVER" alarm on corresponding CA SystemEDGE models.

Before the upgrade, if remote CA SystemEdge model exists, the virtual entities modeled earlier are remodeled to support multi-instance vCenter. As part of that process all the events for those virtual entities are lost.

Note: The latest version of CA SystemEDGE is 5.8. For more information about remotely deploying CA SystemEDGE, see the *CA Virtual Assurance for Infrastructure Managers Implementation Guide*.

The following diagram shows how CA Spectrum gathers information about your VMware virtual environment using the latest remote CA SystemEDGE agent:



As shown in the diagram, the process to gather information about your VMware virtual environment is as follows:

1. The VMware vCenter application manages the ESX hosts in your virtual network. The VMware vCenter application stores detailed data about each ESX host and their virtual machines.
2. The CA SystemEDGE agent communicates with vCenter to gather the details about your virtual network. The CA SystemEDGE agent must have the vCenter Server AIM loaded.
3. Periodically, CA Spectrum retrieves information from CA SystemEDGE and uses it to model and monitor your virtual entities in OneClick.

Because Virtual Host Manager communicates with vCenter, CA Spectrum is aware of spontaneous network configuration changes. Examples are those changes that are due to VMware VMotion, HA technology, or a DRS scenario. Changes that are associated with these events are quickly reflected in OneClick and factored into the root cause analysis.

Models Created for VMware

Virtual Host Manager provides several models to represent the components of your VMware virtual technology network. Understanding the following basic models can help you better understand Discovery and how the virtual environment interfaces with your physical environment.

Note: Deployment of the CA SystemEDGE agent and vCenter Server AIM in your environment impacts the models that Virtual Host Manager displays.

Virtual Host Manager includes the following models and icons for VMware devices in the *remote* deployment scenario:

VMware Manager

Represents a physical or virtual host that contains the CA SystemEDGE agent with vCenter Server AIM loaded. This CA SystemEDGE agent remotely monitors the vCenter application running on a separate host (represented by the VMware vCenter Server model).

Icon:  or 

VMware vCenter Server

Represents a physical or virtual host that contains the vCenter application to manage your VMware virtual environment. The CA SystemEDGE agent with vCenter Server AIM monitors the vCenter application remotely. The CA SystemEDGE agent with vCenter Server AIM is on a separate host (represented by the VMware Manager model).

Icon:  or 

ESX Host

Represents an ESX host, as configured in your VMware virtualization technology. An *ESX host* is a physical computer that uses ESX Server virtualization software to run virtual machines. Hosts provide the CPU and memory resources that virtual machines use and give virtual machines access to storage and network connectivity. In the Universe topology, these models group your virtual entities into a separate view while showing how the virtual environment interacts with the physical network. The ESX host cannot be contacted directly for status information. Instead, the status of these models is inferred from the status of the items that it contains.

Icon: 

ESX Service Console

Represents the ESX service console component of your virtual environment. The *ESX service console* is a Linux kernel running on the ESX host that provides a management interface to the hosted virtual machines.

Icon: 

Virtual Machines

Represents a virtual machine, as configured in your VMware virtualization technology. A *virtual machine (VM)* is a software computer that, like a physical computer, runs an operating system and applications. A virtual machine dynamically consumes resources on its physical host, depending on its workload. Because virtual machines are flexible computing units, their deployment comprises a wide range of environments. Examples include environments such as data centers, cloud computing, test environments, or desktops and laptops. In data center implementations, they are used for server consolidation, workload optimization, or higher energy efficiency.

Icon: 

Virtual Host Manager also creates models these additional VMware entities that organize the ESX hosts and their virtual machines:

Data Centers

Represents a data center, as configured in your VMware virtualization technology. A *data center* serves as a container for your hosts, virtual machines, resource pools, or clusters. Depending on their virtual configuration, data centers can represent organizational structures, such as geographical regions or separate business functions. You can also use data centers to create isolated virtual environments for testing or to organize your infrastructure. Components can interact within data centers, but interaction across data centers is limited. A data center can contain clusters or hosts.

Icon: 

Clusters

Represents a cluster, as configured in your VMware virtualization technology. A *cluster* is a group of ESX hosts and their associated virtual machines. When a host is added to a cluster, the host resources become part of the cluster resources. The cluster manages the resources of all hosts within it. A cluster can contain hosts, resource pools, or virtual machines.

Icon: 

Resource Pools

Represents a resource pool, as configured in your VMware virtualization technology. A *resource pool* defines partitions of physical computing and memory resources of a single host or a cluster. You can partition any resource pool into smaller resource pools to divide and assign resources to specific groups or for specific purposes. You can also hierarchically organize and nest resource pools. A resource pool can contain virtual machines or more resource pools.

Icon: 

Important! Resource pools that are named "Resources" are skipped during Discovery and modeling. This name is designated for internal use only. Therefore, Virtual Host Manager filters these resource pools out of the Discovery results. You can avoid missing models for resource pools and the devices that they contain by specifying a different name for VMware resource pools.

More information:

Viewing Your VMware Virtual Network (see page 49)

Discovering VMware Networks

This section describes the Discovery and modeling process for Virtual Host Manager. The Virtual Host Manager administrator typically performs these tasks.

How to Configure Discovery Options

After installation, configure Virtual Host Manager for vCenter Discovery. Selecting preferences helps Virtual Host Manager to model virtual devices correctly.

Select preferences for the following options:

Automatically Model New Data Centers (see page 34)

Determines whether new data centers that are discovered during vCenter Discovery are modeled automatically.

Maintenance Mode for New Virtual Machines (see page 35)

Lets you decide which newly discovered virtual machines are placed into maintenance mode until you are ready for CA Spectrum to manage them.

Allow Device Model Deletes During vCenter Discovery (see page 36)

Controls how CA Spectrum handles ESX host, ESX service console, and virtual machine models when vCenter no longer manages them. Controls how these models are handled when you configure CA Spectrum to disable management of their parent data center.

Search for Existing Models (see page 37)

Determines the secure domains that Virtual Host Manager searches during a vCenter Discovery.

Discover SNMP-Capable Devices (see page 38)

Controls how SNMP-capable devices are modeled during vCenter Discovery. By default, new models are initially created as VHM models only. But, this option lets you override the default and immediately create SNMP models for devices that meet the necessary criteria.

Retain SNMP-enabled Virtual Machines During VMware Manager Deletion (see page 39)

Controls how CA Spectrum handles SNMP-enabled virtual machine models when a VMware Manager model is deleted.

Configure Automatic Modeling for New Data Centers

For each SpectroSERVER in your networking environment, you can control whether CA Spectrum automatically models new data centers that are found during vCenter Discovery. Modeling data centers automatically means that CA Spectrum manages all data centers in your vCenter environment.

Follow these steps:

1. Open Virtual Host Manager in the Navigation panel (see page 49).

   The main details page opens in the Contents panel for the selected Virtual Host Manager.

2. Click the Information tab.
3. Expand the Configuration, VMware, vCenter Discovery subview.
4. Click Set in the 'Automatically Model New Datacenters' field, and select one of the following options:

   Yes

   (Default) Models all data centers that are found during vCenter Discovery. Includes all of the contained clusters, resource pools, ESX hosts, ESX service consoles, and virtual machines.

   No

   Prevents the modeling of new data centers that are found during vCenter Discovery. CA Spectrum does not model the components that are contained within the data center.

   Use this option if your networking environment includes data centers that do not require monitoring. Then model your data centers manually.

   Your setting is saved, and new data centers are modeled in Virtual Host Manager according to your selection.

More information:

Manage Device Models for Devices Deleted from vCenter (see page 36)
How to Configure Discovery Options (see page 33)

Configure Maintenance Mode for New Virtual Machines

Virtual Host Manager automatically models the virtual machines that vCenter manages. CA Spectrum attempts to manage all discovered models. However, some virtual machines are not ready for CA Spectrum management when they are initially modeled. For example, CA Spectrum generates a Virtual Machine Powered Down alarm when it detects virtual machines that are powered down. To prevent undesired alarms on new models, you can select virtual machine models to be immediately placed into maintenance mode. Later, you can manually disable maintenance mode when you are ready to manage these devices.

Configure the maintenance mode for new virtual machines in OneClick.

Follow these steps:

1. Open Virtual Host Manager in the Navigation panel (see page 49).

   The main details page opens in the Contents panel for the selected Virtual Host Manager.

2. Click the Information tab.
3. Expand the Configuration, VMware, vCenter Discovery subview.
4. Click Set in the "Maintenance Mode for New Virtual Machines" field, and select one of the following options:

   Place only Powered down VMs in Maintenance Mode

   (Default) Applies maintenance mode only to powered-down or suspended virtual machine models at initial vCenter Discovery.

   Place all VMs in Maintenance Mode

   Applies maintenance mode to all new virtual machine models upon initial vCenter Discovery.

   Your setting is saved, and new virtual machines that are modeled in Virtual Host Manager are placed into maintenance mode according to your selection.

More information:

How to Configure Discovery Options (see page 33)

Manage Device Models for Devices Deleted from vCenter

The devices and the relationships between them change frequently in virtual networks. CA Spectrum attempts to reflect these changes accurately. When an ESX host is removed or a virtual machine is deleted in vCenter, CA Spectrum removes the corresponding device model from the Virtual Host Manager hierarchy. The option to "Allow Device Model Deletes During vCenter Discovery" controls whether CA Spectrum deletes the model. This option also controls the handling of device models that are contained in a data center when you disable management of the data center in Virtual Host Manager.

Important! When models are deleted, all notes or other customizations on those models are lost. You can disable this option if your models are likely to be recreated in vCenter later.

You can manage device models for devices that are deleted from vCenter.

Follow these steps:

1. Open Virtual Host Manager in the Navigation panel (see page 49).

   The main details page opens in the Contents panel for the selected Virtual Host Manager.

2. Click the Information tab.

3. Expand the Configuration, VMware, vCenter Discovery subview.

4. Click Set in the "Allow Device Model Deletes During vCenter Discovery" field and select one of the following options:

   Yes

   (Default) Deletes the Virtual Host Manager models that correspond to entities that are no longer managed in vCenter. Also deletes data center models for which you disable modeling in Virtual Host Manager.

   No

   Places Virtual Host Manager models in the LostFound container if their corresponding entity is no longer managed in vCenter. Also places data center models in the LostFound container when you disable modeling for the data center in Virtual Host Manager.

   Note: Models with more associations, such as a model that is included in a Global Collection, are handled differently. These models are removed from the Universe, but they are not moved to the LostFound container.

   Your setting is saved, and device models are handled as such after the device is deleted from vCenter.

More information:

Virtual Host Manager Alarms for VMware (see page 75)
Deleting Virtual Host Manager Models (see page 70)
How to Configure Discovery Options (see page 33)
Configure Automatic Modeling for New Data Centers (see page 34)
Manage SNMP-Enabled Virtual Machine Models After VMware Manager Deletion (see page 39)

Configure Model Searches Across Secure Domains

Rather than creating new models, vCenter Discovery attempts to locate models that exist in the SpectroSERVER. In an environment with Secure Domain Manager deployed, vCenter Discovery searches for models within the same secure domain as your VMware Manager. This domain is the "local" domain. However, some of your virtual environment devices can exist within a different secure domain. In this case, you can configure vCenter Discovery to search all secure domains for existing models.

You configure model searches across secure domains.

Follow these steps:

1. Open Virtual Host Manager in the Navigation panel (see page 49).

   The main details page opens in the Contents panel for the selected Virtual Host Manager.

2. Click the Information tab.
3. Expand the Configuration, VMware, vCenter Discovery subview.
4. Click Set in the "Search for Existing Models" field and select from the following options:

   In vCenter's Secure Domain

   (Default) Searches for existing models within the same secure domain as the vCenter server.

   In All Secure Domains

   Searches for existing models within all secure domains managed by the SpectroSERVER. Select this option only in the following situations:

   - All devices have unique IP addresses.
   - When secure domains are used for security purposes or to isolate network traffic.

   Note: Do not select this option for a NAT environment.

Your setting is saved. vCenter Discovery searches for the specified models in CA Spectrum. When duplicate models (models with the same IP address) exist in multiple secure domains, Virtual Host Manager handles the situation as follows:

- Virtual Host Manager selects the model in the local secure domain, if available.
- If a duplicate model does not exist in the local domain, Virtual Host Manager randomly selects a model from another secure domain.
- In both cases, Virtual Host Manager generates a minor alarm for the duplicate IP addresses on the VMware Manager model.

More information:

How to Configure Discovery Options (see page 33)

Configure SNMP Modeling Preferences

SNMP-capable virtual machines support enriched device monitoring, such as process and file system monitoring capabilities. However, SNMP agents can be costly and time-consuming to deploy. By default, vCenter Discovery creates ESX service consoles and virtual machines as VHM models (see definition on page 270). You can later upgrade them to SNMP models. However, you can also configure vCenter Discovery to model all new SNMP-capable devices as SNMP models. Although vCenter Discovery can take longer to complete, initially modeling as SNMP models avoids manually upgrading these models later.

Important! Enable SNMP modeling *before* you model your vCenter servers. If you model the vCenter servers first, all child models are created as VHM models, which must be manually upgraded to SNMP models.

Follow these steps:

1. Open Virtual Host Manager in the Navigation panel (see page 49).

   The main details page opens in the Contents panel for the selected Virtual Host Manager.

2. Click the Information tab.
3. Expand the Configuration, VMware, vCenter Discovery, SNMP Discovery subview.

   Important! To prepare your devices and CA Spectrum for SNMP Discovery, follow the steps in the subview. If devices are not properly prepared before vCenter Discovery, Virtual Host Manager cannot create SNMP models.

4. Click Set in the 'Discover SNMP-Capable Devices' field and select from the following options:

   Yes

   Enables SNMP modeling during vCenter Discovery. Only those devices that meet the specified criteria in the SNMP Discovery subview text are modeled as SNMP devices. Applies to *new* models only.

   No

   (Default) Models all new devices that are found during vCenter Discovery as VHM models. You can manually upgrade these models to SNMP models later.

   Your setting is saved.

More information:

How to Discover and Model Your Virtual Environment (see page 40)
Adding SNMP Capabilities to VHM Models (see page 45)
How vCenter Discovery Works (see page 43)
Manage SNMP-Enabled Virtual Machine Models After VMware Manager Deletion (see page 39)

Manage SNMP-Enabled Virtual Machine Models After VMware Manager Deletion

By default, SNMP-enabled devices are deleted from CA Spectrum when the following items are deleted:

- VMware Manager model for the device
- VMware folder in the Navigation panel

SNMP-enabled device models can include significant customizations that you want to retain. You can adjust your settings to avoid deleting these models. They are placed into the LostFound container for later use.

You can retain SNMP-enabled device models after VMware Manager or VMware folder deletion.

Follow these steps:

1. Open Virtual Host Manager in the Navigation panel (see page 49).

   The main details page opens in the Contents panel for the selected Virtual Host Manager.

2. Click the Information tab.

3. Expand the Configuration, VMware, vCenter Discovery subview.

4. Click Set in the "Retain SNMP-enabled Virtual Machines During VMware Manager Deletion" field and select one of the following options:

   Yes

   Retains SNMP-enabled virtual machine models in the LostFound container when their VMware Manager or the VMware folder is deleted.

   Note: Models with more associations, such as a model that is included in a Global Collection, are handled differently. These models are removed from the Universe, but they are not moved to the LostFound container.

   No

   (Default) Deletes all virtual machine models when their VMware Manager or the VMware folder is deleted.

   Your setting is saved, and SNMP-enabled device models are handled appropriately when VMware Manager models or the VMware folder is deleted.

How to Discover and Model Your Virtual Environment

To monitor your virtual environment, discover and model your virtual entities—data centers, resource pools, clusters, ESX hosts, ESX service consoles, and virtual machines. Modeling these entities in Virtual Host Manager lets you view your complete network topology in one tool. You can see the relationships between your physical and virtual components.

The main steps for modeling your virtual environment are as follows:

1. Run a standard CA Spectrum Discovery (see page 41).

   This Discovery ensures that the upstream routers and switches are modeled before vCenter Discovery runs. Or, if the SNMP Modeling option is disabled, this step can also model the SNMP-capable ESX service consoles and virtual machines. When modeling these entities, be sure that your modeling options are set correctly to support Virtual Host Manager.

2. Upgrade the CA SystemEDGE model (see page 42).

   This step is required only when your CA SystemEDGE agent on the vCenter server was modeled in a release earlier than CA Spectrum r9.1.

3. Let vCenter Discovery run (see page 43).

   When you model the CA SystemEDGE agent (with the vCenter Server AIM), vCenter Discovery begins automatically. Each of these vCenter Server models has its own vCenter Discovery process. vCenter Discovery finds the virtual entities that vCenter manages and models the ones that do not exist. vCenter Discovery then places the models in the Virtual Host Manager view of the Navigation panel.

More information:

Move an ESX Host to a Different vCenter (see page 48)
Adding SNMP Capabilities to VHM Models (see page 45)
How to Configure Management Options (see page 62)
Configure SNMP Modeling Preferences (see page 38)

Run CA Spectrum Discovery

To discover your VMware environment, run the standard CA Spectrum Discovery. This Discovery ensures that the upstream routers and switches are modeled so that later connections from the virtual entities can be established. You can also model the SNMP-capable ESX service consoles and virtual machines during CA Spectrum Discovery.

Note: Modeling SNMP-capable ESX service consoles and virtual machines is necessary during CA Spectrum Discovery only when the SNMP Modeling option is disabled during vCenter Discovery.

Note: Only an administrator performs this task.

Follow these steps:

1. Open the Discovery console.

   Note: Prepare by knowing the correct community strings, IP addresses, and port numbers for any SNMP agents that run on a nonstandard port.

2. Click  (Creates a new configuration) in the Navigation panel.

3. Configure your options for supporting virtual network modeling:

   a. Click the Modeling Options button in the Modeling Options group.

      The Modeling Configuration dialog opens.

   b. Click the Protocol Options button.

      The Protocol Options dialog opens.

   c. Select the "ARP Tables for Pingables" option, and click OK.

      The Modeling Configuration dialog opens.

   d. (Optional) Click the Advanced Options button in the Advanced Options group. Add your nonstandard SNMP ports (such as the CA SystemEDGE agent port), and click OK.

4. Enter individual IP addresses or the beginning and ending IP addresses in the IP Boundary List fields and click Add.

Note: Be sure that the range of IP addresses includes all servers with CA SystemEDGE and vCenter Server AIM installed and the interconnecting switches and routers. Or you can include the SNMP-capable ESX service consoles and virtual machines for which you want to create SNMP models.

5. Enter any additional values in the Discovery console, and click Discover.

   The following models are created and are added to your network topology in CA Spectrum:

   - vCenter servers and the switches and routers that connect them to your network—Information about your virtual environment comes from the vCenter server. When these vCenter Server models exist in CA Spectrum, vCenter Discovery can begin.
   - ESX service consoles and virtual machines—If you decide not to model these entities with CA Spectrum Discovery, vCenter Discovery creates them as VHM models (see definition on page 270).

   Note: You can also manually model your virtual network by IP address. In this case, we recommend modeling the upstream devices first. Modeling in the correct order ensures that the relationships between these entities are built correctly in the topology. For more information about Discovery, see the *Modeling and Managing Your IT Infrastructure Administrator Guide*.

More information:

Move an ESX Host to a Different vCenter (see page 48)
Adding SNMP Capabilities to VHM Models (see page 45)
How to Configure Management Options (see page 62)
Configure SNMP Modeling Preferences (see page 38)

Upgrade the CA SystemEDGE Model

The CA SystemEDGE agent could have been modeled in CA Spectrum before installing Virtual Host Manager or before the vCenter Server AIM was loaded on the agent. In this case, the existing CA SystemEDGE model is not compatible with Virtual Host Manager. Upgrade the model so that Virtual Host Manager can access the vCenter Server AIM capabilities in CA SystemEDGE. *This procedure is not required if the CA SystemEDGE agent with vCenter Server AIM is modeled after installing CA Spectrum.*

When you change from local to the latest remote CA SystemEDGE deployment, delete the existing CA SystemEDGE model and remodel the new remote CA SystemEDGE in OneClick.

Note: When you are already running the latest remote CA SystemEDGE with the latest vCenter server AIM, the CA SystemEDGE model is upgraded automatically.

More information:

Move an ESX Host to a Different vCenter (see page 48)
Adding SNMP Capabilities to VHM Models (see page 45)
How to Configure Management Options (see page 62)

How vCenter Discovery Works

vCenter Discovery is a specialized discovery process that gathers detailed information about your virtual environment entities. vCenter Discovery finds the virtual entities that vCenter manages and models the ones that do not exist. vCenter Discovery then places the models in the Virtual Host Manager view of the Navigation panel.

A key benefit of vCenter Discovery is that it runs automatically in the background, continually keeping your virtual environment data updated in CA Spectrum. Understanding how vCenter Discovery works reinforces the importance of properly installing and modeling the various components of Virtual Host Manager.

The vCenter Discovery process works as follows:

1. When the CA SystemEDGE agent and vCenter Server AIM are operational, the AIM communicates with vCenter servers to gather information about the virtual entities it manages. The vCenter Server AIM stores this information.

   Important! The CA SystemEDGE agent and vCenter Server AIM must be installed and configured so that CA SystemEDGE, vCenter, and CA Spectrum can communicate. If they cannot, vCenter Discovery cannot run.

2. During CA Spectrum Discovery, CA Spectrum creates a vCenter Server model for each server that is referenced in step 1. CA Spectrum intelligence is enabled to handle communication between CA Spectrum and the CA SystemEDGE agent.

3. CA Spectrum polls the vCenter Server AIM to gather the vCenter information that was stored in Step 1.

4. CA Spectrum begins vCenter Discovery. The information from the AIM is used to update modeling in the CA Spectrum Topology tab and the Virtual Host Manager hierarchy in the Navigation panel, as follows:

   a. If you enable SNMP Discovery before Step 2, Virtual Host Manager Discovery creates SNMP models for all new SNMP-capable models meeting the SNMP Discovery criteria.

      Note: By default, SNMP Discovery is disabled during vCenter Discovery.

   b. VHM models (see definition on page 270) are created for data centers, clusters, and resource pools.

      Important! Resource pools that are named "Resources" are skipped during Discovery and modeling. This name is designated for internal use only. Therefore, Virtual Host Manager filters these resource pools out of the Discovery results. You can avoid missing models for resource pools and the devices that they contain by specifying a different name for VMware resource pools.

   c. Previously existing ESX service console and virtual machine models are changed to VHM models.

   d. VHM models are created for the ESX service consoles and virtual machines that are not yet modeled in CA Spectrum.

   e. VHM models are created for the ESX host models. These models display their associated ESX service console and virtual machine models in the Navigation panel, under Virtual Host Manager and the Universe topology.

   f. All models for your virtual network are added to the Virtual Host Manager portion of the Navigation panel.

   Note: In a virtual environment, devices on separate ESX hosts can have the same IP or MAC address. In this case, CA Spectrum creates duplicate models for each occurrence of an IP or MAC address.

5. vCenter Discovery automatically repeats this process at each regularly scheduled vCenter polling interval.

   Note: By default, the vCenter polling interval is controlled by a setting on the VMware Manager model. Or you can control vCenter polling independent of the vCenter Server device model using the vCenter server application model.

More information:

Move an ESX Host to a Different vCenter (see page 48)
Adding SNMP Capabilities to VHM Models (see page 45)
How to Configure Management Options (see page 62)
Controlling vCenter Server AIM Polling (see page 68)
Configure Model Searches Across Secure Domains (see page 37)

Adding SNMP Capabilities to VHM Models

SNMP-capable virtual machines support enriched device monitoring, such as process and file system monitoring capabilities, that can provide added value to your solution. However, SNMP agents can be costly and time-consuming to deploy throughout an enterprise. When an SNMP agent is not available or SNMP Discovery is disabled, Virtual Host Manager creates ESX service consoles and virtual machines as VHM models (see definition on page 270).

Later, you can install an SNMP agent on any virtual machine. You can then upgrade its modeling in CA Spectrum. Depending on your needs, you can upgrade to SNMP models as follows:

- **Upgrade only selected devices**—This method works quickly when you have a small selection of models that require an upgrade. This method first deletes the VHM models and child models. After CA Spectrum deletes the models, the new SNMP models are created during the next vCenter Discovery and placed in Virtual Host Manager. This method requires you to know the IP addresses for the models to upgrade.
- **Upgrade all SNMP-capable VHM models**—This method upgrades models in batch, and this method is preferred when upgrading Virtual Host Manager to a new release. For this method, you are not required to know the IP addresses of individual models. Another advantage is that after CA Spectrum deletes the VHM models, the upgraded SNMP models are immediately placed in the Virtual Host Manager hierarchy. You do not have to wait for the next polling cycle. Therefore, the child models are not left unmanaged. The drawback to this method is that it can take a long time to complete. The time that is required to complete this upgrade depends on how many community strings and SNMP ports Virtual Host Manager must search when locating SNMP-capable devices.

  Note: Virtual Host Manager attempts to identify SNMP agents on powered-up pingable virtual machines only.

Important! When models are deleted, all notes or other customizations on those models are lost.

Upgrade Selected VHM Models to SNMP Models

When an SNMP agent is not available or SNMP Discovery is disabled during vCenter Discovery, Virtual Host Manager creates VHM models (see definition on page 270). This modeling applies to ESX service consoles and virtual machines. Later, you can install an SNMP agent on any virtual machine. You can then upgrade its modeling in CA Spectrum. You are required to know the IP addresses for the device models you want to upgrade. Manually selecting models to upgrade works quickly, but all notes or customizations on these models are lost during the upgrade.

Follow these steps:

1. Deploy or enable an SNMP agent on the device, if required.
2. Model the device again using one of the following methods:
   - CA Spectrum Discovery
   - Model individual devices by IP address

   When the new SNMP-capable model is created, CA Spectrum removes the previous model from Virtual Host Manager and deletes the model. At the next vCenter Server AIM polling cycle, CA Spectrum adds the SNMP-capable model to Virtual Host Manager in the Navigation panel.

   Important! When models are deleted, all notes or other customizations on those models are lost.

More information:

Deleting Virtual Host Manager Models (see page 70)
How to Discover and Model Your Virtual Environment (see page 40)
Manage Device Models for Devices Deleted from vCenter (see page 36)

Upgrade All VHM Models to SNMP Models

Virtual Host Manager creates ESX service consoles and virtual machines as VHM models (see definition on page 270) in the following cases:

- When an SNMP agent is not available.
- When SNMP Discovery is disabled during vCenter Discovery.

Later, you can install an SNMP agent on any virtual machine and then upgrade its modeling in CA Spectrum. When upgrading in batch, CA Spectrum searches your VHM models, locating those models that are now SNMP-capable devices. Then CA Spectrum converts them to SNMP models. This method can take a long time, depending on how many community strings and ports Virtual Host Manager must search. However, this method ensures that child models are not unmanaged while parent models are upgrading.

You can upgrade all VHM models for VMware to SNMP models.

Follow these steps:

1. Deploy or enable an SNMP agent on your devices, as required.
2. Open Virtual Host Manager in the Navigation panel (see page 49).

   The main details page opens in the Contents panel for the selected Virtual Host Manager.
3. Select the VMware Manager model in the Navigation panel that manages the models to upgrade.
4. Click the Information tab.
5. Expand the VMware Manager Modeling Control, ICMP-Only Device Upgrades subview.
6. Click the Upgrade ICMP-Only Devices button.

   Important! When models are deleted, all notes or other customizations on those models are lost.

   Virtual Host Manager searches the devices that the vCenter Server AIM manages on the selected VMware Manager device. Virtual Host Manager upgrades all ICMP-only devices that meet the criteria for SNMP devices and places them within the Virtual Host Manager hierarchy.

Move an ESX Host to a Different vCenter

Moving an ESX host from one CA Spectrum managed vCenter to another can cause modeling problems when both vCenter hosts are modeled on the same SpectroSERVER. Some possible symptoms of these modeling problems are as follows:

- CA Spectrum deletes the models that are associated with the ESX host and does not recreate them after the move.
- False Proxy Lost alarms are created and remain, even though the new vCenter can contact the ESX host and all hosted virtual machines.

If you move your ESX host in the correct order, you can avoid these problems.

To move an ESX host to a different vCenter server, use the following procedure.

Follow these steps:

1. (Optional) Change the "Allow Device Model Deletes During vCenter Discovery" option to No (see page 36).

   Note: Perform this step only if both the originating and destination vCenters are modeled in the same SpectroSERVER. This setting keeps the existing ESX host, ESX service console, and virtual machine models when they become unmanaged by the first vCenter server. Therefore, customizations or historical details for the models are preserved and available after the move.

2. Open VMware and remove the ESX host from management of the first vCenter server.
3. Wait for Virtual Host Manager in the Navigation panel to reflect the changes.
4. Open VMware and add the ESX host into the destination vCenter server.

   Note: Virtual Host Manager is not DSS (see definition on page 268) aware. Therefore, when moving the ESX host to a vCenter server modeled on a different SpectroSERVER, a new set of models are created. These models represent the ESX host, ESX service console, and the hosted virtual machines.

5. (Optional) Change the "Allow Device Model Deletes During vCenter Discovery" option back to Yes on the originating vCenter server model.

   The ESX host is successfully moved from one vCenter server to a second vCenter server.

More information:

How to Discover and Model Your Virtual Environment (see page 40)
Run CA Spectrum Discovery (see page 41)
Upgrade the CA SystemEDGE Model (see page 42)
How vCenter Discovery Works (see page 43)

Viewing Your VMware Virtual Environment

This section describes concepts for viewing your VMware virtual environment and the associated alarms. The basic steps are no different from the standard CA Spectrum procedures. However, this section describes conceptual differences and details that only apply to the VMware virtual technology.

Viewing Your VMware Virtual Network

On the Explorer tab, the Virtual Host Manager node provides a hierarchical tree structure. This layout helps you visualize the logical relationships between your virtual environment resources.

Using this information, you can see how resources are shared among your virtual hosts. This information can help you identify opportunities to reorganize and optimize your virtual environment. The hierarchy also provides a quick way to monitor the performance of your resources and troubleshoot alarms.

Because Virtual Host Manager is not aware of a DSS environment (see definition on page 268), it is located within a landscape hierarchy. The following example, showing where Virtual Host Manager appears on the Explorer tab in the Navigation panel, illustrates the virtual environment hierarchy:

```
[-] SpectroSERVER host
    [+] Universe
    [-] Virtual Host Manager
        [-] VMware
            [-] VMware Manager 1
                [-] vCenter server 1
                    [-] Datacenter 1
                        [-] ESX host 1
                         .  ESX service console 1
                         .  Virtual machine 1
                         .  Virtual machine 2
                [-] vCenter server 2
                    [-] Datacenter 2
                        [-] ESX host 2
                             .  ESX service console 2
                             .  Virtual machine 3
                             .  Virtual machine 4
                                [+] Resource pool 1
                                 .  Virtual machine A
                                 .  Virtual machine B
                        [+] Cluster 1
                        [-] Cluster 2
                            [-] ESX host A
                                 .  ESX service console A
                             .  Virtual machine 3
                             .  Virtual machine 4
                            [-] Resource Pool 2
                                 .  Virtual machine C
                                [+] Resource Pool A
                                [+] Resource Pool B
                    [+] Datacenter 3
            [-] VMware Manager 2
                [-] vCenter server 3
                    [-] Datacenter 4
                        [-] ESX host 1
                         .  ESX service console 1
                         .  Virtual machine 1
                         .  Virtual machine 2
                [-] vCenter server 4
                    [-] Datacenter 5
                        [-] ESX host 2
                             .  ESX service console 2
                             .  Virtual machine 3
                             .  Virtual machine 4
```

Virtual Host Manager is the root node for the entire virtual environment that this SpectroSERVER manages. Selecting this node in the Navigation panel displays Virtual Host Manager details in the Contents panel. You can view details such as events and alarms that are related to your virtual environment.

Directly under Virtual Host Manager, virtual environments are organized within folders that represent the associated technology. In the example hierarchy above, the VMware folder contains the portion of the virtual environment that was created using VMware virtualization technology. In this folder, Virtual Host Manager lists all CA SystemEDGE servers with the vCenter Server AIM and the vCenter servers that this SpectroSERVER manages. These entities are represented separately as a VMware Manager model with a vCenter Server model directly beneath it in the hierarchy.

Selecting a VMware Manager in the Navigation panel displays details in the Contents panel, such as the Configuration, Managed Environment, and Events.

Each vCenter server contains only the portion of the entire virtual environment that it manages. Selecting a vCenter server in the Navigation panel displays details in the Contents panel, such as Configuration and Utilization of the selected vCenter servers.

Under each vCenter server, the hierarchy represents the logical relationships among the following virtual entities:

- **Data Centers**

  A data center can contain clusters or hosts. Selecting a data center in the Navigation panel displays details in the Contents panel. These details include events and alarms that are related to the data center or a list of clusters. Components can interact within data centers, but interaction across data centers is limited.

- **Clusters**

  Clusters can contain ESX hosts, resource pools, or virtual machines. Selecting a cluster in the Navigation panel displays details in the Contents panel, which include:

  - Events and alarms that are related to the cluster.
  - A list of ESX hosts and virtual machines that are contained in the cluster.
  - The DRS and HA settings.

- **Resource pools**

  A resource pool can contain virtual machines or other resource pools. Selecting a resource pool in the Navigation panel displays details in the Contents panel, which include:

  - Overall CPU usage.
  - Events and alarms that are related to the resource pool.
  - A list of other virtual network objects that are contained in the resource pool.

Important! Resource pools that are named "Resources" are skipped during Discovery and modeling. This name is designated for internal use only. Therefore, Virtual Host Manager filters these resource pools out of the Discovery results. You can avoid missing models for resource pools and the devices that they contain by specifying a different name for VMware resource pools.

- **ESX hosts**

  An ESX host can contain an ESX service console, resource pools, or virtual machines. Selecting an ESX host in the Navigation panel displays details in the Contents panel, which include:

  - Total virtual machine memory.
  - CPU state.
  - A list of virtual machines that the ESX host manages.

  Note: When a cluster contains an ESX host, the virtual machines that are associated with the host are not grouped under the host. Instead, they appear under the cluster beside the ESX host on the Explorer tab.

- **ESX service consoles**

  The ESX service console model appears as a child to its corresponding ESX host model. The ESX service console model is always a leaf node on the Virtual Host Manager hierarchy tree. This model has the same name as its parent. The model icon in the Contents and Component Detail panels distinguishes the ESX service console models from their parent ESX host model. The DeviceType attribute also distinguishes these models. Selecting an ESX service console in the Navigation panel displays details in the Contents panel.

  Note: The ESX service console model is the only VMware model type within Virtual Host Manager that does not provide a Virtual Host Manager-specific subview on the Information tab.

- **Virtual machines**

  A virtual machine is always a leaf node on the Virtual Host Manager hierarchy tree. Selecting a virtual machine in the Navigation panel displays details in the Contents panel, including power status, memory usage, and related events and alarms.

More information:

Custom Subviews for Virtual Entity Types (see page 55)
Run CA Spectrum Discovery (see page 41)

Understanding the VMware Virtual Topology

The vCenter server, ESX host, ESX service console, and virtual machine models that are created for your virtual environment are integrated into the topology views. ESX host models automatically group their associated ESX service console and virtual machines. The topology shows how these ESX service consoles and virtual machines are connected to your physical network entities.

The following example shows how these models can appear on the Explorer tab in the Navigation panel under the Universe group:

```
[-] Universe
     .  Physical switch 1
     .  Physical switch 2
    [-] ESX host
          .  ESX service console
          .  Fanout 1
          .  Fanout 2
          .  Virtual machine 1
          .  Virtual machine 2
          .  Virtual machine 3
```

Selecting one of these models displays these relationships graphically on the Topology tab in the Contents panel.

How the VMware Data is Updated in Virtual Host Manager

During your initial vCenter Discovery, CA Spectrum populates the Virtual Host Manager hierarchy in the Navigation panel with your virtual device models. After CA Spectrum builds this initial hierarchy, your virtual network configuration can change frequently. Virtual Host Manager continually works to keep this information accurate in CA Spectrum. For example, the following events can change your virtual network configuration:

- Adding a new vCenter server to be managed by an existing CA SystemEDGE.
- Creating or deleting datacenters, clusters, resource pools, ESX hosts, or virtual machines in the vCenter application
- HA or DRS settings in VMware, which can cause virtual machines to move spontaneously to a new ESX host
- Manually migrating a virtual machine from one ESX host to another

To keep your information accurate, Virtual Host Manager detects these changes by polling the vCenter Server AIM. Therefore, your virtual network configuration changes, if any, are reflected in CA Spectrum at each polling cycle. CA Spectrum also receives traps from the AIM and generates the corresponding events. By reviewing the event log, you can find out when configuration changes occur. Example configuration changes include when a virtual device is migrated because of HA or DRS. When it detects a change in your virtual network configuration, CA Spectrum performs the following tasks:

- Updates the placement of your virtual entity models in the Virtual Host Manager hierarchy of the Explorer tab
- *Automatically* rediscovers connections to the affected ESX service console and virtual machine models and associates them with the correct ESX host in the Universe topology

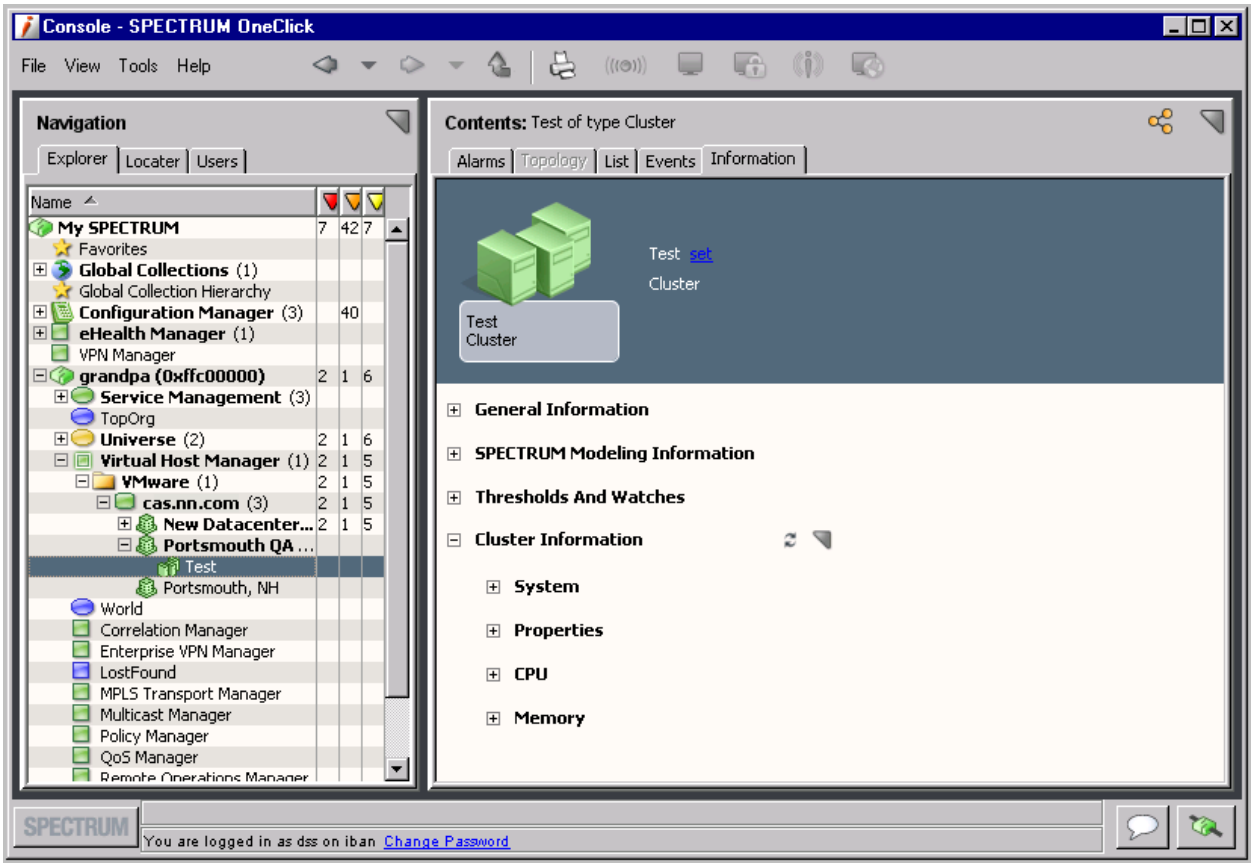
  Important! To reestablish connections to your virtual models correctly, all interconnecting routers and switches in your physical network must be modeled. If these models do not exist before connections to your virtual devices are rediscovered, CA Spectrum cannot resolve those connections in the Universe topology view. The ESX hosts are placed in the same LAN container as the CA SystemEDGE model.

More information:

Configure and Monitor Resource Status (see page 67)
How Virtual Host Manager Works (see page 11)
Move an ESX Host to a Different vCenter (see page 48)
Manage Device Models for Devices Deleted from vCenter (see page 36)
Viewing Your VMware Virtual Network (see page 49)

Custom Subviews for Virtual Entity Types

Your Virtual Host Manager models collectively provide information about your virtual environment. Individually, each model provides unique information or configuration settings, depending on the virtual entity type it represents. This custom subview appears on the Information tab in the Contents panel. These subviews can contain real-time data, such as disk space available or memory utilization. Also, these subviews provide access to threshold settings. For example, the custom subview for a cluster is the "Cluster Information" subview, as shown:



The ESX service console model is the only VMware model type within Virtual Host Manager that does not provide a Virtual Host Manager-specific subview.

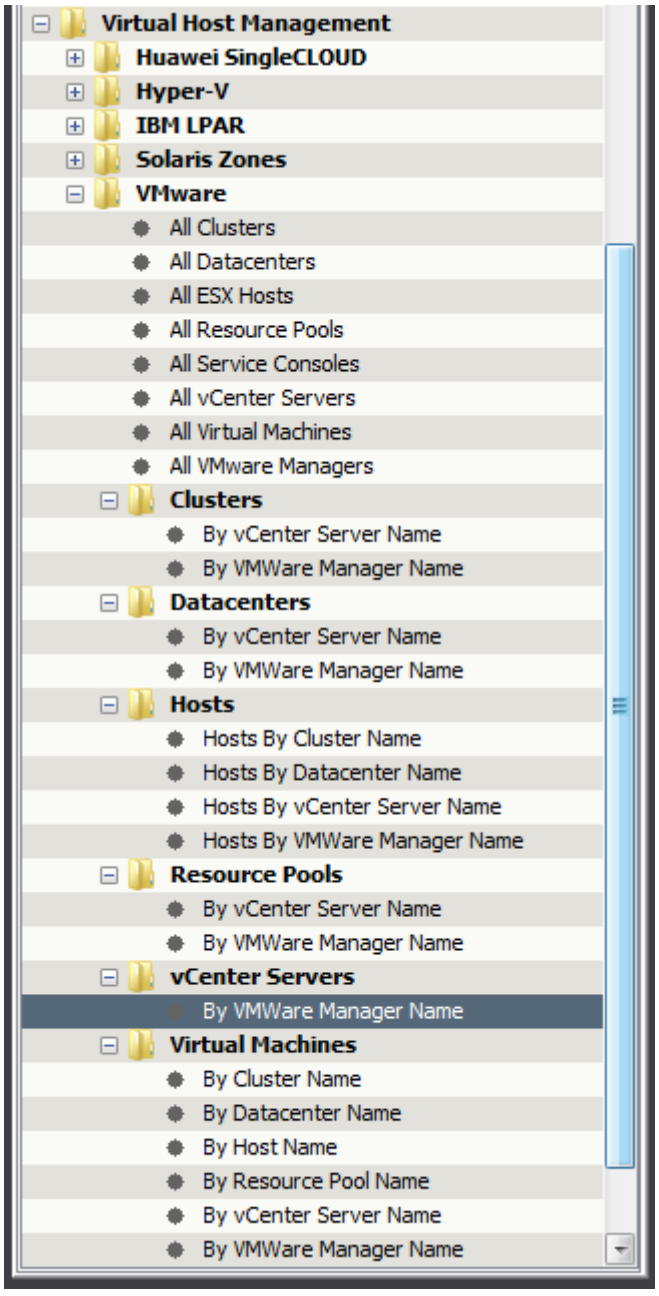
Note: The vCenter model provides combined information for all virtual devices that the vCenter server manages. Select the VMware Manager model in the Navigation panel to see information about the selected manager and combined information about all of its entities. These entities include vCenter server, ESX hosts, ESX service consoles, virtual machines, virtual switches, NICs, and datastores. This information is the same data that is displayed on the Information tab for each individual entity model. The combined subview in the VMware Manager model can provide a good overview about all of the virtual entities that it manages.

More information:

Configure and Monitor Resource Status (see page 67)
Viewing Your VMware Virtual Network (see page 49)

Locater Tab for VMware Searches

In addition to viewing details about your virtual environment on the Explorer tab, you can also use the Locater tab to run preconfigured Virtual Host Manager searches. The search options are grouped under the Virtual Host Management, VMware folder on the Locater tab, as shown:



These detailed searches can help you investigate information that is related to virtual entities only, such as a specific resource pool or ESX host. For example, if you know the name of a specific ESX host, you can search for all virtual machines that it manages. Creating this list of virtual machines can be useful when checking the status of a group of virtual machines. Or, you can use the list to determine which machines require management changes in VMware. Example management changes include moving the virtual machines to a different ESX or placing them in maintenance mode.

Note: Although Virtual Host Manager is not DSS (see definition on page 268) aware, these preconfigured searches let you select multiple landscapes to search in the search parameters.

The Locater tab in the Navigation panel includes the following searches for Virtual Host Manager information:

All Clusters

Locates all clusters that have been modeled in the CA Spectrum database for the virtual network.

All Datacenters

Locates all datacenters that have been modeled in the CA Spectrum database for your virtual network.

All ESX Hosts

Locates all ESX host servers that have been modeled in the CA Spectrum database for your virtual network.

All Resource Pools

Locates all resource pools that have been modeled in the CA Spectrum database for your virtual network.

All Service Consoles

Locates all ESX service consoles that have been modeled in the CA Spectrum database for your virtual network.

All vCenter Servers

Locates all VMware vCenter host servers that have been modeled in the CA Spectrum database for your virtual network.

All Virtual Machines

Locates all virtual machines that have been modeled in the CA Spectrum database for your virtual network.

All VMware Managers

Locates all servers hosting the CA SystemEDGE agent with vCenter Server AIM enabled and that have been modeled in the CA Spectrum database for your virtual network.

Clusters

Locates Clusters in the CA Spectrum database. Results are limited to only those entities that the containers that are specified in one of the following searches manage:

- By Vmware Manager Name
- By vCenter Server Name

Datacenters

Locates Datacenters in the CA Spectrum database. Results are limited to only those entities that the containers that are specified in one of the following searches manage:

- By Vmware Manager Name
- By vCenter Server Name

Hosts

Locates ESX host servers or ESX service consoles in the CA Spectrum database. Results are limited to only those entities that the containers that are specified in one of the following searches manage:

- ESX Hosts By Cluster Name
- ESX Hosts By Datacenter Name
- By VMware Manager Name
- By vCenter Server Name

Resource Pools

Locates Resource Pools in the CA Spectrum database. Results are limited to only those entities that the containers that are specified in one of the following searches manage:

- By Vmware Manager Name
- By vCenter Server Name

vCenter Servers

Locates vCenter Servers in the CA Spectrum database. Results are limited to only those entities that the containers that are specified in one of the following searche manage:

- By Vmware Manager Name

Virtual Machines

Locates virtual machines in the CA Spectrum database. Results are limited to only the virtual machines that the containers that are specified in one of the following searches manage:

- By Cluster Name
- By Datacenter Name

- By Host Name
- By Resource Pool Name
- By VMware Manager Name
- By vCenter Server Name

More information:

Viewing Your VMware Virtual Network (see page 49)

Status Monitoring Options

CA Spectrum provides a wide range of options for monitoring the state of your virtual network resources. The status information available for a resource varies, depending on the type of virtual entity you are monitoring. Also, your ability to configure a status option depends on its type. For example, some status options are read-only, but others let you configure threshold values, enable behaviors, or select an alarm severity. Providing this range of options and levels of customization, CA Spectrum lets you decide how best to monitor the performance of your virtual network.

Status fields are located in the OneClick subviews. All status information for a given virtual environment is available on the VMware Manager model in a tabular format. Also, each virtual entity type that has a unique model in CA Spectrum provides a subset of the same status information for easy viewing. Status-related settings, including the alert type, monitor, and thresholds, can be set from either subview location.

The following tables outline the type of status information available for each virtual entity type. The Subview Location column describes where the corresponding status fields are located in OneClick. For example, CA Spectrum lets you monitor "memory" information for your resource pool models. Thus, the corresponding status fields are available from the Resource Pool and VMware Manager subviews on the Information tab in OneClick. To explore the exact status options available for each status information type, locate the subview in OneClick.

Datacenter

Status Information Type	Subview Location
Overall	Datacenter and VMware Manager

Resource Pool

Status Information Type	Subview Location
Overall	Resource Pool and VMware Manager
CPU	Resource Pool and VMware Manager
Memory	Resource Pool and VMware Manager

Virtual Machine

Status Information Type	Subview Location
Percent ready	Virtual Machine and VMware Manager
CPU	Virtual Machine and VMware Manager
Memory	Virtual Machine and VMware Manager
Heartbeat	Virtual Machine and VMware Manager
Power	Virtual Machine and VMware Manager
OS state	Virtual Machine and VMware Manager
Connected	Virtual Machine and VMware Manager
VMware tools	Virtual Machine and VMware Manager
Virtual NICs	VMware Manager only

ESX Host

Status Information Type	Subview Location
CPU	ESX Host and VMware Manager
Sensor ■ CPU ■ Memory ■ Fan ■ Temperature ■ Voltage ■ Power	VMware Manager only
Physical NICs	VMware Manager only

ESX Service Console

Status Information Type	Subview Location
Memory	ESX Host and VMware Manager

Datastores

Status Information Type	Subview Location
Free space	vCenter only
Capacity	vCenter only

vCenter

Status Information Type	Subview Location
Overall	vCenter
CPU	vCenter
Memory	vCenter

More information:

Virtual Host Manager Alarms for VMware (see page 75)
Configure and Monitor Resource Status (see page 67)

How to Configure Management Options

After your virtual network is modeled, you can configure Virtual Host Manager options for viewing and managing your device models. Configuring your preferences helps ensure that Virtual Host Manager handles your virtual device models correctly and monitors only the information that is important to you.

To configure your installation of Virtual Host Manager, perform the following procedures after you discover and model your virtual network:

- Configure the vCenter Server AIM options. These options let you select settings for the CA SystemEDGE vCenter Server AIM, such as the vCenter Server AIM polling interval and various traps.
- Configure threshold values and other status monitoring options (see page 67). These options let you determine the information that you want to monitor and how CA Spectrum manages the various events that occur in your virtual network.

More information:

Upgrade the CA SystemEDGE Model (see page 42)

Configure the vCenter Server AIM

The vCenter Server AIM communicates with vCenter to manage and collect information about your virtual network. In Virtual Host Manager, you can configure the AIM to determine how it handles traps, and events. The AIM settings let you balance the information to gather against the amount of required resources.

To configure the vCenter Server AIM in Virtual Host Manager, use the following procedure.

Follow these steps:

1. Open Virtual Host Manager in the Navigation panel (see page 49).

   The main details page opens in the Contents panel for the selected Virtual Host Manager.
2. Locate and click your VMware Manager on the Explorer tab in the Navigation panel.

   The tabs in the Contents panel are populated with details about all vCenter servers.
3. Click the Information tab.
4. Expand the SystemEDGE Application Insight Modules (AIMs), VMware vCenter, Configuration subview.
5. Click Set to change the settings for the following fields, as needed:

   Trap Enable Mask

   Determines which class of traps the vCenter Server AIM sends. The value that is entered in this field determines the class. The values are as follows:

   0

   Sends no traps.

   1

   Sends detected vCenter change traps.

   2

   Sends detected AIM state change traps.

   3

   Sends detected vCenter change traps and detected AIM state change traps.

4

Sends AIM configuration change traps only.

5

Sends AIM configuration change and detected vCenter change traps.

6

Sends AIM configuration change traps and detected AIM state change traps.

7

(Default) Sends all traps.

Default: 7

Limits: 0-7

Log Level

Specifies the level of information that is written to the vCenter Server AIM log file. The levels are cumulative (for example, log level 4 writes all messages at levels 0 through 4). The following log levels are available:

- 0: Fatal
- 1: Critical
- 2: Warning
- 3: Info
- 4: Debug
- 5: Debug Low
- 6: Debug Lower
- 7: Debug Lowest

Default: 2

Note: Specifying a debug level greater than 4 is not recommended.

6. Expand Configuration, Instances subview.

   A table containing all vCenter server instances and their corresponding parameters are displayed.

7. In the Instances table, set any of the following parameters on the required vCenter server instance.

   Poll Interval (Seconds)

   Specifies the time interval (in seconds) when the vCenter Server AIM polls and caches status and modeling information from the vCenter server. This polling retrieves the following status and modeling updates and more:

   - Virtual machine powered down status
   - ESX host disconnected
   - New data center available
   - New ESX host
   - New virtual machine

   Default: 120

   Limits: Numbers greater than or equal to 30

   Note: For best results, we recommend that you set this interval no larger than the CA Spectrum poll cycle interval.

   VC Event Poll (Seconds)

   Specifies the time interval (in seconds) when the vCenter Server AIM polls and caches event information from the vCenter server. This polling interval affects the polling of the vCenter event queue.

   Default: 120

   Limits: Numbers greater than or equal to 120

   VC Event Enable

   Determines how Virtual Host Manager handles events that are collected from the vCenter server and from the vCenter Server AIM. The following options are available:

   Disable

   Specifies that no events are collected.

   Collect

   Specifies that events are gathered but no traps are sent for those events having traps.

   Collect and trap

   Specifies that the events are gathered and traps are sent.

   Default: Disable

VC Event Monitor Info

Determines whether vCenter information events are collected. The options are Enable and Disable.

Default: Disable

VC Event Monitor User

Determines whether vCenter user events are collected. The options are Enable and Disable.

Default: Disable

VC Event Monitor Error

Determines whether vCenter error events are collected. The options are Enable and Disable.

Default: Disable

VC Event Monitor Warning

Determines whether vCenter warning events are collected. The options are Enable and Disable.

Default: Disable

Your vCenter Server AIM is configured with your selections.

More information:

How to Configure Management Options (see page 62)

Configure and Monitor Resource Status

You can monitor the status of virtual resources in OneClick. For example, you can view the total physical memory, used physical memory, percent of free space on a datastore, and more. Also, you can set monitoring options, such as enabling alerts and setting threshold values for traps. This information can help you optimize your virtual network performance and troubleshoot alarms.

Note: The vCenter Server AIM sets and manages the traps, but you can configure these threshold values from the OneClick subviews. A read/write community string is required to change any threshold values or settings.

You can view or configure resource status options and information for virtual devices on the Information tab.

Follow these steps:

1. Open Virtual Host Manager in the Navigation panel (see page 49).

   The main details page opens in the Contents panel for the selected Virtual Host Manager.

2. Locate and click the virtual device on the Explorer tab in the Navigation panel.

   The device details display in the Contents panel.

3. Click the Information tab.

   Multiple subviews are available for viewing. Generally, the subview at the bottom of the tab includes the resource allocation and utilization information for the selected model. For example, a datacenter model displays a subview that is named "Datacenter Information". This subview includes details for the specific datacenter model that you selected in the Navigation panel.

4. Expand the appropriate subview.

   All available resource status details and monitoring options for the selected device model are displayed.

   Note: The VMware Manager model provides combined information for all virtual devices that the VMware Manager manages. Select the VMware Manager model in the Navigation panel to see information about all the vCenter servers and combined information about all of its entities. These entities include ESX hosts, ESX service consoles, virtual machines, virtual switches, NICs, and datastores. This information is the same data that is displayed on the Information tab for each individual entity model. The combined subview in the VMware Manager model can provide a good overview about all of the virtual entities that it manages.

More information:

Virtual Host Manager Alarms for VMware (see page 75)
How to Configure Management Options (see page 62)
Custom Subviews for Virtual Entity Types (see page 55)

Controlling vCenter Server AIM Polling

When tuning Virtual Host Manager performance, you can change the vCenter server polling rate or you can disable vCenter polling. By default, the polling attributes on the vCenter Server device model control the VMware-related polling behavior. Or you can change this VMware-related polling behavior independently. The vCenter application model, VMWareVCAIMApp, controls your VMware-related polling.

The following two attribute values on the application specifically control the VMware polling logic:

- PollingStatus
- Polling_Interval

Both the vCenter server and the VMWareVCAIMApp application model contain these attributes. PollingStatus enables and disables polling, while Polling_Interval controls the polling frequency. If their values are different, the VMWareVCAIMApp application model attribute values take precedence.

As stated, CA Spectrum allows you to set the values for the device model and application model separately. This capability lets you fine-tune your VMware-related polling independently of the vCenter server device polling. For both attributes, modifying the attribute on the vCenter Server device model also changes the corresponding application model attribute if their values are the same.

More information:

How vCenter Discovery Works (see page 43)

Configure the vCenter Server Polling Interval

You can change the vCenter server polling rate to increase or decrease the frequency. Configure the polling interval by setting the Polling_Interval attribute on the vCenter application model.

Follow these steps:

1. Open OneClick and click the Locater tab in the Navigation panel.
2. Expand the Application Models folder and double-click 'By Device IP Address.'

   A search dialog opens.
3. Enter the IP address for your vCenter server in the Device IP Address field and click OK.

   A list of application models for the vCenter server appears in the Contents panel.
4. Select the VMWareVCAIMApp application model.

   The application model details appear in the Component Details panel.
5. Click the Information tab in the Component Details panel.
6. Double-click the CA Spectrum Modeling Information subview.
7. Click Set in the Polling Interval (sec) field, enter a new value.

   Note: A value of 0 disables vCenter server polling.

   The vCenter server polling interval setting is configured.

Disable vCenter Server Polling

You can disable vCenter polling. Disabling vCenter polling is the same as disabling Virtual Host Manager. You can disable polling by setting the PollingStatus attribute on the vCenter application model.

To disable vCenter server polling on the application model, use the following procedure.

Follow these steps:

1. Open OneClick and click the Locater tab in the Navigation panel.
2. Expand the Application Models folder and double-click 'By Device IP Address.'

   A search dialog opens.
3. Enter the IP address for your vCenter server in the Device IP Address field, and click OK.

   A list of application models for the vCenter server appears in the Contents panel.

4. Select the VMWareVCAIMApp application model.

   The application model details appear in the Component Details panel.

5. Click the Information tab in the Component Details panel.
6. Click the CA Spectrum Modeling Information subview.
7. Click 'set' in the Polling field and select Off.

   Polling is disabled for the selected vCenter server.

Disabling DNS Lookup for Virtual Machines

Starting with 9.4 release, you can disable the DNS lookup for a virtual machine that has a blank IP address. You can have scenarios when you do not want CA Spectrum do the DNS lookup for a virtual machine with a blank IP address. In such scenarios, you can set the attribute "VMWare_vmDNSLookuponBlankIPAddr" to "No" at the Virtual Host Manager level in OneClick. When this attribute is set to "No", CA Spectrum skips the DNS lookup for a virtual machine with a blank IP address. As a result, the IP address of such a virtual machine is not populated in OneClick.

If this attribute is set to "Yes", CA Spectrum performs a DNS lookup to find the IP address of a virtual machine without IP address. If CA Spectrum finds the IP address of that virtual machine, that IP address is populated in the OneClick.

Deleting Virtual Host Manager Models

Generally, models can be deleted from OneClick at any time. However, Virtual Host Manager restricts your ability to delete models from the Virtual Host Manager hierarchy in the Navigation panel. To delete models manually, you have the following two options:

- Delete the VMware folder or a vCenter server model in Virtual Host Manager
- Remove a virtual entity from your VMware virtual environment using vCenter

In Virtual Host Manager, models are sometimes deleted automatically. The following circumstances cause CA Spectrum to delete Virtual Host Manager models automatically:

- **VMware folder or VMware Manager model is deleted**

  If you delete a VMware Manager model or the VMware folder, CA Spectrum deletes all related child models. The set of deleted models includes the vCenter Server model that is related to the remote VMware Manager model.

- **An entity is removed from VMware**

  As you delete data centers, resource pools, clusters, ESX hosts, and virtual machines in VMware, CA Spectrum also deletes those models and their child models from Virtual Host Manager.

- **Disabled data center in Virtual Host Manager**

  If you disable management of a data center, CA Spectrum deletes the child models that are related to that data center.

- **Upgraded models exist**—In some cases an ESX service console or virtual machine is first modeled for Virtual Host Manager without SNMP capabilities. If SNMP capabilities are later added to a VHM model (see definition on page 270), the previous model is deleted and replaced with the new SNMP-capable model.

Note: Although the default setting is to delete models, you can configure Virtual Host Manager to retain the models instead. In this case, Virtual Host Manager places the ESX host, ESX service console, and virtual machine models in the LostFound container when they are removed from Virtual Host Manager. This setting is respected when you remove an entity from VMware or you disable a data center in Virtual Host Manager. This setting does not apply when you delete the VMware folder or you delete a VMware Manager model. The setting also does not apply when you remove a VMware Manager and vCenter Server model or upgrade a VHM model.

More information:

Duplicate Models Created After SNMP and vCenter Discovery (see page 261)
Adding SNMP Capabilities to VHM Models (see page 45)
Manage Device Models for Devices Deleted from vCenter (see page 36)
Manage SNMP-Enabled Virtual Machine Models After VMware Manager Deletion (see page 39)

Distributed and Selective Management

This section describes the concepts and procedures for selectively managing individual data centers on your vCenter servers. This section also describes how to distribute the management of data centers across multiple SpectroSERVERs.

Selective Data Center Modeling

By default, each vCenter Server model monitors all data centers that it manages within your virtual environment. Virtual Host Manager lets you selectively monitor only a subset of these data centers. To perform selective modeling, you can configure each vCenter Server model to enable or disable modeling for the individual data centers that it manages.

This feature offers the following benefits:

- Organizations can disable management for data centers that do not require monitoring, such as a lab environment.
- Virtual Host Manager can distribute management of your virtual environment.

More information:

Distributed Management of Your Virtual Environment (see page 73)

How to Selectively Manage Your Datacenters

By default, each vCenter server model monitors all data centers that it manages within your virtual environment. However, you can configure your vCenter server models to monitor a subset of data centers. This feature is useful when you have data centers that do not require monitoring, such as a lab environment.

The following process describes how to configure your vCenter server to monitor only selected data centers:

1. Select your preference for automatically modeling data centers in Virtual Host Manager (see page 34). This setting is used as the default for your data center models in Step 3.
2. Model your vCenter server (see page 41).
3. Enable on each vCenter server the selected data centers for monitoring. The vCenter server models only the data centers and its contained components for which you enable modeling.

Distributed Management of Your Virtual Environment

Using the selective data center modeling feature, you can distribute the management of your data centers across multiple SpectroSERVERs. For large organizations with geographically dispersed networks or large virtual environments, the potential benefits include the following:

- Improved Virtual Host Manager performance—Resources required to model each data center can be spread across multiple SpectroSERVERs. Ideally, we recommend modeling using a single SpectroSERVER to reduce resources required to poll from multiple servers. However, if a single SpectroSERVER cannot effectively manage your virtual environment, a distributed environment can improve your Virtual Host Manager performance despite the additional polling resources required.
- Organizational flexibility—Because of organizational or geographical boundaries, you may prefer to distribute the management of data centers across multiple SpectroSERVERs.

You can accomplish distributed management by first modeling your vCenter servers on separate SpectroSERVERs. In each SpectroSERVER environment, you can then selectively enable or disable the data centers managed by each vCenter server.

For example, you model the 'cas' vCenter server on two SpectroSERVERs: SS_1 and SS_2. After vCenter Discovery, Virtual Host Manager discovers that 'cas' manages the following three data centers:

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

On each SpectroSERVER, you can configure data center modeling for 'cas' as follows:

Data Center	cas on SS_1	cas on SS_2
DCenter-A	enabled	disabled
DCenter-B	enabled	disabled
DCenter-C	disabled	enabled

In this scenario, management of the data centers for 'cas' is distributed across the two SpectroSERVERs.

Important! Distributed data center management is not a scalable solution. For every vCenter server that is modeled on a SpectroSERVER, Virtual Host Manager must poll *all* data center data during each polling interval. Therefore, even if you disable modeling for a data center, Virtual Host Manager polls the data center. To minimize duplication of effort when polling, be mindful of how many SpectroSERVERs model the same vCenter server.

More information:

Selective Data Center Modeling (see page 71)

How to Distribute Management of Your Virtual Environment

To help improve Virtual Host Manager performance or organization, you can use the selective data center modeling feature. Distributed management spreads your data center modeling across multiple SpectroSERVERs.

The process for distributing management is similar to the selective data center modeling process, with a few additional steps, as follows:

1. Select your preference for automatically modeling data centers in Virtual Host Manager (see page 34). In a distributed data center management environment, you must decide how to handle new data centers added to VMware. When configuring Virtual Host Manager for data center management, you have the following two options:

   - Disable automatic data center modeling for all SpectroSERVERs—In this case, you must manually model all new data centers that you want Virtual Host Manager to monitor. Although it requires manual modeling, this option helps ensure that Virtual Host Manager is monitoring only the data centers that require management.
   - Enable automatic data center modeling on *one* SpectroSERVER, and disable for all others—This option ensures that all new data centers are modeled on one SpectroSERVER. We recommend this option so that important network components are not forgotten. After your data center models appear in Virtual Host Manager, you can manually move their management to a different SpectroSERVER, if needed.

   Important! Do not enable automatic data center modeling on multiple SpectroSERVERs. Virtual Host Manager models all new data centers on multiple SpectroSERVERs, resulting in duplicate effort, which can affect Virtual Host Manager performance.

2. Model your vCenter server (see page 41). Be sure to model this vCenter server on each SpectroSERVER where you manage one or more of its data centers.
3. On each SpectroSERVER, enable on each vCenter server the selected data centers to monitor. The vCenter server models only the data centers and its contained components for which you enable modeling.
4. Configure the CA SystemEDGE agent to send traps to each SpectroSERVER (see page 75). To ensure that data centers are properly monitored, traps must be sent to all SpectroSERVERs where your vCenter servers are modeled.

Trap Management in a Distributed Data Center Environment

To monitor data centers and their components, the related traps must reach the SpectroSERVER where each data center is managed. In a distributed data center management scenario, configure the CA SystemEDGE agent to send traps to each SpectroSERVER where your vCenter servers are modeled.

When properly configured, CA Spectrum sends all traps that are generated by the vCenter Server AIM to these SpectroSERVERs. Each SpectroSERVER filters the traps and drops the traps that are generated for data centers and their components that are *not* modeled on that SpectroSERVER. Only the traps that are related to modeled data center components generate events and alarms.

Note: For more information about configuring traps on the vCenter Server AIM, see the *CA Virtual Assurance for Infrastructure Managers Implementation Guide*.

Alarms and Fault Isolation for VMWare

This section describes the traps used by Virtual Host Manager and the resulting alarms. This section also explains how Virtual Host Manager fault isolation differs from basic CA Spectrum fault isolation.

Virtual Host Manager Alarms for VMware

To alert you to problems within your virtual network, CA Spectrum generates alarms. Alarms are created in two ways:

- Traps sent from the CA SystemEDGE agent
- Polling

Two alarms are generated from polling: Powered Down/Suspended and Proxy Lost/Unavailable. However, several traps can generate alarms on your virtual devices. CA Spectrum supports all traps that are sent by the vCenter Server AIM from the CA SystemEDGE agent. To optimize these traps, you can configure the threshold values for each virtual device individually.

If a trap breaches your threshold value and generates an alarm, CA Spectrum uses the value of the “state” varbind passed with the trap to determine the alarm severity. All state varbinds have the following possible values, which receive the same CA Spectrum alarms:

- 0: Unknown
- 1: OK

- 2: Warning
- 3: Critical

CA Spectrum maps these vCenter states to a CA Spectrum alarm severity, as shown:

vCenter State	CA Spectrum Alarm Severity
0: Unknown	Clear
1: OK	Clear
2: Warning	Minor (Yellow)
3: Critical	Major (Orange)

More information:

Configure and Monitor Resource Status (see page 67)
Manage Device Models for Devices Deleted from vCenter (see page 36)
Manage SNMP-Enabled Virtual Machine Models After VMware Manager Deletion (see page 39)

How CA Spectrum Forwards Traps from CA SystemEDGE

CA Spectrum supports all traps that are sent by the vCenter Server AIM. These traps are initially sent to the vCenter CA SystemEDGE model. If the destination for a trap is not the vCenter model, CA Spectrum forwards the trap to the correct virtual model.

Note: For specific event codes related to the traps, use the Event Configuration application and filter on "0x056e." Or you can launch MIB tools to view the traps in the Trap Support table for the "EMPIRE-CAVMVCA-MIB" MIB. For more information about using the Event Configuration application, see the *Event Configuration User Guide*. For more information about using MIB tools, see the *Modeling and Managing Your IT Infrastructure Administrator Guide*.

CA Spectrum determines where to forward the trap by using the following process:

1. When CA Spectrum receives a trap, it maps the UID of the entity type to a well-known varbind location.

   Note: For the Host Sensor traps, CA Spectrum uses the virtual entity name, not the UID. If multiple hosts have the same vCenter name, CA Spectrum maps to the first entry.

2. CA Spectrum uses this UID to look up and locate the CA Spectrum model that is tied to a given UID. The entity type of all traps is predetermined. Depending on the results of the look-up, CA Spectrum forwards the trap as follows:

   - If it finds a CA Spectrum model of a specific type with a given UID, CA Spectrum forwards the event and corresponding alarm to the destination model.
   - If it cannot find a CA Spectrum model for a given UID, CA Spectrum generates a new generic event (0x56e109f) on the vCenter model. This new event includes the following details:
     - Trap details
     - Entity type searched for
     - Additional information from attempts to find the information about a model

     Note: CA Spectrum often cannot find a related model when a trap is sent immediately after changing your virtual network entities in vCenter. vCenter Discovery has not yet identified and created the corresponding model in CA Spectrum.

Traps Supported in Virtual Host Manager

All traps that are generated by the vCenter Server AIM are supported in CA Spectrum. The traps are initially sent to the vCenter model. Then they are forwarded to a corresponding virtual entity type (that is, the "destination" entity), depending on the type of trap. Using these traps, you can monitor the performance of your virtual network, resolve any resulting alarms, or trigger events.

Note: For more information about traps generated by the vCenter Server AIM, see the *CA Virtual Assurance for Infrastructure Managers Administration Guide* and *CA Virtual Assurance for Infrastructure Managers Administration Guide*.

The following tables list the traps for a specific destination entity type and specify whether the trap generates an alarm.

Cluster Traps

Trap Name	Trap OID	Alarm?
vmvcAimClusterHADRSChangeTrap	1.3.6.1.4.1.546.1.1.0.165253	No
vmvcAimClusterRenamedTrap	1.3.6.1.4.1.546.1.1.0.165254	No
vmvcAimClusterDRSConfigChangeTrap	1.3.6.1.4.1.546.1.1.0.165255	No

Data Center Traps

Trap Name	Trap OID	Alarm?
vmvcAimDCRenamedTrap	1.3.6.1.4.1.546.1.1.0.165248	No
vmvcAimDCConfigChangeTrap	1.3.6.1.4.1.546.1.1.0.165249	No
vmvcAimDCOverallStateChangeTrap	1.3.6.1.4.1.546.1.1.0.165240	Yes
vmvcAimDCTotalCPUStateChangeTrap	1.3.6.1.4.1.546.1.1.0.165245	Yes
vmvcAimDCTotalMEMStateChangeTrap	1.3.6.1.4.1.546.1.1.0.165250	Yes

ESX Host Traps

Trap Name	Trap OID	Alarm?
vmvcAimHostCpuStateChangeTrap	1.3.6.1.4.1.546.1.1.0.165208	Yes
vmvcAimHostTotalCpuStateChangeTrap	1.3.6.1.4.1.546.1.1.0.165209	Yes
vmvcAimHostTotalMemStateChangeTrap	1.3.6.1.4.1.546.1.1.0.165210	Yes
vmvcAimHostConfigChangeTrap	1.3.6.1.4.1.546.1.1.0.165212	No
vmvcAimHostTotalVMCpuStateChangeTrap	1.3.6.1.4.1.546.1.1.0.165213	Yes
vmvcAimHostThresholdChangeTrap	1.3.6.1.4.1.546.1.1.0.165215	No
vmvcAimHostVMotionTrap	1.3.6.1.4.1.546.1.1.0.165218	No
vmvcAimHostConnectionStateTrap	1.3.6.1.4.1.546.1.1.0.165219	No**
vmvcAimHostTotalVMMemStateChangeTrap	1.3.6.1.4.1.546.1.1.0.165220	Yes
vmvcAimPNICStateChangeTrap	1.3.6.1.4.1.546.1.1.0.165241	Yes
vmvcAimPNICAddedTrap	1.3.6.1.4.1.546.1.1.0.165242	No
vmvcAimPNICRemovedTrap	1.3.6.1.4.1.546.1.1.0.165243	No
vmvcAimPNICConfigChangeTrap	1.3.6.1.4.1.546.1.1.0.165244	No
vmvcAimHostDiskAddedTrap	1.3.6.1.4.1.546.1.1.0.165291	No
vmvcAimHostDiskRemovedTrap	1.3.6.1.4.1.546.1.1.0.165292	No

Trap Name	Trap OID	Alarm?
vmvcAimCPUSensorStateChangeTrap*	1.3.6.1.4.1.546.1.1.0.165281	Yes
vmvcAimMemSensorStateChangeTrap*	1.3.6.1.4.1.546.1.1.0.165282	Yes
vmvcAimFanSensorStateChangeTrap*	1.3.6.1.4.1.546.1.1.0.165283	Yes
vmvcAimVoltageSensorStateChangeTrap*	1.3.6.1.4.1.546.1.1.0.165284	Yes
vmvcAimTempSensorStateChangeTrap*	1.3.6.1.4.1.546.1.1.0.165285	Yes
vmvcAimPowerSensorStateChangeTrap*	1.3.6.1.4.1.546.1.1.0.165286	Yes
vmvcAimHostFTConfigChangeTrap	1.3.6.1.4.1.546.1.1.0.165955	No
vmvcAimHostPowerStateTrap	1.3.6.1.4.1.546.1.1.0.165910	No
vmvcAimStatVMSRMStatusChangeTrap	1.3.6.1.4.1.546.1.1.0.165969	No

*The vCenter ESX host name is used to locate the ESX host model in CA Spectrum. If two ESX host models exists with the same name, CA Spectrum alarms on the first model matching the name.

**These traps do not generate alarms because CA Spectrum vCenter polling intelligence detects and generates these alarms on the next vCenter polling cycle.

ESX Service Console Traps

Trap Name	Trap OID	Alarm?
vmvcAimHostMemStateChangeTrap	1.3.6.1.4.1.546.1.1.0.165211	Yes
vmvcAimHostMemOtherStateChangeTrap	1.3.6.1.4.1.546.1.1.0.165214	Yes

Note: Thresholds that generate these traps are configured using the Host Information subview for the ESX host model.

Resource Pool Traps

Trap Name	Trap OID	Alarm?
vmvcAimResourcePoolCpuStateChangeTrap	1.3.6.1.4.1.546.1.1.0.165258	Yes
vmvcAimResourcePoolConfigChangeTrap	1.3.6.1.4.1.546.1.1.0.165259	No
vmvcAimResourcePoolRenamedTrap	1.3.6.1.4.1.546.1.1.0.165260	No
vmvcAimResourcePoolMemStateChangeTrap	1.3.6.1.4.1.546.1.1.0.165264	Yes
vmvcAimResourcePoolHealthStateChangeTrap	1.3.6.1.4.1.546.1.1.0.165265	Yes
vmvcAimResourcePoolVCConfigChangeTrap	1.3.6.1.4.1.546.1.1.0.165962	No

vCenter Server Traps

CA Spectrum asserts the vCenter Server traps on the VMware Manager and vCenter Server models or on the vCenter Server model only, depending on your CA SystemEDGE deployment scenario.

Trap Name	Trap OID	Alarm?
vmvcAimServerStateChangeTrap	1.3.6.1.4.1.546.1.1.0.165201	Yes
vmvcAimVCCPUStateChangeTrap	1.3.6.1.4.1.546.1.1.0.165203	Yes
vmvcAimVCMemStateChangeTrap	1.3.6.1.4.1.546.1.1.0.165206	Yes
vmvcAimHostAddedTrap***	1.3.6.1.4.1.546.1.1.0.165216	No
vmvcAimHostRemovedTrap***	1.3.6.1.4.1.546.1.1.0.165217	No
vmvcAimVMAddedTrap***	1.3.6.1.4.1.546.1.1.0.165222	No
vmvcAimVMRemovedTrap***	1.3.6.1.4.1.546.1.1.0.165223	No
vmvcAimVMMigratedTrap***	1.3.6.1.4.1.546.1.1.0.165230	No
vmvcAimDCAddedTrap***	1.3.6.1.4.1.546.1.1.0.165246	No
vmvcAimDCRemovedTrap***	1.3.6.1.4.1.546.1.1.0.165247	No
vmvcAimClusterAddedTrap***	1.3.6.1.4.1.546.1.1.0.165251	No
vmvcAimClusterRemovedTrap***	1.3.6.1.4.1.546.1.1.0.165252	No
vmvcAimResourcePoolAddedTrap***	1.3.6.1.4.1.546.1.1.0.165256	No
vmvcAimResourcePoolRemovedTrap***	1.3.6.1.4.1.546.1.1.0.165257	No
vmvcAimTemplateAddedTrap	1.3.6.1.4.1.546.1.1.0.165261	No
vmvcAimTemplateRemovedTrap	1.3.6.1.4.1.546.1.1.0.165262	No
vmvcAimTemplateRenamedTrap	1.3.6.1.4.1.546.1.1.0.165263	No
vmvcAimCustomizationSpecAddedTrap	1.3.6.1.4.1.546.1.1.0.165266	No
vmvcAimCustomizationSpecRemovedTrap	1.3.6.1.4.1.546.1.1.0.165267	No
vmvcAimDatastoreAddedTrap	1.3.6.1.4.1.546.1.1.0.165271	No
vmvcAimDatastoreRemovedTrap	1.3.6.1.4.1.546.1.1.0.165272	No
vmvcAimDatastoreAccessibleStateChangeTrap	1.3.6.1.4.1.546.1.1.0.165273	Yes
vmvcAimDatastoreConfigChangeTrap	1.3.6.1.4.1.546.1.1.0.165274	No
vmvcAimDatastoreRenamedTrap	1.3.6.1.4.1.546.1.1.0.165275	No
vmvcAimDatastoreFreeSpaceStateChangeTrap	1.3.6.1.4.1.546.1.1.0.165276	Yes
vmvcAimDCFolderAddedTrap	1.3.6.1.4.1.546.1.1.0.165277	No
vmvcAimDCFolderRemovedTrap	1.3.6.1.4.1.546.1.1.0.165278	No
vmvcAimDCFolderConfigChangeTrap	1.3.6.1.4.1.546.1.1.0.165279	No

Trap Name	Trap OID	Alarm?
vmvcAimSnapshotAddedTrap	1.3.6.1.4.1.546.1.1.0.165287	No
vmvcAimSnapshotRemovedTrap	1.3.6.1.4.1.546.1.1.0.165288	No
vmvcAimSnapshotCurrentUpdateTrap	1.3.6.1.4.1.546.1.1.0.165289	No
vmvcAimSCSIControllerAddedTrap	1.3.6.1.4.1.546.1.1.0.165296	No
vmvcAimSCSIControllerRemovedTrap	1.3.6.1.4.1.546.1.1.0.165297	No
vmvcAimServerTotalCPUStateChangeTrap	1.3.6.1.4.1.546.1.1.0.165293	Yes
vmvcAimServerTotalMemStateChangeTrap	1.3.6.1.4.1.546.1.1.0.165294	Yes
vmvcAimServerTotalDSFreeSpaceStateChangeTrap	1.3.6.1.4.1.546.1.1.0.165295	Yes
vmvcAimVSwitchStateChangeTrap	1.3.6.1.4.1.546.1.1.0.165235	Yes
vmvcAimVMGuestDiskAddedTrap	1.3.6.1.4.1.546.1.1.0.165920	No
vmvcAimVMGuestDiskRemovedTrap	1.3.6.1.4.1.546.1.1.0.165921	No
vmvcAimVMGuestDiskStateChangeTrap	1.3.6.1.4.1.546.1.1.0.165922	No
vmvcAimVMGuestDiskConfigChangeTrap	1.3.6.1.4.1.546.1.1.0.165923	No
vmvcAimStorageSensorStateChangeTrap	1.3.6.1.4.1.546.1.1.0.165905	Yes

***These events are generated on the vCenter server because vCenter Discovery generates similar events on each entity that is discovered or removed from CA Spectrum management.

VMware Manager Traps

Trap Name	Trap OID	Alarm?
vmvcAimServerReadyTrap	1.3.6.1.4.1.546.1.1.0.165200	No
vmvcAimVCConfigChangeTrap	1.3.6.1.4.1.546.1.1.0.165202	No
vmvcAimVCThresholdChangeTrap	1.3.6.1.4.1.546.1.1.0.165204	No
vmvcAimVCEventReceivedTrap	1.3.6.1.4.1.546.1.1.0.165205	No
vmvcAimVSwitchAddedTrap	1.3.6.1.4.1.546.1.1.0.165915	No
vmvcAimVSwitchRemovedTrap	1.3.6.1.4.1.546.1.1.0.165916	No
vmvcAimVSwitchConfigChangeTrap	1.3.6.1.4.1.546.1.1.0.165917	No
vmvcAimHostVNICAddedTrap	1.3.6.1.4.1.546.1.1.0.165925	No
vmvcAimHostVNICRemovedTrap	1.3.6.1.4.1.546.1.1.0.165926	No
vmvcAimPortGroupAddedTrap	1.3.6.1.4.1.546.1.1.0.165930	No
vmvcAimPortGroupRemovedTrap	1.3.6.1.4.1.546.1.1.0.165931	No

Trap Name	Trap OID	Alarm?
vmvcAimPortGroupVCConfigChangeTrap	1.3.6.1.4.1.546.1.1.0.165932	No
vmvcAimDistribVSwitchAddedTrap	1.3.6.1.4.1.546.1.1.0.165935	No
vmvcAimDistribVSwitchRemovedTrap	1.3.6.1.4.1.546.1.1.0.165936	No
vmvcAimDistribVSwitchStateChangeTrap	1.3.6.1.4.1.546.1.1.0.165937	Yes
vmvcAimDistribVSwitchConfigChangeTrap	1.3.6.1.4.1.546.1.1.0.165938	No
vmvcAimDistribVSwitchVCConfigChangeTrap	1.3.6.1.4.1.546.1.1.0.165939	No
vmvcAimDVPortGroupAddedTrap	1.3.6.1.4.1.546.1.1.0.165940	No
vmvcAimDVPortGroupRemovedTrap	1.3.6.1.4.1.546.1.1.0.165941	No
vmvcAimDVPortGroupVCConfigChangeTrap	1.3.6.1.4.1.546.1.1.0.165942	No
vmvcAimDVUplinkPortGroupAddedTrap	1.3.6.1.4.1.546.1.1.0.165943	No
vmvcAimDVUplinkPortGroupRemovedTrap	1.3.6.1.4.1.546.1.1.0.165944	No
vmvcAimDVUplinkPortGroupVCConfigChangeTrap	1.3.6.1.4.1.546.1.1.0.165945	No
vmvcAimDistribVSwitchPortPolicyChangeTrap	1.3.6.1.4.1.546.1.1.0.165950	No
vmvcAimDVPortGroupPortPolicyChangeTrap	1.3.6.1.4.1.546.1.1.0.165951	No
vmvcAimCustSpecNICAddedTrap	1.3.6.1.4.1.546.1.1.0.165960	No
vmvcAimCustSpecNICRemovedTrap	1.3.6.1.4.1.546.1.1.0.165961	No
vmvcAimVAppAddedTrap	1.3.6.1.4.1.546.1.1.0.165963	No
vmvcAimVAppRemovedTrap	1.3.6.1.4.1.546.1.1.0.165964	No
vmvcAimVAppVCConfigChangeTrap	1.3.6.1.4.1.546.1.1.0.165965	No
vmvcAimVMAddedTovAppTrap	1.3.6.1.4.1.546.1.1.0.165966	No
vmvcAimVMRemovedFromvAppTrap	1.3.6.1.4.1.546.1.1.0.165967	No
vmvcAimVMvAppVCConfigChangeTrap	1.3.6.1.4.1.546.1.1.0.165968	No
vmvcAimNetFolderAddedTrap	1.3.6.1.4.1.546.1.1.0.165970	No
vmvcAimNetFolderRemovedTrap	1.3.6.1.4.1.546.1.1.0.165971	No
vmvcAimNetFolderConfigChangeTrap	1.3.6.1.4.1.546.1.1.0.165972	No
vmvcAimCustomizationSpecChangeTrap	1.3.6.1.4.1.546.1.1.0.165280	No
vmvcAimCustSpecNICChangeTrap	1.3.6.1.4.1.546.1.1.0.165973	No

Virtual Machine Traps

Trap Name	Trap OID	Alarm?
vmvcAimVMCpuStateChangeTrap	1.3.6.1.4.1.546.1.1.0.165221	Yes
vmvcAimVMConfigChangeTrap	1.3.6.1.4.1.546.1.1.0.165224	No
vmvcAimVMThresholdChangeTrap	1.3.6.1.4.1.546.1.1.0.165225	No
vmvcAimVMPercentReadyTrap	1.3.6.1.4.1.546.1.1.0.165226	Yes
vmvcAimVMRenamedTrap	1.3.6.1.4.1.546.1.1.0.165227	No
vmvcAimVMBehaviourChangeTrap	1.3.6.1.4.1.546.1.1.0.165228	No
vmvcAimVMConnectionStateChangeTrap	1.3.6.1.4.1.546.1.1.0.165229	No**
vmvcAimVMNICStateChangeTrap	1.3.6.1.4.1.546.1.1.0.165231	Yes
vmvcAimVMNICAddedTrap	1.3.6.1.4.1.546.1.1.0.165232	No
vmvcAimVMNICRemovedTrap	1.3.6.1.4.1.546.1.1.0.165233	No
vmvcAimVMNICConfigChangeTrap	1.3.6.1.4.1.546.1.1.0.165234	No
vmvcAimVMVDiskStateChangeTrap	1.3.6.1.4.1.546.1.1.0.165236	Yes
vmvcAimVMVDiskAddedTrap	1.3.6.1.4.1.546.1.1.0.165237	No
vmvcAimVMVDiskRemovedTrap	1.3.6.1.4.1.546.1.1.0.165238	No
vmvcAimVMVDiskConfigChangeTrap	1.3.6.1.4.1.546.1.1.0.165239	No
vmvcAimVMMemStateChangeTrap	1.3.6.1.4.1.546.1.1.0.165268	Yes
vmvcAimVMPowerStateChangeTrap	1.3.6.1.4.1.546.1.1.0.165269	No**
vmvcAimVMHBStateChangeTrap	1.3.6.1.4.1.546.1.1.0.165270	No
vmvcAimVMFTConfigChangeTrap	1.3.6.1.4.1.546.1.1.0.165956	No
vmvcAimVMFTFailoverTrap	1.3.6.1.4.1.546.1.1.0.165957	Yes
vmvcAimVMVCConfigChangeTrap	1.3.6.1.4.1.546.1.1.0.165958	No
vmvcAimVMVDiskSizeChangeTrap	1.3.6.1.4.1.546.1.1.0.165902	No

**These traps do not generate alarms because CA Spectrum vCenter polling intelligence detects and generates these alarms on the next vCenter polling cycle.

More information:

Configure and Monitor Resource Status (see page 67)
How to Configure Management Options (see page 62)
How CA Spectrum Forwards Traps from CA SystemEDGE (see page 76)

Fault Management for Virtual Networks

The goal of fault isolation is to narrow down the root cause of a networking problem. Finding the root cause can help you to troubleshoot and quickly correct the problem or to correct the problem programmatically with automated scripts. Deciding which devices are the root cause of an alarm can be difficult, because problems with a single device can cause several devices in your network to generate events.

For example, losing contact with an ESX host often means that you have also lost contact with the virtual machines that the ESX manages. Therefore, the ESX device model and all affected virtual machines generate alarms. Using fault isolation techniques, Virtual Host Manager correlates these alarms to identify a single root cause.

Virtual networks provide a unique management opportunity because they provide CA Spectrum an alternate management perspective. CA Spectrum can gather information through direct contact with your virtual devices or through the virtual network management application, VMware vCenter. This alternate management perspective enhances standard CA Spectrum fault management in two ways:

- **Enhanced contact lost alarms**—Two sources of information about a device mean Virtual Host Manager can pinpoint the cause and more easily correlate events to a single root cause.
- **Proxy failure alarms**—*Proxy management* is the act of managing network devices using an alternate management source in place of or in addition to the primary manager. For example, CA Spectrum can manage virtual network devices by contacting them directly or through the virtual technology application's contact with the devices. When vCenter loses contact with a virtual network device, Virtual Host Manager generates a Proxy Management Lost alarm for each device. These alarms are unique,alerting you that *management* of the device through the *proxy* is affected, not the state of the device or direct (SNMP) management.

How Fault Isolation Works when Device Contact is Lost

To help you troubleshoot networking problems with your devices, CA Spectrum uses fault isolation to narrow down the root cause of an alarm. For virtual networks, Virtual Host Manager uses information from direct contact with the device plus information provided by vCenter through the vCenter Server AIM. In many cases, standard CA Spectrum fault management can pinpoint the root cause. But in special circumstances, the method for isolating problems in a virtual network goes beyond the standard methods.

The type of fault isolation Virtual Host Manager uses to discover the root cause depends on which devices are alarming and the type of events the devices generate. The following scenarios describe two unique fault management situations and how CA Spectrum isolates the networking error in your virtual network.

Scenario 1: Virtual machine is powered down or suspended

In a virtual environment, the virtual management application can provide more details than CA Spectrum can discover through standard device monitoring. For example, the management application is aware when a virtual machine is placed into one of the following modes:

- Powered down
- Suspended

If a virtual machine is in one of these modes and CA Spectrum loses contact with it, but proxy management (see definition on page 269) of the ESX host is uninterrupted, CA Spectrum determines the root cause as follows:

1. When CA Spectrum loses contact with the virtual machine, it generates a Contact Lost alarm.
2. During its next polling cycle, the vCenter server model polls the vCenter Server AIM to gather information about the virtual machines. Because vCenter manages the virtual machines, it can provide a unique view into the possible cause of alarms generated by a virtual machine.
3. If vCenter finds that a virtual machine is powered down or suspended, it generates the appropriate alarm.

   Note: The Powered Down and Suspend alarms are cleared upon the first vCenter polling cycle after the virtual machine is powered on.
4. Virtual Host Manager correlates these Powered Down and Suspend alarms to the corresponding Contact Lost alarm created by CA Spectrum. Virtual Host Manager makes the Contact Lost alarm appear as a symptom of the Powered Down or Suspend alarms.

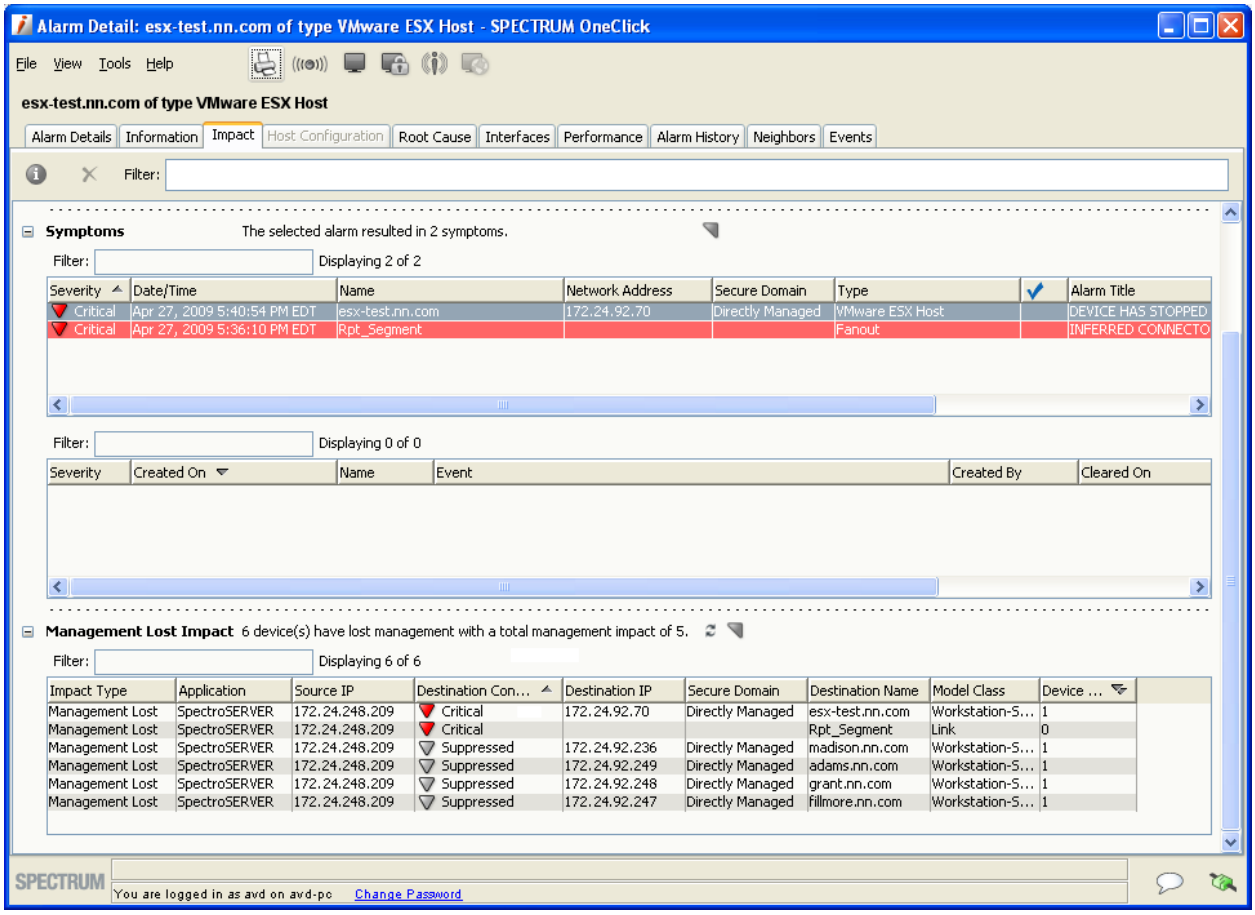
Scenario 2: ESX host is down

If CA Spectrum loses contact with a modeled ESX service console and all virtual machines running on that host, CA Spectrum checks the status of the upstream routers and switches. Depending on their status, CA Spectrum determines the root cause as follows:

- All upstream devices for one or more virtual machines or the ESX service console are unavailable—Standard CA Spectrum fault isolation techniques determine the root cause, as follows:
  - Device Stopped Responding to Polls alarm—Generated on the ESX host when at least one upstream connected device for any virtual machine or ESX service console is up.
  - Gateway Unreachable alarm—Generated on the ESX host when *all* upstream connected devices are down.
- At least one upstream device is available for every virtual machine and ESX service console model connected to the ESX host—CA Spectrum infers that the ESX host is the root cause and responds as follows:
  a. The ESX service console model and all virtual machines, ports, and fanouts that are directly connected to the ESX service console model or virtual machine models generate the standard fault isolation alarms.
  b. Virtual Host Manager creates a Physical Host Down alarm for the ESX host model.
  c. All fault isolation-related alarms that are created for the impacted devices (such as virtual machines, ESX service consoles, ports, and fanouts) are correlated to the Physical Host Down alarm, making them symptoms of the Physical Host Down alarm. These symptom alarms appear in the Symptoms table on the Impact tab for the Physical Host Down alarm.

     Note: For each ESX host model, Virtual Host Manager creates a "virtual fault domain." This domain includes the ESX host, ESX service console, and virtual machines, plus all ports and fanouts directly connected to the ESX service console model or virtual machines. When the ESX host generates the Physical Host Down alarm, all standard fault isolation alarms within the domain are correlated to it. Correlating these alarms as symptoms indicates that the Physical Host Down alarm on the ESX host is the root cause.
  d. All impacted devices are listed in the Management Lost Impact table on the Impact tab for the Physical Host Down alarm.

Note: Devices that are suppressed do not have a corresponding alarm in the Symptoms table, which is why the following example shows only two alarms but six impacted devices:



e. If all upstream devices for one or more virtual machines or the ESX service console go down, CA Spectrum can no longer reliably state that the fault lies with the ESX host. Therefore, CA Spectrum clears the Physical Host Down alarm and applies the standard CA Spectrum fault isolation techniques.

More information:

Determining Virtual Machines Affected by ESX Outages (see page 90)

How Fault Isolation Works when Proxy Management is Lost

The VMware vCenter application used to create your virtual network provides CA Spectrum a unique management opportunity. CA Spectrum can use the standard methods to contact your virtual devices directly, plus CA Spectrum can simultaneously gather virtual device information from vCenter. In this sense, vCenter is a "proxy" from which CA Spectrum gathers virtual device information. If CA Spectrum loses direct contact with a device, it generates alarms. Likewise, if vCenter loses contact with a virtual device or if Virtual Host Manager loses contact with the vCenter application, Virtual Host Manager generates alarms—Proxy Management Lost alarms (see definition on page 269).

In response, CA Spectrum attempts to isolate the cause of the proxy management failure. Proxy fault isolation is similar to the standard CA Spectrum fault isolation, except that these alarms alert you to the fact that *proxy* management of a virtual device is affected. Proxy management fault isolation cannot tell you whether a virtual device is up or down. However, it is important to know when contact through the proxy is lost, because you could be missing important virtual information about a device.

The type of proxy fault isolation Virtual Host Manager uses to discover the root cause depends on which devices are alarming and the type of events the devices generate. The following scenarios describe two unique proxy fault management situations and how Virtual Host Manager isolates the networking error in your virtual network.

Scenario 1: Contact between vCenter and ESX is lost

If vCenter loses contact with one of the ESX hosts it is managing, the vCenter data about that ESX and all hosted virtual devices is lost. To isolate the problem, Virtual Host Manager determines the root cause as follows:

1. A Proxy Management Lost alarm is generated on the ESX host, ESX service console, all hosted virtual machines, and any resource pools defined in that ESX.
2. The virtual machine alarms are correlated to the ESX Proxy Management Lost alarm, making them symptoms of the ESX alarm. Correlating these alarms as symptoms indicates that the ESX alarm is the root cause.
3. If CA Spectrum also loses contact with the ESX host and generates a Physical Host Down alarm, the Proxy Management Lost alarm generated for the ESX is correlated to the Physical Host Down alarm. In this case, the Proxy Management Lost alarm becomes a symptom of the Physical Host Down alarm. Correlating this alarm as a symptom indicates that the Physical Host Down alarm on the ESX is the root cause.

Scenario 2: Contact between CA Spectrum and vCenter is lost

If CA Spectrum loses contact with a vCenter model, CA Spectrum loses vCenter data about all virtual models managed by that vCenter server. To isolate the problem, Virtual Host Manager determines the root cause as follows:

1. CA Spectrum generates Proxy Management Lost alarms for all virtual models managed by that vCenter server, including virtual machines, ESX hosts, ESX service consoles, datacenters, resource pools, and clusters. CA Spectrum also generates a separate Proxy Unavailable alarm that vCenter server model.
2. The virtual machine alarms are correlated to their corresponding ESX model alarm.
3. The ESX, datacenter, resource pool, and cluster alarms are correlated to the vCenter model Proxy Unavailable alarm.
4. The vCenter alarm is correlated to another alarm generated by standard CA Spectrum fault management, such as the alarms created for the following situations:
   - Lost management of vCenter (that is, a problem occurred with the remote SystemEDGE agent)
   - Machine contact is lost
   - vCenter is in maintenance mode

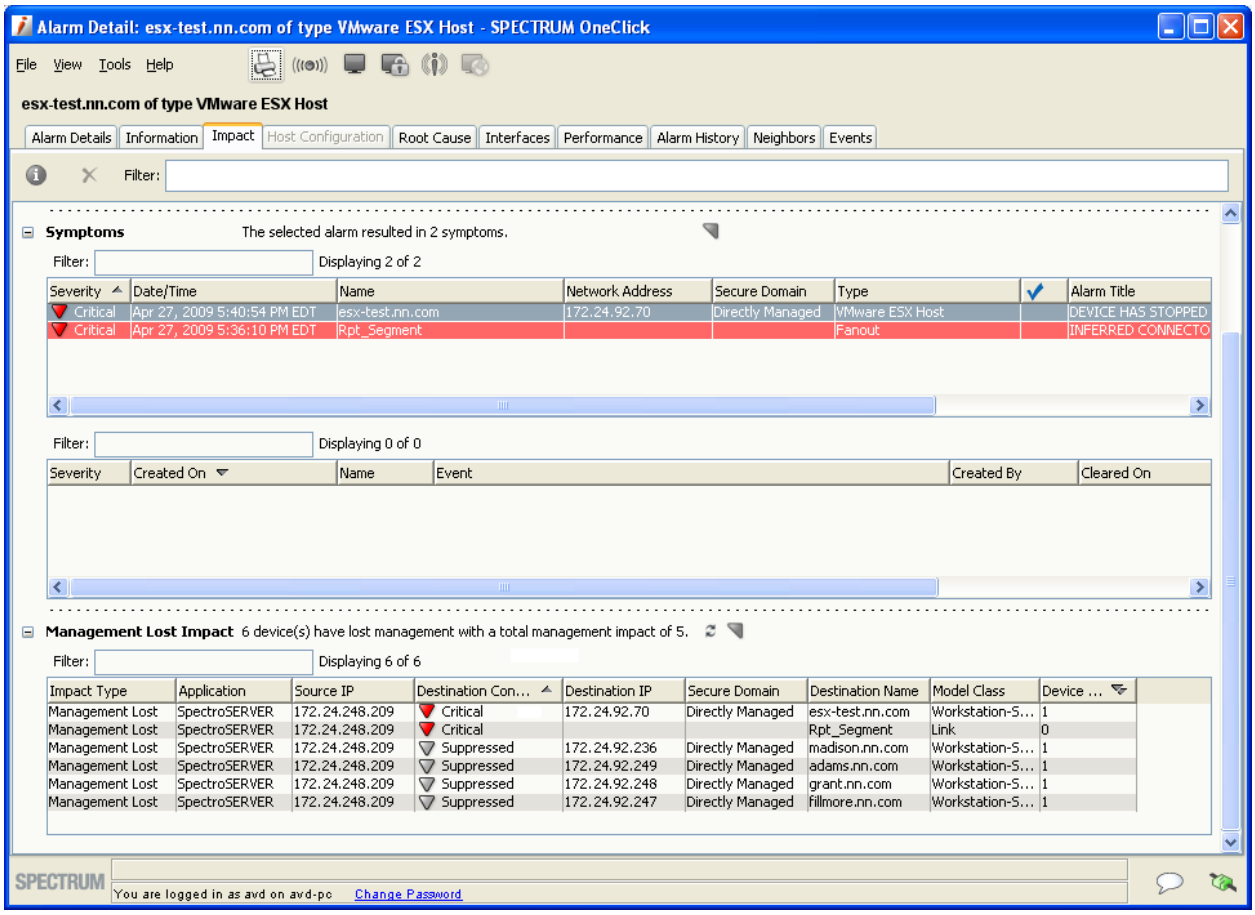
More information:

How Fault Isolation Works when Device Contact is Lost (see page 84)

Determining Virtual Machines Affected by ESX Outages

When contact with an ESX is interrupted or the ESX goes down, all virtual machines hosted by the ESX are affected. Because vCenter cannot communicate with the ESX to get usage information, you might not receive alarms for a critical virtual machine that is hosted on that ESX. To find out whether a critical virtual machine is affected, access a list of affected virtual machines on the Impact tab of the alarm. The following views are available:

- Symptoms view—displays all symptom alarms that the affected virtual machines generate
- Management Lost Impact view—lists the virtual machines that are affected by the alarm



More information:

How Fault Isolation Works when Device Contact is Lost (see page 84)

Chapter 4: Solaris Zones

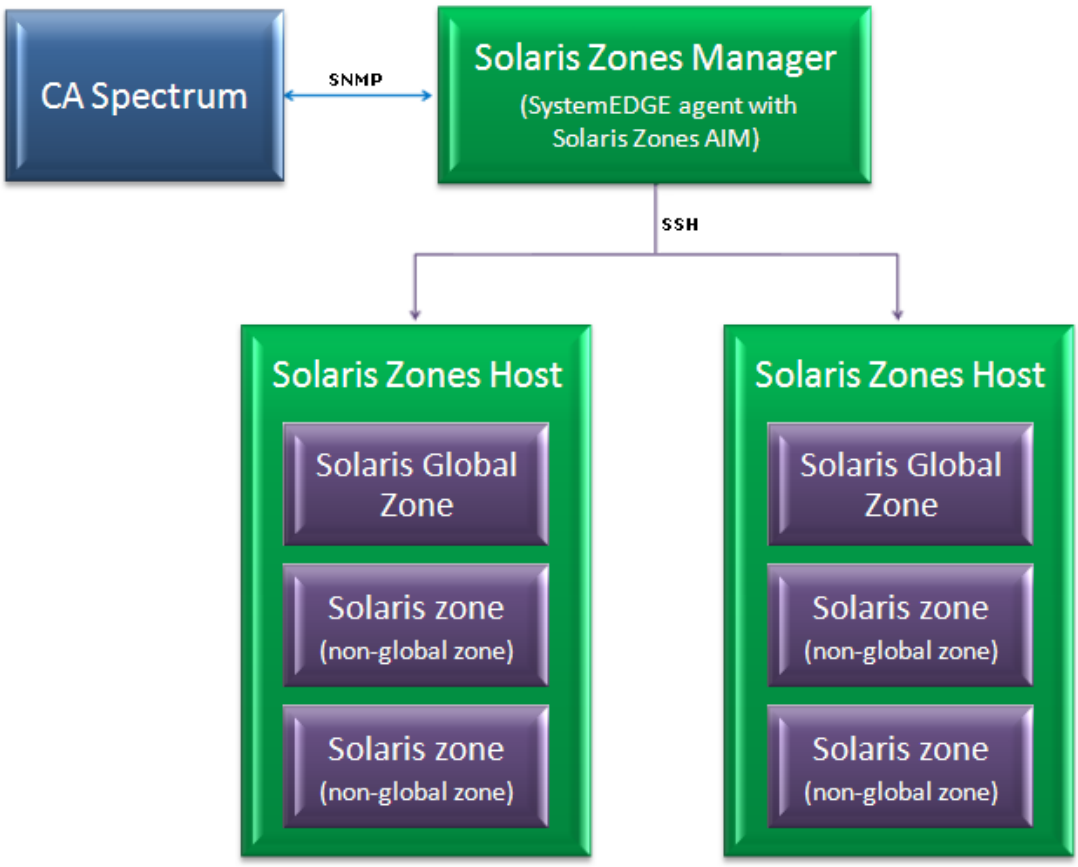
This section is for Solaris Zones virtualization technology users and describes how to use Virtual Host Manager to manage your virtual entities created with Solaris Zones.

This section contains the following topics:

How Virtual Host Manager Works with Solaris Zones

Virtual Host Manager monitor your virtual network entities seamlessly with your physical network entities. You get a full view of your network where you can troubleshoot networking issues for both types of entities. Although your virtual network entities behave like physical components, the process for monitoring those entities differs from the general CA Spectrum monitoring process. Understanding how this process works can help you locate and resolve networking issues related to your virtual network.

The *Solaris Zones Manager* in Virtual Host Manager is the CA SystemEDGE agent with the Solaris Zones AIM enabled. The Solaris Zones Managers are responsible for reporting on all of the configured Solaris zones. Virtual Host Manager communicates with the Solaris Zones Managers to gather details about your Solaris Zones virtual environment. The following diagram shows how CA Spectrum gathers information about your Solaris Zones virtual environment using the Solaris Zones Manager:



As shown in the diagram, the process to gather information about your Solaris Zones virtual environment is as follows:

1. The Solaris Global Zone in each Solaris Zones Host communicates with each Solaris zone (that is, the non-global zones) it contains.
2. The Solaris Zones Manager uses SSH to communicate with each Solaris Global Zones to gather details about your virtual environment.
3. Periodically, CA Spectrum communicates with the Solaris Zones Manager to retrieve this information. The Solaris Zones Manager has the CA SystemEDGE agent installed with the Solaris Zones AIM enabled. CA Spectrum uses SNMP to communicate with the CA SystemEDGE agent and uses the information to model and monitor your virtual environment in CA Spectrum.

More information:

How Virtual Host Manager Works (see page 11)
Understanding the Virtual Topology (see page 115)
How the Solaris Zones Data is Updated in Virtual Host Manager (see page 119)

Models Created for Solaris Zones

Virtual Host Manager provides several models to represent the components of your Solaris Zones virtual technology network. Understanding the following basic models can help you better understand Discovery and how the virtual environment interfaces with your physical environment:

- **Solaris Zones Manager**

  Each Solaris Zones Manager represents a server that contains the CA SystemEDGE agent with Solaris Zones AIM loaded.

- **Solaris Zones Host**

  Solaris Zones Hosts represent the physical hardware of the Solaris Host managed by Virtual Host Manager. These models serve as container models within the Universe topology, helping to group your virtual entities into a separate view while showing where the virtual environment interfaces with your physical network. The Solaris Zones Host cannot be contacted directly for status information. Instead, the status of these models is inferred from the status of its contained items.

- **Solaris Global Zone**

  The *Solaris Global Zone* is the management operating system running on the Solaris Zones Host that Solaris Zones uses to configure the hosted Solaris zone instances. The Solaris Global Zone models provide Virtual Host Manager a means to gather information about your Solaris Zones virtual environment.

- **Solaris zone**

  A *Solaris zone* is a non-global zone instance managed by Virtual Host Manager that runs on a Solaris Zones Host.

More information:

Viewing Your Solaris Zones Virtual Environment (see page 115)

Getting Started with Solaris Zones

This section describes the configuration and modeling process for Virtual Host Manager. These tasks are typically performed only once per installation by the administrator.

How to Configure Discovery Options

After Virtual Host Manager is installed, you can configure Virtual Host Manager for Solaris Zones Discovery. Configuring your preferences helps ensure that Virtual Host Manager models your virtual devices correctly.

To configure your installation of Virtual Host Manager for Solaris Zones Discovery, select your preferences from the following options:

- Maintenance Mode for New Solaris Zones (see page 95)—Lets you decide which newly discovered Solaris zone instances to place into maintenance mode until you are ready for CA Spectrum to manage them.
- Allow Device Model Deletes During Solaris Zones Discovery (see page 96)—Controls how CA Spectrum handles Solaris Zones virtualization technology models when Virtual Host Manager no longer manages them.
- Search for Existing Models (see page 97)—Determines which secure domains Virtual Host Manager searches during a Solaris Zones Discovery.

- Discover SNMP-Capable Devices (see page 98)—Controls how SNMP-capable devices are modeled during Solaris Zones Discovery. By default, new models are initially created as VHM models only. But, this option lets you override the default and immediately create SNMP models for devices that meet the necessary criteria.
- Retain SNMP-enabled Solaris Zones During Solaris Zones Manager Deletion (see page 99)—Controls how CA Spectrum handles SNMP-enabled Solaris zone models when a Solaris Zones Manager model is deleted.

Configure Maintenance Mode for New Solaris Zone Instances

Virtual Host Manager automatically models the Solaris zone instances in your Solaris Zones virtual environment. CA Spectrum attempts to manage all models that are discovered. However, some new Solaris zones are not ready for CA Spectrum management when they are initially modeled. For example, a non-running Solaris zone causes CA Spectrum to generate a Contact Lost alarm. To prevent undesired alarms on new Solaris zone models, you can decide which new models are immediately placed into maintenance mode. Later, you can manually disable maintenance mode when you are ready for CA Spectrum to manage these devices.

Follow these steps:

1. Open Virtual Host Manager in the Navigation panel (see page 115).

   The main details page opens in the Contents panel for the selected Virtual Host Manager.

2. Click the Information tab.
3. Expand the Configuration, Solaris Zones, Solaris Zones Discovery subview.
4. Click Set in the 'Maintenance Mode for New Solaris Zones' field and select one of the following options:

   Place non-running Solaris zones in Maintenance Mode

   (Default) Applies maintenance mode to only non-running Solaris zone models upon initial Solaris Zones Discovery.

   Place all Solaris zones in Maintenance Mode

   Applies maintenance mode to all new Solaris zone models upon initial Solaris Zones Discovery.

   Your setting is saved and new Solaris zone instances created by Virtual Host Manager are placed into maintenance mode per your selection.

More information:

How to Configure Discovery Options (see page 94)
Status Monitoring Options (see page 122)

Manage Device Models for Devices Deleted from Solaris

The devices and the relationships among them change frequently in virtual environments. Maintaining accurate and timely data about your virtual environment in CA Spectrum is challenging. For example, when a Solaris Zones Host or Solaris zone instance is removed, CA Spectrum removes the corresponding device models from Virtual Host Manager in the Navigation panel. However, should CA Spectrum retain or delete the model? You can select settings to control model deletion.

Important! When models are deleted, all notes or other customizations on those models are lost. You can disable this option if your models are likely to be recreated in your Solaris Zones environment later.

Follow these steps:

1. Open Virtual Host Manager in the Navigation panel (see page 115).

   The main details page opens in the Contents panel for the selected Virtual Host Manager.

2. Click the Information tab.

3. Expand the Configuration, Solaris Zones, Solaris Zones Discovery subview.

4. Click Set in the 'Allow Device Model Deletes During Solaris Zones Discovery' field and select one of the following options:

   Yes

   (Default) Deletes the Virtual Host Manager models that correspond to entities no longer managed by your Solaris Zones environment.

   No

   Places Virtual Host Manager models in the LostFound container if their corresponding entity is no longer managed by your Solaris Zones environment.

   Note: Models with more associations, such as a model that is included in a Global Collection, are handled differently. These models are removed from the Universe, but they are not moved to the LostFound container.

   Your setting is saved, and device models are handled accordingly after the device is deleted from your Solaris Zones environment.

More information:

How to Configure Discovery Options (see page 94)
Deleting Virtual Host Manager Models (see page 114)
Virtual Host Manager Alarms for Solaris Zones (see page 125)
Traps Supported in Virtual Host Manager (see page 127)
Move a Solaris Zone Instance to a New Solaris Zones Host (see page 108)
Duplicate MAC, Different IP Address Alarm Generated on Solaris Zones Models (see page 263)
Manage SNMP-Enabled Solaris Zone Models After Solaris Zones Manager Deletion (see page 99)

Configure Model Searches Across Secure Domains

Rather than creating new models, Solaris Zones Discovery attempts to locate models in the SpectroSERVER. In an environment with Secure Domain Manager deployed, Solaris Zones Discovery searches for models within the same secure domain as your Solaris Zones Manager. This domain is the "local" domain. However, some of your virtual environment devices can exist within a different secure domain. In this case, you can configure Solaris Zones Discovery to search all secure domains for existing models.

Follow these steps:

1. Open Virtual Host Manager in the Navigation panel (see page 49).

   The main details page opens in the Contents panel for the selected Virtual Host Manager.

2. Click the Information tab.
3. Expand the Configuration, Solaris Zones, Solaris Zones Discovery subview.
4. Click Set in the 'Search for Existing Models' field.
5. Select from the following options:

   In Zone Manager's Secure Domain

   (Default) Searches for existing models within the same secure domain as the Solaris Zones Manager server.

   In All Secure Domains

   Searches for existing models within all secure domains managed by the SpectroSERVER. Select this option only in the following situations:

   - All devices have unique IP addresses.
   - When secure domains are used for security purposes or to isolate network traffic.

   Note: Do not select this option for a NAT environment.

Your setting is saved. Solaris Zones Discovery searches for existing models in CA Spectrum that match your selection. If duplicate models (models that share the same IP address) exist in multiple secure domains, Virtual Host Manager does the following:

- Selects the model in the local secure domain, if available.
- If a duplicate model does not exist in the local domain, Virtual Host Manager randomly selects a model from another secure domain.
- In both cases, Virtual Host Manager generates a minor alarm for the duplicate IP addresses on the Solaris Zones Manager model.

More information:

How to Configure Discovery Options (see page 94)

Configure SNMP Modeling Preferences

SNMP-capable devices support enriched device monitoring, such as process and file system monitoring capabilities. However, SNMP agents can be costly and time-consuming to deploy. By default, Solaris Zones Discovery creates Solaris Global Zones and Solaris zone instances as VHM models (see definition on page 270). You can later upgrade them to SNMP models. However, you can also configure Solaris Zones Discovery to model all new SNMP-capable devices as SNMP models. Although Solaris Zones Discovery can take longer to complete, initially modeling these as SNMP models avoids manually upgrading these models later.

Important! Enable SNMP modeling *before* you model your Solaris Zones Hosts. If you model the Solaris Zones Hosts first, all child models are created as VHM models, which must be manually upgraded to SNMP models.

Follow these steps:

1. Open Virtual Host Manager in the Navigation panel (see page 49).

   The main details page opens in the Contents panel for the selected Virtual Host Manager.

2. Click the Information tab.
3. Expand the Configuration, Solaris Zones, Solaris Zones Discovery, SNMP Discovery subview.

   Important! Follow the steps in the subview to prepare your devices and CA Spectrum for SNMP Discovery. If devices are not properly prepared before Solaris Zones Discovery, Virtual Host Manager cannot create SNMP models.

4. Click 'set' in the 'Discover SNMP-Capable Devices' field and select from the following options:

   Yes

   Enables SNMP modeling during Solaris Zones Discovery. Only devices that meet the criteria specified in the SNMP Discovery subview text are modeled as SNMP devices. Applies to *new* models only.

   No

   (Default) Models all new devices found during Solaris Zones Discovery as VHM models. You can manually upgrade these models to SNMP models later.

   Your setting is saved and new devices are modeled in Virtual Host Manager according to your selection.

More information:

How to Discover and Model Your Virtual Environment (see page 100)
How Solaris Zones Discovery Works (see page 103)
Add SNMP Capabilities to VHM Models (see page 104)
Manage SNMP-Enabled Solaris Zone Models After Solaris Zones Manager Deletion (see page 99)

Manage SNMP-Enabled Solaris Zone Models After Solaris Zones Manager Deletion

By default, SNMP-enabled devices are deleted from CA Spectrum when the following items are deleted:

- Solaris Zones Manager model for the device
- Solaris Zones folder in the Navigation panel

SNMP-enabled device models can include significant customizations that you want to retain. You can adjust your settings to avoid deleting these models. They are placed into the LostFound container for later use.

Follow these steps:

1. Open Virtual Host Manager in the Navigation panel (see page 49).

   The main details page opens in the Contents panel for the selected Virtual Host Manager.

2. Click the Information tab.

3. Expand the Configuration, Solaris Zones, Solaris Zones Discovery subview.

4. Click Set in the 'Retain SNMP-enabled Solaris Zones During Solaris Zones Manager Deletion' field and select one of the following options:

   Yes

   Retains SNMP-enabled Solaris zone models in the LostFound container when their Solaris Zones Manager or the Solaris Zones folder is deleted.

   Note: Models with more associations, such as a model that is included in a Global Collection, are handled differently. These models are removed from the Universe, but they are not moved to the LostFound container.

   No

   (Default) Deletes all Solaris zone models when their Solaris Zones Manager or the Solaris Zones folder is deleted.

   Your setting is saved, and SNMP-enabled device models are handled accordingly when Solaris Zones Manager models or the Solaris Zones folder is deleted.

More information:

How to Configure Discovery Options (see page 94)
Manage Device Models for Devices Deleted from Solaris (see page 96)
Deleting Virtual Host Manager Models (see page 114)

How to Discover and Model Your Virtual Environment

To monitor your virtual environment, discover and model your virtual entities—Solaris Zones Hosts, Solaris Global Zones, and Solaris zone instances. Modeling these entities in Virtual Host Manager lets you view your complete network topology in one tool, showing the relationships between your physical and virtual components.

The main steps for modeling your virtual environment are as follows:

1. Run a standard CA Spectrum Discovery (see page 101).

   The purpose of this Discovery is to ensure that the upstream routers and switches are modeled before Solaris Zones Discovery runs. Or, if the SNMP Modeling option is disabled, this step can also model the SNMP-capable Solaris Global Zones and Solaris zones. When modeling these entities, be sure that your modeling options are set correctly to support Virtual Host Manager.

2. Upgrade the CA SystemEDGE model (see page 102).

   This step is required only when your CA SystemEDGE agent on the Solaris Zones Manager host was modeled in a release earlier than CA Spectrum r9.1.2.

3. Let Solaris Zones Discovery run (see page 103).

   When you model the CA SystemEDGE agent with Solaris Zones AIM on the Solaris Zones Manager host, Solaris Zones Discovery begins automatically. Each of these Solaris Zones Manager models has its own Solaris Zones Discovery process. The purpose of Solaris Zones Discovery is to find the virtual entities in your Solaris Zones environment, model the ones that do not exist, and place them in the Virtual Host Manager view of the Navigation panel.

More information:

How to Configure Management Options (see page 109)
Move a Solaris Zone Instance to a New Solaris Zones Host (see page 108)
Duplicate MAC, Different IP Address Alarm Generated on Solaris Zones Models (see page 263)
Add SNMP Capabilities to VHM Models (see page 104)
Configure SNMP Modeling Preferences (see page 98)

Run CA Spectrum Discovery

To discover your Solaris Zones environment, run the standard CA Spectrum Discovery. This Discovery ensures that the upstream routers and switches are modeled so that later connections from the virtual entities can be established. You can also model the SNMP-capable Solaris Global Zones and Solaris zone instances during CA Spectrum Discovery.

Note: Modeling SNMP-capable Solaris Global Zones and Solaris zone instances is necessary during CA Spectrum Discovery only when the SNMP Modeling option is disabled during Solaris Zones Discovery.

Note: Only an administrator performs this task.

Follow these steps:

1. Open the Discovery console.

   Note: Before modeling, be sure that you know the correct community strings, IP addresses, and port numbers for any SNMP agents that run on a nonstandard port.

2. Click the  (Creates a new configuration) button in the Navigation panel.

3. Configure your options to support virtual network modeling, as follows:

   a. Click the Modeling Options button in the Modeling Options group.

      The Modeling Configuration dialog opens.

   b. Click the Protocol Options button.

      The Protocol Options dialog opens.

c. Select the ARP Tables for Pingables option, and click OK.

The Modeling Configuration dialog opens.

d. (Optional) Click the Advanced Options button in the Advanced Options group, add your nonstandard SNMP ports (such as the SystemEDGE agent port), and click OK.

4. Enter individual IP addresses or the beginning and ending IP addresses in the IP Boundary List fields and click Add.

Note: Be sure that the range of IP addresses includes Solaris Zones Managers, interconnecting switches and routers, and the SNMP-capable Solaris Global Zones and Solaris zone instances that require SNMP models.

5. Enter any additional values in the Discovery console, and click the Discover button.

The following models are created and added to your network topology in CA Spectrum:

- Solaris Zones Manager hosts and the switches and routers that connect them to your network—Information about your virtual environment comes from the Solaris Zones Manager. When these Solaris Zones Manager models exist in CA Spectrum, Solaris Zones Discovery can begin.
- Solaris Global Zones and Solaris zone instances—If you decide not to model these entities with CA Spectrum Discovery, Solaris Zones Discovery creates them as VHM models (see definition on page 270).

Note: You can also manually model your virtual network by IP address. Always model in the correct order: connecting routers and switches, SNMP-capable Solaris Global Zones and Solaris zone instances, then your Solaris Zones Managers. Modeling in the correct order ensures that the relationships among these entities are built correctly in the topology. For more information, see the *Modeling and Managing Your IT Infrastructure Administrator Guide*.

More information:

How to Configure Management Options (see page 109)
Move a Solaris Zone Instance to a New Solaris Zones Host (see page 108)
Add SNMP Capabilities to VHM Models (see page 104)
Configure SNMP Modeling Preferences (see page 98)

Upgrade the CA SystemEDGE Model

The CA SystemEDGE agent could have been modeled in CA Spectrum before installing Virtual Host Manager or before the Solaris Zones AIM was loaded on the agent. In this case, the existing CA SystemEDGE model is not compatible with Virtual Host Manager. Upgrade the model so that Virtual Host Manager can access the Solaris Zones AIM capabilities in CA SystemEDGE. *This procedure is not required if the CA SystemEDGE agent with Solaris Zones AIM is loaded and is modeled after installing CA Spectrum.*

To upgrade the CA SystemEDGE model, right-click the model and select Reconfiguration, Reconfigure Model.

The CA SystemEDGE model is upgraded to support the Solaris Zones AIM.

Note: You can also send a reconfigure model action to CA SystemEDGE using the CLI. For more information, see the *Modeling and Managing Your IT Infrastructure Administrator Guide*.

More information:

How to Configure Management Options (see page 109)
Move a Solaris Zone Instance to a New Solaris Zones Host (see page 108)
Add SNMP Capabilities to VHM Models (see page 104)

How Solaris Zones Discovery Works

Solaris Zones Discovery is a specialized discovery process that gathers detailed information about your virtual network entities. Solaris Zones Discovery obtains the Solaris Zones technology entities, models the ones that do not exist in CA Spectrum, and place them under Virtual Host Manager in the Navigation panel. A key benefit of Solaris Zones Discovery is that it runs automatically in the background to keep your virtual network data updated. Understanding how Solaris Zones Discovery works reinforces the importance of properly installing and modeling the various Virtual Host Manager components.

The Solaris Zones Discovery process works as follows:

1. After the Solaris Zones Manager is configured correctly (the CA SystemEDGE agent is installed with the Solaris Zones AIM enabled), the Solaris Zones Manager uses SSH to contact each Solaris Global Zone that it manages. The Solaris Zones Manager gathers and stores this information.

   Important! Install the CA SystemEDGE agent with Solaris Zones AIM on the Solaris Zones Manager host. The Solaris Zones Manager and CA Spectrum must be able to communicate. If they cannot, Solaris Zones Discovery cannot run.

2. During CA Spectrum Discovery, CA Spectrum creates a model for each Solaris Zones Manager that is referenced in Step 1. Communication is enabled between CA Spectrum and the CA SystemEDGE agent.

3. CA Spectrum polls the Solaris Zones AIM to gather the Solaris Zones Manager information that was stored in Step 1.

4. CA Spectrum begins Solaris Zones Discovery. The information from the AIM is used to update modeling in the CA Spectrum Topology tab and the Virtual Host Manager hierarchy in the Navigation panel, as follows:

   a. If you enable SNMP Discovery before Step 2, Virtual Host Manager Discovery creates SNMP models for all new SNMP-capable models that meet the SNMP Discovery criteria.

      Note: By default, SNMP Discovery is disabled during Solaris Zones Discovery.

   b. VHM models (see definition on page 270) are created for the remaining non-SNMP Solaris Zones hosts, Solaris Global Zones, and Solaris zone instances, as follows:

      - Existing Solaris Global Zones and Solaris zone models are promoted to VHM models.
      - VHM models are created for the Solaris Global Zone servers and Solaris zone instances that *do not* exist in CA Spectrum.
      - VHM models are created for the Solaris Zones Host models. These models group their associated Solaris Global Zones and Solaris zone models in the Navigation panel, under Virtual Host Manager and the Universe topology.

   c. All models for your virtual network are added to the Virtual Host Manager portion of the Navigation panel.

   Note: In a virtual environment, devices on separate Solaris Zones hosts can have the same IP or MAC address. In this case, CA Spectrum creates duplicate models for each occurrence of an IP or MAC address.

5. Solaris Zones Discovery automatically repeats this process at each regularly scheduled Solaris Zones technology polling interval.

   Note: By default, the Solaris Zones polling interval is controlled by the polling interval on the Solaris Zones Manager device model. Or you can control Solaris Zones polling independent of the Solaris Zones Manager device model. Use the Solaris Zones virtual technology application model.

Add SNMP Capabilities to VHM Models

Although SNMP provides enriched device monitoring, such as process or file monitoring, SNMP agents can be costly and time-consuming to deploy. When an SNMP agent is not available or SNMP Discovery is disabled, Virtual Host Manager creates Solaris Global Zones and Solaris zone instances as VHM models (see definition on page 270).

Later, you can install an SNMP agent on these devices and upgrade their modeling in CA Spectrum. Options for upgrading to SNMP models are as follows:

- **Upgrade only selected devices**—This method works quickly when you have a small selection of models to upgrade. The VHM models and child models are deleted first. One drawback of this method is that after CA Spectrum deletes the models, you must wait for Solaris Zones Discovery to create the new SNMP models and place them in Virtual Host Manager. Knowledge of the IP addresses for the models to upgrade is required.
- **Upgrade all SNMP-capable VHM models**—This method upgrades models in batch, and it is preferred when upgrading Virtual Host Manager to a new release. Knowledge of the IP addresses of individual models is not required. Another advantage is that after CA Spectrum deletes the VHM models, the upgraded SNMP models are immediately placed in the Virtual Host Manager hierarchy without waiting for the next polling cycle. Therefore, the child models are not left unmanaged.

  This method can take a long time to complete. The time required depends on how many community strings and SNMP ports Virtual Host Manager must search when locating SNMP-capable devices.

  Note: Virtual Host Manager attempts to identify SNMP agents on operational Solaris zone instances only.

Important! When models are deleted, all notes or other customizations on those models are lost.

More information:

How to Discover and Model Your Virtual Environment (see page 100)
How Solaris Zones Discovery Works (see page 103)
Deleting Virtual Host Manager Models (see page 114)
Upgrade the CA SystemEDGE Model (see page 102)
Configure SNMP Modeling Preferences (see page 98)

Upgrade Selected VHM Models to SNMP Models

When an SNMP agent is not available or SNMP Discovery is disabled during Solaris Zones Discovery, Virtual Host Manager creates Solaris Global Zones and Solaris zone instances as VHM models (see definition on page 270). Later, you can install an SNMP agent on these devices and upgrade their modeling in CA Spectrum. You must know the IP addresses for the device models to upgrade. Manually selecting models to upgrade works quickly, but all notes or customizations on these models are lost during the upgrade.

Follow these steps:

1. Deploy or enable an SNMP agent on the device, if needed.
2. Model the device again using one of the following methods:
   - CA Spectrum Discovery
   - Model individual devices by IP address

   When the new SNMP-capable model is created, CA Spectrum deletes the previous model from Virtual Host Manager. At the next Solaris Zones AIM polling cycle, CA Spectrum adds the SNMP-capable model to Virtual Host Manager in the Navigation panel.

   Important! When models are deleted, all notes or other customizations on those models are lost.

More information:

Manage Device Models for Devices Deleted from Solaris (see page 96)
How to Discover and Model Your Virtual Environment (see page 100)
Deleting Virtual Host Manager Models (see page 114)

Upgrade All VHM Models to SNMP Models

When an SNMP agent is not available or SNMP Discovery is disabled during Solaris Zones Discovery, Virtual Host Manager creates Solaris Global Zones and Solaris zone instances as VHM models (see definition on page 270). Later, you can install an SNMP agent on these devices and upgrade their modeling in CA Spectrum. When upgrading in batch, CA Spectrum searches your VHM models and locates those that are now SNMP-capable devices. Then CA Spectrum converts them to SNMP models. This method can take a long time to complete, depending on how many community strings and ports Virtual Host Manager must search. However, this method ensures that child models are not unmanaged while parent models are upgrading.

Follow these steps:

1. Deploy or enable an SNMP agent on your devices, as needed.
2. Open Virtual Host Manager in the Navigation panel (see page 49).

   The main details page opens in the Contents panel for the selected Virtual Host Manager.
3. Select the Solaris Zones Manager model in the Navigation panel that manages the models to upgrade.
4. Click the Information tab.
5. Expand the Solaris Zones Manager, CA Spectrum Modeling Control subview.
6. Click the Upgrade ICMP-Only Devices button.

   Important! When models are deleted, all notes or other customizations on those models are lost.

   Virtual Host Manager searches the devices managed by the Solaris Zones AIM on the selected Solaris Zones Manager. Virtual Host Manager upgrades all ICMP-only devices that meet the criteria for SNMP devices and places them within the Virtual Host Manager hierarchy.

Move a Solaris Zone Instance to a New Solaris Zones Host

Moving a Solaris zone from one Solaris Zones host to another can result in lost data. The risk depends on your Virtual Host Manager configuration. The Solaris Zones AIM does not support zone migration. To Virtual Host Manager, a move is seen as two events—the Solaris zone is deleted from the original Solaris Zones Host, and a new Solaris zone is added to the new Solaris Zones Host. In this case, Virtual Host Manager deletes the original Solaris zone model and creates a new one. If you customized the original model, deleting it can result in lost data. You can avoid this data loss when you configure your Virtual Host Manager settings correctly before moving the Solaris zone instance.

Follow these steps:

1. Change the 'Allow Device Model Deletes During Solaris Zones Discovery' option to No (see page 96).

   Note: Disabling this option means that CA Spectrum does not delete the Solaris zone model from CA Spectrum when the model is removed from Virtual Host Manager management.

2. Use the Solaris Zones virtualization technology to remove the Solaris zone from the original Solaris Zones host.

3. Wait for Virtual Host Manager to reflect the changes in the Navigation panel.

4. Use the Solaris Zones virtualization technology to add the Solaris zone to the other Solaris Zones host.

   When Solaris Zones Discovery finds the new Solaris zone, Virtual Host Manager reconciles it with the existing model. Virtual Host Manager places that model into Virtual Host Manager management.

5. (Optional) Change the 'Allow Device Model Deletes During Solaris Zones Discovery' option back to Yes on the originating Solaris Zones Manager model.

   The Solaris zone instance is successfully moved.

More information:

How to Discover and Model Your Virtual Environment (see page 100)
How Solaris Zones Discovery Works (see page 103)
Run CA Spectrum Discovery (see page 101)
How the Solaris Zones Data is Updated in Virtual Host Manager (see page 119)
Upgrade the CA SystemEDGE Model (see page 102)

How to Configure Management Options

After your virtual network is modeled, you can configure Virtual Host Manager options for viewing and managing your device models. Configuring your preferences helps ensure that Virtual Host Manager handles your virtual device models correctly and monitors only the information that is important to you.

To configure your installation of Virtual Host Manager, perform the following procedures after you discover and model your virtual network:

- Configure the Solaris Zones AIM options (see page 109)—These options let you select settings for the CA SystemEDGE Solaris Zones AIM, such as the AIM polling interval and various traps.
- Configure threshold values and other status monitoring options (see page 111)—These options let you determine which information you want to monitor and how CA Spectrum manages the various events that occur in your virtual environment.

More information:

How the Solaris Zones Data is Updated in Virtual Host Manager (see page 119)
Upgrade the CA SystemEDGE Model (see page 102)

Configure the Solaris Zones AIM

The Solaris Zones AIM communicates with the Solaris Zones Manager to manage and collect information about your virtual environment. In Virtual Host Manager, you can configure the AIM to determine how it handles polling, traps, and events. The Solaris Zones AIM configuration settings let you decide the right balance of information to gather against the amount of required resources.

Follow these steps:

1. Open Virtual Host Manager in the Navigation panel (see page 115).

   The main details page opens in the Contents panel for the selected Virtual Host Manager.

2. Locate and click your Solaris Zones Manager on the Explorer tab in the Navigation panel.

   The tabs in the Contents panel are populated with details about your Solaris Zones Manager.

3. Click the Information tab.

4. Expand the Solaris Zones Manager, Solaris Zones AIM subview.

5. Click Set to change the settings for the following fields, as needed:

   AIM Poll Interval (Seconds)

   Specifies the time interval (in seconds) when the Solaris Zones AIM polls and caches status and modeling information from the configured Solaris Zones Hosts. This polling retrieves status and modeling updates, such as a Solaris zone not-running status, Solaris Zones Host disconnected, new Solaris zone available, new Solaris Zones Host, and more.

   Default: 120

   Limits: Numbers greater than or equal to 120

   Note: For best results, we recommend that you set this interval no larger than the CA Spectrum poll cycle interval.

   AIM Log Level

   Specifies the level of information written to the Solaris Zones AIM log file. The levels are cumulative (for example, log level 4 writes all messages at levels 0 through 4). The log levels are as follows:

   - 0: Fatal
   - 1: Critical
   - 2: Warning
   - 3: Info
   - 4: Debug
   - 5: Debug Low
   - 6: Debug Lower
   - 7: Debug Lowest

   Default: 2

   Note: Specifying a debug level greater than 4 is discouraged.

   Your Solaris Zones AIM is configured with your selections.

More information:

How to Configure Management Options (see page 109)
Duplicate MAC, Different IP Address Alarm Generated on Solaris Zones Models (see page 263)

Configure and Monitor Resource Status

You can monitor the status of your virtual resources in OneClick. For example, you can view the total memory, used memory, percent of CPU usage, and more. Also, you can set monitoring options, such as enabling alerts and setting threshold values for traps. Configuring and viewing this information can help you optimize your virtual network performance and troubleshoot alarms.

Note: Traps are set on and managed by the Solaris Zones AIM, but you can configure these threshold values from the OneClick subviews. A read/write community string is required to change any threshold values or settings.

You can view or configure resource status options and information for virtual devices on the Information tab.

Follow these steps:

1. Open Virtual Host Manager in the Navigation panel (see page 115).

   The main details page opens in the Contents panel for the selected Virtual Host Manager.

2. Locate and click the virtual device on the Explorer tab in the Navigation panel.

   The device details display in the Contents panel.

3. Click the Information tab.

   Multiple subviews are available for viewing. Generally, the subview at the bottom of the tab includes the resource allocation and utilization information for the selected model. For example, a Solaris Zones Host model displays a subview named "Solaris Zone Host Information" that includes details for the specific model you selected in the Navigation panel.

4. Expand the appropriate subview.

   All available resource status details and monitoring options for the selected device model are displayed.

   Note: The Solaris Zones Manager model provides combined information for all virtual devices managed by the Solaris Zones Manager. That is, selecting the Solaris Zones Manager model in the Navigation panel displays information about the selected Solaris Zones Manager host *and* combined information about all Solaris Zones Hosts, Solaris Global Zones, Solaris zone instances, physical and virtual NICs, projects, host disks, and more. This information is the same data displayed on the Information tab for each individual entity model. The combined view in the Solaris Zones Manager model can provide a good overview about all of the virtual entities it manages.

More information:

How to Configure Management Options (see page 109)
Custom Subviews for Virtual Entity Types (see page 120)
Status Monitoring Options (see page 122)
Virtual Host Manager Alarms for Solaris Zones (see page 125)

Controlling Solaris Zones AIM Polling

When tuning Virtual Host Manager performance, you can change the Solaris Zones Manager polling rate or disable Solaris Zones technology polling. By default, the polling attributes on the Solaris Zones Manager model control the Solaris Zones-related polling behavior. Or you can change this Solaris Zones-related polling behavior independently. The Solaris Zones virtual technology application model, SolarisZoneAimApp, controls your Solaris Zones-related polling.

The following two attribute values on the application specifically control the Solaris Zones technology polling logic:

- PollingStatus
- Polling_Interval

Both the Solaris Zones Manager device model and the SolarisZoneAimApp application model contain these attributes. PollingStatus disables and enables polling, while Polling_Interval controls the polling frequency. If the values are different for these models, the SolarisZoneAimApp application model attribute values take precedence. For both PollingStatus and Polling_Interval, modifying the attribute on the Solaris Zones Manager device model also changes the corresponding application model attribute if their values are the same.

This ability to set the value for the device model and application model lets you fine-tune your Solaris Zones-related polling. For example, you can set the polling interval higher for the application model, but set a lower value for device models. This scenario can improve Virtual Host Manager performance by reducing the frequency of polling for less critical devices in your environment.

More information:

How Solaris Zones Discovery Works (see page 103)

Configure the Solaris Zones AIM Polling Interval

You can change the Solaris Zones AIM polling rate. Configure the polling interval by setting the Polling_Interval attribute on the Solaris Zones virtual technology application model.

Follow these steps:

1. Open OneClick and click the Locater tab in the Navigation panel.
2. Expand the Application Models folder and double-click 'By Device IP Address.'

   A search dialog opens.
3. Enter the IP address for your Solaris Zones Manager in the Device IP Address field, and click OK.

   A list of application models for the Solaris Zones Manager appears in the Contents panel.
4. Select the SolarisZoneAimApp application model.

   The application model details appear in the Component Details panel.
5. Click the Information tab in the Component Details panel.
6. Click the Modeling Information subview.
7. Click 'set' in the Polling Interval (sec) field, and enter a new value.

   Note: Changing the Polling Interval value from any number to 0 also sets the Polling field to Off, disabling Solaris Zones AIM polling. However, if you set the Polling Interval to 0 and set the Polling field to On, Solaris Zones AIM polling continues, using the polling interval for the Solaris Zones Manager device.

   The Solaris Zones AIM polling interval setting is configured.

Disable Solaris Zones AIM Polling

You can disable Solaris Zones AIM polling. Disabling Solaris Zones polling is the same as disabling Virtual Host Manager. Disable polling by setting the PollingStatus attribute on the Solaris Zones virtual technology application model.

Follow these steps:

1. Open OneClick and click the Locater tab in the Navigation panel.
2. Expand the Application Models folder and double-click 'By Device IP Address.'

   A search dialog opens.
3. Enter the IP address for your Solaris Zones Manager in the Device IP Address field, and click OK.

   A list of application models for the Solaris Zones Manager appears in the Contents panel.

4. Select the SolarisZoneAimApp application model.

   The application model details appear in the Component Details panel.

5. Click the Information tab in the Component Details panel.
6. Click the CA Spectrum Modeling Information subview.
7. Click 'set' in the Polling field and select Off.

   Polling is disabled for the Solaris Zones AIM on the selected Solaris Zones Manager.

Deleting Virtual Host Manager Models

Generally, models can be deleted from OneClick at any time. However, Virtual Host Manager restricts your ability to delete models from the Virtual Host Manager hierarchy in the Navigation panel. To delete models manually, you have the following two options:

- Delete the Solaris Zones folder or a Solaris Zones Manager model in Virtual Host Manager
- Remove a virtual entity using your Solaris Zone virtualization technology

In Virtual Host Manager, models are sometimes deleted automatically. The following circumstances cause CA Spectrum to automatically delete Virtual Host Manager models:

- **Solaris Zones folder deleted or Solaris Zones Manager model removed from Virtual Host Manager**

  If you remove a Solaris Zones Manager model or delete the Solaris Zones folder from the Navigation panel, CA Spectrum deletes all related child models.

- **An entity removed from Solaris Zones virtual environment**

  As you delete Solaris Zones Hosts and Solaris zones using your Solaris Zones virtualization technology, CA Spectrum also deletes those models and their child models from Virtual Host Manager.

- **Upgraded models exist**—In some cases, a Solaris Global Zone or Solaris zone is first modeled for Virtual Host Manager without SNMP capabilities. If SNMP capabilities are later added to a VHM model (see definition on page 270), the previous model is deleted and replaced with the new SNMP-capable model.

Note: Although the default setting is to delete the models, you can configure Virtual Host Manager to place the Solaris Zones Host, Solaris Global Zones, and Solaris zone instances in the LostFound container when they are removed from Virtual Host Manager. This configuration setting applies only when you remove devices using your Solaris Zones virtual environment. However, this setting does not apply when you delete the Solaris Zones folder, remove a Solaris Zones Manager model, or upgrade a VHM model.

Viewing Your Solaris Zones Virtual Environment

This section describes concepts for viewing your Solaris Zones virtual environment and the associated alarms. The basic steps are no different from the standard CA Spectrum procedures. However, this section describes conceptual differences and details that only apply to the Solaris Zones virtual technology.

More information:

Run CA Spectrum Discovery (see page 101)
Custom Subviews for Virtual Entity Types (see page 120)
Locater Tab for Solaris Zones (see page 121)
How Virtual Host Manager Works with Solaris Zones (see page 91)
Models Created for Solaris Zones (see page 93)

Understanding the Virtual Topology

The models created for your Solaris Zones technology environment are integrated into the Navigation panel in the following places:

- **Virtual Host Manager node**—The Virtual Host Manager node provides a hierarchical tree structure that helps you to visualize the relationships between your virtual environment resources, as configured in your Solaris Zones technology.
- **Universe topology view**—This view shows which Solaris Global Zones and Solaris zones are associated with a Solaris Zones Host. It also provides a layer 2 view of the network, showing how Solaris Global Zones and Solaris zone instances are connected to the network. You can use this view to resolve alarms involving these virtual network models.

Note: For more information about using the OneClick interface, see the *Operator Guide*.

Virtual Host Manager in the Navigation panel

Virtual Host Manager displays the logical relationships between your virtual environment resources, as configured in your Solaris Zones virtual technology. Using this information, you can see how resources are shared among your Solaris Zones Managers, which can help you identify opportunities to reorganize and optimize your virtual environment. This hierarchy also provides a quick way to monitor the performance of your resources and troubleshoot their alarms.

Because Virtual Host Manager is not aware of a DSS environment (see definition on page 268), it is located within a landscape hierarchy. The following example shows where Virtual Host Manager fits into the Navigation panel and illustrates the virtual environment hierarchy:

```
[-] SpectroSERVER host
    [+] Universe
    [-] Virtual Host Manager
        [-] Solaris Zones
            [+] Solaris Zones Manager 1
            [-] Solaris Zones Manager 2
                [-] Solaris Zones Host 1
                      Solaris Global Zone
                      Solaris zone 1
                      Solaris zone 2
                [+] Solaris Zones Host 2
                [+] Solaris Zones Host 3
```

Virtual Host Manager is the root node for the entire virtual environment managed by this SpectroSERVER. Selecting this node in the Navigation panel displays Virtual Host Manager details in the Contents panel. You can view details such as events and alarms related to your virtual environment as a whole.

Directly under Virtual Host Manager, virtual environments are organized within folders that represent the technology with which they are created. In the example hierarchy above, the Solaris Zones folder contains the portion of the virtual environment that was created using Solaris Zones virtualization technology. In this folder, Virtual Host Manager lists all Solaris Zones Manager hosts managed by this SpectroSERVER.

Each Solaris Zones Manager contains only the portion of the entire virtual environment that it manages. Selecting a Solaris Zones Manager in the Navigation panel displays details in the Contents panel, such as the Solaris Zones Hosts or Solaris zone instances managed by the selected Solaris Zones Manager. You can also view general statistics and view details about other components that are not modeled in CA Spectrum, such as the following:

- Resource pools
- Projects
- Processor sets
- Physical and virtual NICs
- Host disks
- Containers

Under each Solaris Zones Manager, the hierarchy represents the logical relationships between the following entities:

- **Solaris Zones Hosts**

  A Solaris Zones Host contains the Solaris Global Zone and Solaris zone instances (that is, your non-global zones (see page 269)) that it manages. Selecting a Solaris Zones Host in the Navigation panel displays details in the Contents panel such as events and alarms related to the Solaris Zones Host, memory usage, status, and more.

- **Solaris Global Zones**

  The Solaris Global Zone model appears as a child to its corresponding Solaris Zones Host model and is always a leaf node on the Virtual Host Manager hierarchy tree. This model shares the same name as its parent. The model icon in the Contents and Component Detail panels distinguishes the Solaris Global Zones models from their parent Solaris Zones Host model. The DeviceType attribute also distinguishes these models. Selecting a Solaris Global Zone in the Navigation panel displays details in the Contents panel such as system status, CPU usage, memory usage, and more.

- **Solaris zone**

  A Solaris zone instance is always a leaf node on the Virtual Host Manager hierarchy tree. Selecting a Solaris zone in the Navigation panel displays details in the Contents panel such as events and alarms related to the Solaris zone instance, memory usage, status, and more.

Virtual environment in the Universe topology

The Solaris Zones Manager, Solaris Zones Host, Solaris Global Zone, and Solaris zone models created for your virtual environment are also integrated into the Universe topology view. Solaris Zones Host models automatically group their associated Solaris Global Zones and Solaris zone instances. The topology shows how these Solaris Global Zones and Solaris zone instances are connected to your physical network entities.

The following example shows how these models can appear in the Navigation panel under the Universe node:

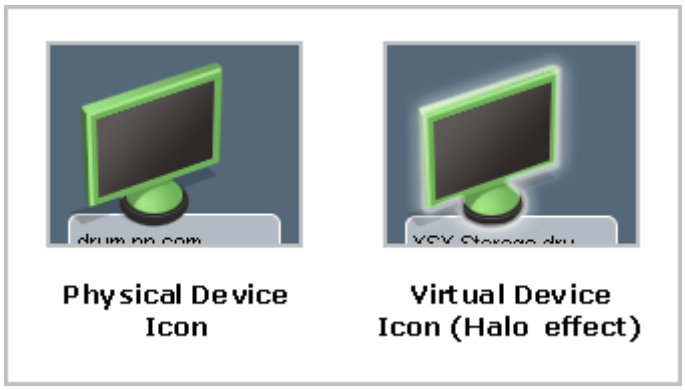
```
[-] Universe
        Physical switch 1
        Physical switch 2
    [-] Solaris Zones Host
            Fanout A
            Fanout B
            Solaris Global Zone
            Solaris zone A
            Solaris zone B
            Solaris zone C
```

More information:

Custom Subviews for Virtual Entity Types (see page 120)
How the Solaris Zones Data is Updated in Virtual Host Manager (see page 119)
Models Created for Solaris Zones (see page 93)

Icons for Virtual Devices

Virtual Host Manager provides icons that are designed specifically to distinguish devices in your virtual environment. To distinguish physical and virtual entities, the virtual device icons have a halo-like appearance around the outer edge. For example, a virtual device model icon displays a halo around the perimeter, as follows:



For physical servers that host virtual devices, Virtual Host Manager uses a distinctive honeycomb pattern on the device icon, as follows:

Note: For Solaris Zones technology, the only virtual entity models created in Virtual Host Manager are for Solaris zone instances. All other entities modeled for your virtual environment, such as the Solaris Zones Host, Solaris Global Zones, and Solaris Zones Manager, are physical devices.

How the Solaris Zones Data is Updated in Virtual Host Manager

During your initial Solaris Zones Discovery, CA Spectrum populates Virtual Host Manager hierarchy in the Navigation panel with your virtual device models. After CA Spectrum builds this initial hierarchy, your virtual network configuration can change, and Virtual Host Manager must continually work to keep this information accurate in CA Spectrum. For example, the following events can change your virtual network configuration:

- Creating or deleting a Solaris zone on a Solaris Zones Host
- Manually moving a Solaris zone from one Solaris Zones Host to another

To keep your information accurate, Virtual Host Manager detects these changes by polling the Solaris Zones AIM. Therefore, your virtual network configuration is updated in CA Spectrum at each polling cycle. CA Spectrum also receives traps from the AIM and generates the corresponding events. By reviewing the event log, you can find out when configuration changes occur, such as when a new Solaris zone is created.

When a Solaris zone is deleted, CA Spectrum removes the models from the Virtual Host Manager hierarchy in the Navigation panel. When the AIM detects an addition to your virtual network configuration, such as provisioning a new Solaris zone or placing one into management, CA Spectrum performs the following tasks:

- Updates the placement of your virtual device models in the Virtual Host Manager hierarchy of the Navigation panel
- *Automatically* rediscovers connections to the affected Solaris Global Zone and Solaris zone models and associates them with the correct Solaris Zones Host in the Universe topology.

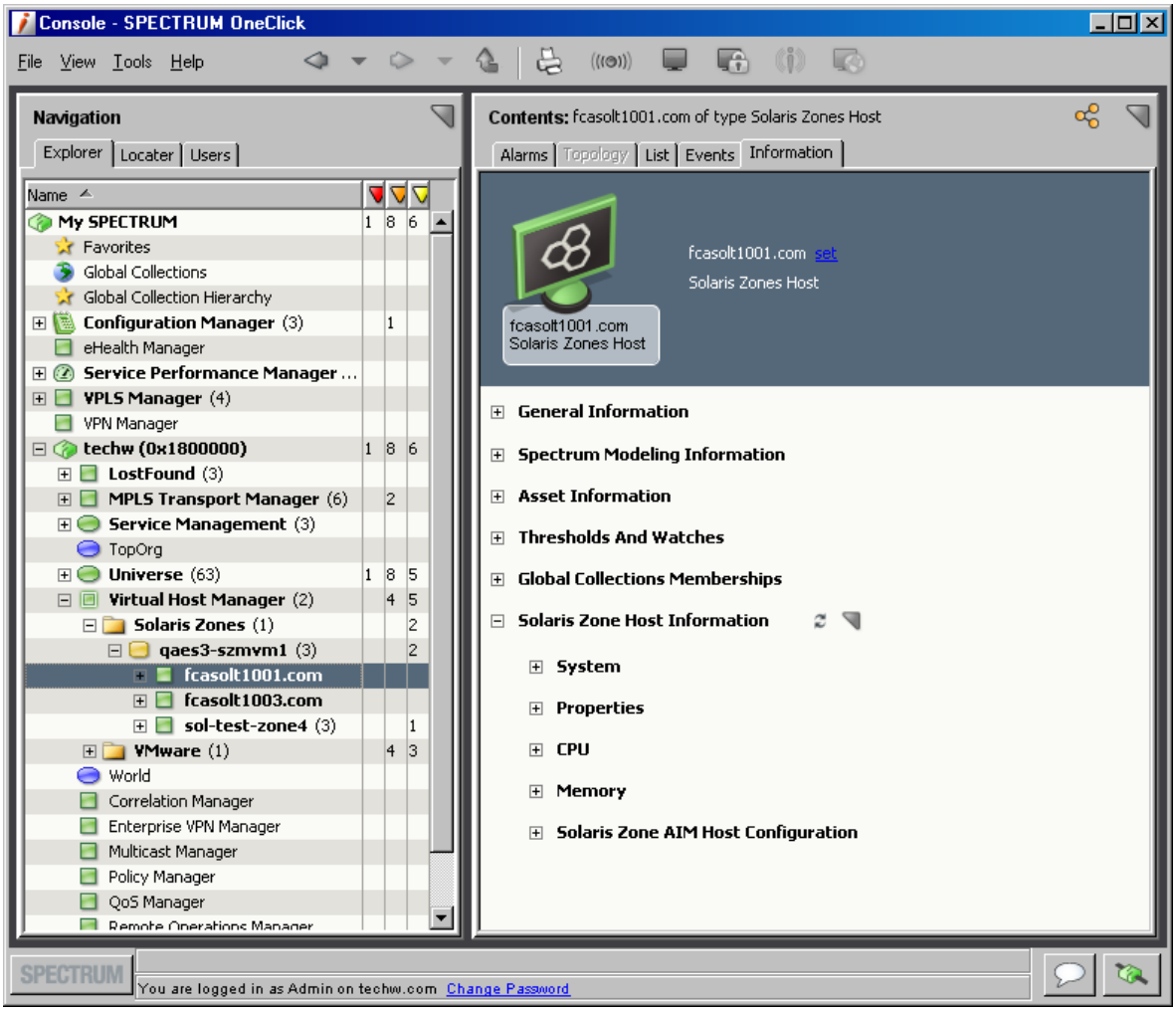
  Important! To reestablish connections to your virtual models correctly, all interconnecting routers and switches in your physical network must be modeled. If these models do not exist before connections to your virtual devices are rediscovered, CA Spectrum cannot resolve those connections and display the information correctly in the Universe topology view. The Solaris Zones Hosts are placed in the same LAN container as the CA SystemEDGE model.

More information:

How Virtual Host Manager Works (see page 11)
Manage Device Models for Devices Deleted from Solaris (see page 96)
Configure and Monitor Resource Status (see page 111)
Move a Solaris Zone Instance to a New Solaris Zones Host (see page 108)
Models Created for Solaris Zones (see page 93)
Viewing Your Solaris Zones Virtual Environment (see page 115)

Custom Subviews for Virtual Entity Types

Your Virtual Host Manager models collectively provide information about your virtual environment. Individually, each model provides unique information or configuration settings, depending on the virtual entity type it represents. This custom subview appears on the Information tab in the Contents panel. These subviews can contain real-time data, such as CPU status or memory utilization, and provide access to threshold settings. For example, the custom subview for a Solaris Zones Host is the "Solaris Zone Host Information" subview, as shown:



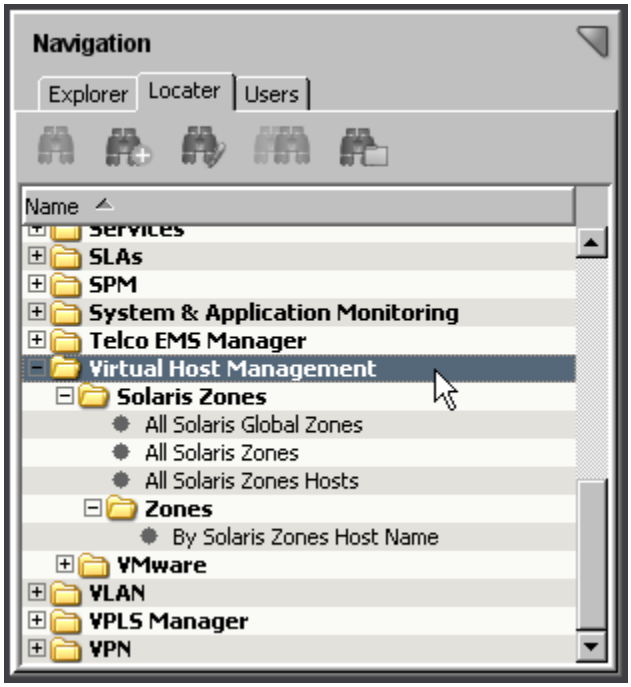
Note: The Solaris Zones Manager model provides combined information for all virtual devices managed by the Solaris Zones Manager. That is, selecting the Solaris Zones Manager model in the Navigation panel displays information about the selected Solaris Zones Manager host *and* combined information about all Solaris Zones Hosts, Solaris Global Zones, Solaris zone instances, physical and virtual NICs, projects, host disks, and more. This information is the same data displayed on the Information tab for each individual entity model. The combined view in the Solaris Zones Manager model can provide a good overview about all of the virtual entities it manages.

More information:

Configure and Monitor Resource Status (see page 111)
Understanding the Virtual Topology (see page 115)

Locater Tab for Solaris Zones

In addition to viewing details about your virtual environment on the Explorer tab, you can also use the Locater tab to run preconfigured Virtual Host Manager searches. The search options are grouped under the Virtual Host Manager, Solaris Zones folder on the Locater tab, as shown:



These detailed searches can help you investigate information related to virtual entities only, such as all Solaris Zones Hosts within a single landscape.

Note: Although Virtual Host Manager is not DSS (see definition on page 268) aware, these preconfigured searches let you select multiple landscapes to search in the search parameters.

The Locater tab in the Navigation panel includes the following searches for Solaris Zones:

All Solaris Global Zones

Locates all Solaris Global Zones that have been modeled in the CA Spectrum database for your virtual network.

All Solaris Zones

Locates all Solaris zone instances that have been modeled in the CA Spectrum database for your virtual network.

All Solaris Zones Hosts

Locates all Solaris Zones Hosts that have been modeled in the CA Spectrum database for your virtual network.

Zones, By Solaris Zones Host Name

Locates all Solaris zone instances (including Solaris Zones Hosts) that have been modeled in the CA Spectrum database for your virtual network, limited to only those Solaris zones managed by a selected Solaris Zones Host.

Status Monitoring Options

CA Spectrum provides a wide range of options for monitoring the state of your virtual network resources. The status information available for a resource varies, depending on the type of virtual entity you are monitoring. Also, your ability to configure a status option depends on its type. For example, some status options are read-only, but others let you configure threshold values, enable behaviors, or select an alarm severity. Providing this range of options and levels of customization, CA Spectrum lets you decide how to best monitor the performance of your virtual network.

Status fields are located in the OneClick subviews. All status information for a given virtual environment is available on the Solaris Zones Manager model in a tabular format. Also, each virtual entity type that has a unique model in CA Spectrum provides a subset of the same status information for easy viewing. Status-related settings, including the alert type, monitor, and thresholds, can be set from either view location.

The following tables outline the type of status information available for each virtual entity type. The Subview Locations column describes where the corresponding status fields are located in OneClick. For example, "memory" information for your Solaris zone models is available on the Information tab in the following two locations:

- Solaris Zone Information subview for the Solaris zone model
- Solaris Zones Manager, Managed Environment, Zones subview for the Solaris Zones Manager model

To explore the exact status options available for each status information type, locate the subview in OneClick.

Solaris Zones Manager

Status Information Type	Subview Locations
Overall	Solaris Zones Manager

Solaris Zones Host

Status Information Type	Subview Locations
Overall	Solaris Zones Host, Solaris Zones Manager
CPU	Solaris Zones Host, Solaris Zones Manager
Memory	Solaris Zones Host, Solaris Zones Manager

Solaris Global Zone

Status Information Type	Subview Locations
System	Solaris Global Zone, Solaris Zones Manager
CPU	Solaris Global Zone, Solaris Zones Manager
Memory	Solaris Global Zone, Solaris Zones Manager

Solaris Zone

Status Information Type	Subview Locations
Overall	Solaris Zone, Solaris Zones Manager
Memory	Solaris Zone, Solaris Zones Manager
CPU	Solaris Zone, Solaris Zones Manager
Aggregate CPU	Solaris Zone, Solaris Zones Manager

Resource Pool

Status Information Type	Subview Locations
Overall	Solaris Zones Manager

Project

Status Information Type	Subview Locations
Overall	Solaris Zones Manager
Memory	Solaris Zones Manager
CPU	Solaris Zones Manager

Processor Set

Status Information Type	Subview Locations
Overall	Solaris Zones Manager

Physical NIC

Status Information Type	Subview Locations
Overall	Solaris Zones Manager
Connection	Solaris Zones Manager
Link state	Solaris Zones Manager

Virtual NIC

Status Information Type	Subview Locations
Overall	Solaris Zones Manager
Connection	Solaris Zones Manager
Utilization	Solaris Zones Manager

Host Disk

Status Information Type	Subview Locations
Overall	Solaris Zones Manager
Capacity	Solaris Zones Manager
Usage	Solaris Zones Manager
Available space	Solaris Zones Manager
State of read	Solaris Zones Manager
State of write	Solaris Zones Manager

Alarms and Fault Isolation for Solaris Zones

This section describes the traps used by Virtual Host Manager and the resulting alarms. This section also explains how Virtual Host Manager fault isolation differs from basic CA Spectrum fault isolation.

Virtual Host Manager Alarms for Solaris Zones

To alert you to problems within your virtual network, CA Spectrum generates alarms. Alarms are created in two ways:

- Traps sent from the CA SystemEDGE agent
- Polling

Polling generates four alarms: Solaris Zones Proxy Lost, Solaris Zones Host Proxy Lost, Solaris Zones Manager Unavailable, and Solaris Zone Not Running. However, several traps can generate alarms on your virtual devices. CA Spectrum supports all traps sent by the Solaris Zones AIM from the CA SystemEDGE agent. To optimize these traps, you can configure the threshold values for each virtual device individually.

If a trap breaches your threshold value and generates an alarm, CA Spectrum uses the value of the “state” varbind that is passed with the trap to determine the alarm severity. All state varbinds have the following possible values, which receive the same CA Spectrum alarms:

- 1: OK
- 2: Warning
- 3: Critical

CA Spectrum maps these Solaris Zones technology states to a CA Spectrum alarm severity, as shown:

Solaris Zones State	CA Spectrum Alarm Severity
1: OK	Clear
2: Warning	Minor (Yellow)
3: Critical	Major (Orange)

More information:

Manage Device Models for Devices Deleted from Solaris (see page 96)
Configure and Monitor Resource Status (see page 111)
Status Monitoring Options (see page 122)
Manage SNMP-Enabled Solaris Zone Models After Solaris Zones Manager Deletion (see page 99)

How CA Spectrum Forwards Traps from CA SystemEDGE

CA Spectrum supports all traps sent by the Solaris Zones AIM. These traps are initially sent to the Solaris Zones CA SystemEDGE model. If the destination for a trap is not the Solaris Zones model, CA Spectrum forwards the trap to the correct virtual model.

Note: For specific event codes related to the traps, use the Event Configuration application and filter on "0x056e." Or you can launch MIB tools to view the traps in the Trap Support table for the "EMPIRE-CASUNZA-MIB" MIB. For more information about using the Event Configuration application, see the *Event Configuration User Guide*. For more information about using MIB tools, see the *Modeling and Managing Your IT Infrastructure Administrator Guide*.

CA Spectrum determines where to forward the trap by using the following process:

1. When CA Spectrum receives a trap, it uses varbind information in the trap to locate the correct virtual entity.
   - For traps that are forwarded to a Solaris Zones Host, CA Spectrum uses the UID to locate the correct host.
   - For traps that are forwarded to a Solaris zone, CA Spectrum uses the UID to determine first the correct Solaris Zones Host. Then, CA Spectrum locates the correct Solaris zone within the list of zones that this Solaris Zones Host manages.
2. CA Spectrum uses this UID to look up and locate the CA Spectrum model that is tied to a given UID. The entity type that is associated with all traps is predetermined. Depending on the results of the look-up, CA Spectrum forwards the trap as follows:
   - If it finds a CA Spectrum model of a specific type with a given UID, CA Spectrum forwards the event and corresponding alarm to the destination model.
   - If it cannot find a CA Spectrum model for a given UID, CA Spectrum generates a new generic event on the Solaris Zones Manager model. This new event includes details about the trap.

     Note: CA Spectrum often cannot find a related model when a trap is sent immediately after changing your virtual network entities in Solaris Zones. Solaris Zones Discovery has not yet identified and created the corresponding model in CA Spectrum.

More information:

Traps Supported in Virtual Host Manager (see page 127)

Traps Supported in Virtual Host Manager

All traps generated by the Solaris Zones AIM are supported in CA Spectrum. The traps are initially sent to the Solaris Zones Manager model. Then, the traps are forwarded to a corresponding virtual entity type (that is, the "destination" entity), depending on the type of trap. Using these traps, you can monitor the performance of your virtual network, resolve any resulting alarms, or trigger events.

Note: For more information about traps generated by the Solaris Zones AIM, see the *CA Virtual Assurance for Infrastructure Managers Implementation Guide*.

The following tables list the traps for a specific destination entity type and specify whether the trap generates an alarm.

Solaris Zones Manager Traps

Trap Name	Trap OID	Alarm?
zoneAimHostDeleteTrap	1.3.6.1.4.1.546.1.1.0.165448	No
zoneAimHostAddTrap	1.3.6.1.4.1.546.1.1.0.165449	No

Solaris Zones Host Traps

Trap Name	Trap OID	Alarm?
zoneAimHostConfigChangeTrap	1.3.6.1.4.1.546.1.1.0.165401	No
zoneAimHostStateChangeTrap	1.3.6.1.4.1.546.1.1.0.165402	Yes
zoneAimHostCPUStateChangeTrap	1.3.6.1.4.1.546.1.1.0.165403	Yes
zoneAimHostMemStateChangeTrap	1.3.6.1.4.1.546.1.1.0.165404	Yes
zoneAimHostTotalZoneCPUStateChangeTrap	1.3.6.1.4.1.546.1.1.0.165405	Yes
zoneAimHostTotalZoneMemStateChangeTrap	1.3.6.1.4.1.546.1.1.0.165406	Yes
zoneAimHostThresholdChangeTrap	1.3.6.1.4.1.546.1.1.0.165407	No
zoneAimHostConnectionStateChangeTrap	1.3.6.1.4.1.546.1.1.0.165408	No
zoneAimContainerAddedTrap	1.3.6.1.4.1.546.1.1.0.165416	No
zoneAimContainerRemovalTrap	1.3.6.1.4.1.546.1.1.0.165417	No
zoneAimPNICAddedTrap	1.3.6.1.4.1.546.1.1.0.165425	No
zoneAimPNICRemovalTrap	1.3.6.1.4.1.546.1.1.0.165426	No
zoneAimPNICConfigChangeTrap	1.3.6.1.4.1.546.1.1.0.165427	No

Trap Name	Trap OID	Alarm?
zoneAimPNICStateChangeTrap	1.3.6.1.4.1.546.1.1.0.165428	Yes
zoneAimHostDiskAddedTrap	1.3.6.1.4.1.546.1.1.0.165433	No
zoneAimHostDiskRemovalTrap	1.3.6.1.4.1.546.1.1.0.165434	No
zoneAimHostDiskConfigChangeTrap	1.3.6.1.4.1.546.1.1.0.165435	No
zoneAimHostDiskStateChangeTrap	1.3.6.1.4.1.546.1.1.0.165436	Yes
zoneAimHostDiskAvailStateChangeTrap	1.3.6.1.4.1.546.1.1.0.165437	Yes
zoneAimHostDiskThresholdChangeTrap	1.3.6.1.4.1.546.1.1.0.165438	No
zoneAimResourcePoolAddedTrap	1.3.6.1.4.1.546.1.1.0.165439	No
zoneAimResourcePoolRemovalTrap	1.3.6.1.4.1.546.1.1.0.165440	No
zoneAimResourcePoolConfigChangeTrap	1.3.6.1.4.1.546.1.1.0.165441	No
zoneAimResourcePoolStateChangeTrap	1.3.6.1.4.1.546.1.1.0.165442	Yes
zoneAimResourcePoolSchedChangeTrap	1.3.6.1.4.1.546.1.1.0.165443	No
zoneAimProcessorSetAddedTrap	1.3.6.1.4.1.546.1.1.0.165444	No
zoneAimProcessorSetRemovalTrap	1.3.6.1.4.1.546.1.1.0.165445	No
zoneAimProcessorSetConfigChangeTrap	1.3.6.1.4.1.546.1.1.0.165446	No
zoneAimProcessorSetStateChangeTrap	1.3.6.1.4.1.546.1.1.0.165447	Yes

Solaris Global Zone and Solaris Zone Traps

Trap Name	Trap OID	Alarm?
zoneAimZoneCPUStateChangeTrap	1.3.6.1.4.1.546.1.1.0.165409	Yes
zoneAimZoneMemStateChangeTrap	1.3.6.1.4.1.546.1.1.0.165410	Yes
zoneAimZoneConfigChangeTrap	1.3.6.1.4.1.546.1.1.0.165411	No
zoneAimZoneThresholdChangeTrap	1.3.6.1.4.1.546.1.1.0.165412	No
zoneAimZoneAddedTrap	1.3.6.1.4.1.546.1.1.0.165413	No
zoneAimZoneRemovedTrap	1.3.6.1.4.1.546.1.1.0.165414	No
zoneAimZoneRunningStateChangeTrap	1.3.6.1.4.1.546.1.1.0.165415	Yes
zoneAimProjectCPUStateChangeTrap	1.3.6.1.4.1.546.1.1.0.165418	Yes
zoneAimProjectMemStateChangeTrap	1.3.6.1.4.1.546.1.1.0.165419	Yes
zoneAimProjectAddedTrap	1.3.6.1.4.1.546.1.1.0.165420	No
zoneAimProjectRemovalTrap	1.3.6.1.4.1.546.1.1.0.165421	No
zoneAimProjectConfigChangeTrap	1.3.6.1.4.1.546.1.1.0.165422	No

Trap Name	Trap OID	Alarm?
zoneAimProjectThresholdChangeTrap	1.3.6.1.4.1.546.1.1.0.165423	No
zoneAimProjectOverallStateChangeTrap	1.3.6.1.4.1.546.1.1.0.165424	Yes
zoneAimVNICAddedTrap	1.3.6.1.4.1.546.1.1.0.165429	No
zoneAimVNICRemovalTrap	1.3.6.1.4.1.546.1.1.0.165430	No
zoneAimVNICConfigChangeTrap	1.3.6.1.4.1.546.1.1.0.165431	No
zoneAimVNICStateChangeTrap	1.3.6.1.4.1.546.1.1.0.165432	Yes

More information:

Configure and Monitor Resource Status (see page 111)
How to Configure Management Options (see page 109)
How the Solaris Zones Data is Updated in Virtual Host Manager (see page 119)
Status Monitoring Options (see page 122)
How CA Spectrum Forwards Traps from CA SystemEDGE (see page 126)

Fault Management for Virtual Networks

The goal of fault isolation is to narrow down the root cause of a networking problem. Finding the root cause can help you to troubleshoot and quickly correct the problem or to correct the problem programmatically with automated scripts. Deciding which devices are the root cause of an alarm can be difficult, because problems with a single device can cause several devices in your network to generate events.

For example, losing contact with a Solaris Zones Host often means that you have also lost contact with the Solaris zone instances it manages. Therefore, the Solaris Zones Host device model and all affected Solaris zone instances generate alarms. Using fault isolation techniques, Virtual Host Manager correlates these alarms in an attempt to identify a single root cause.

Virtual networks provide a unique management opportunity, because they provide CA Spectrum an alternate management perspective. That is, CA Spectrum can gather information through direct contact with your virtual devices or through the virtual network management technology, Solaris Zones. This alternate management perspective enhances standard CA Spectrum fault management in two ways:

- **Enhanced Contact Lost alarms**—Two sources of information about a device means Virtual Host Manager can pinpoint the cause and more easily correlate events to a single root cause.
- **Proxy Failure alarms**—*Proxy management* is the act of managing network devices using an alternate management source in place of or in addition to the primary manager. For example, CA Spectrum can manage virtual network devices by contacting them directly or through the virtual technology application's contact with the devices. When Solaris Zones virtualization technology loses contact with a virtual network device, Virtual Host Manager generates one of the Proxy Management Lost alarms for each device. These alarms are unique, because they are alerting you to the fact that *management* of the device through the *proxy* is affected, not the state of the device or direct (SNMP) management.

How Fault Isolation Works when Device Contact is Lost

To help you troubleshoot networking problems with your devices, CA Spectrum uses fault isolation to narrow down the root cause of an alarm. For virtual networks, Virtual Host Manager uses information from direct contact with the device plus information provided by Solaris Zones technology through the Solaris Zones AIM. In many cases, standard CA Spectrum fault management can pinpoint the root cause. But in special circumstances, the method for isolating problems in a virtual network go beyond the standard methods.

The type of fault isolation Virtual Host Manager uses to discover the root cause depends on which devices are alarming and the type of events the devices generate. The following scenarios describe two unique fault management situations and how CA Spectrum isolates the networking error in your virtual network.

Scenario 1: Solaris zone instance is not running

In a virtual environment, the virtual management application can provide more details than CA Spectrum can discover through standard device monitoring. For example, the Solaris Zones virtualization technology is aware when a Solaris zone changes from the "running" state to something else, such as the "installed" state.

If a Solaris zone is no longer running and CA Spectrum loses contact with it, but proxy management (see definition on page 269) of the Solaris Zones Manager is uninterrupted, CA Spectrum determines the root cause as follows:

1. When CA Spectrum loses contact with a Solaris zone, it generates a Contact Lost alarm.
2. During its next polling cycle, the Solaris Zones Manager model polls the Solaris Zones AIM to gather information about the Solaris zone. Because Solaris Zones technology manages the Solaris zone instances, it can provide a unique view into the possible cause of alarms generated by a Solaris zone.
3. If the Solaris Zones technology finds that the Solaris zone is in the not-running mode, it generates a Zone Not Running alarm.

   Note: This alarm is cleared upon the first Solaris Zones AIM polling cycle after the Solaris zone is running again.
4. Virtual Host Manager correlates the Contact Lost alarm to the corresponding Zone Not Running alarm created by CA Spectrum. Virtual Host Manager makes the Contact Lost alarm appear as a symptom of the Zone Not Running alarm.

Scenario 2: Solaris Zones Host is down

If CA Spectrum loses contact with a modeled Solaris Global Zone and all Solaris zones running on that host, CA Spectrum checks the status of the upstream routers and switches. Depending on their status, CA Spectrum determines the root cause as follows:

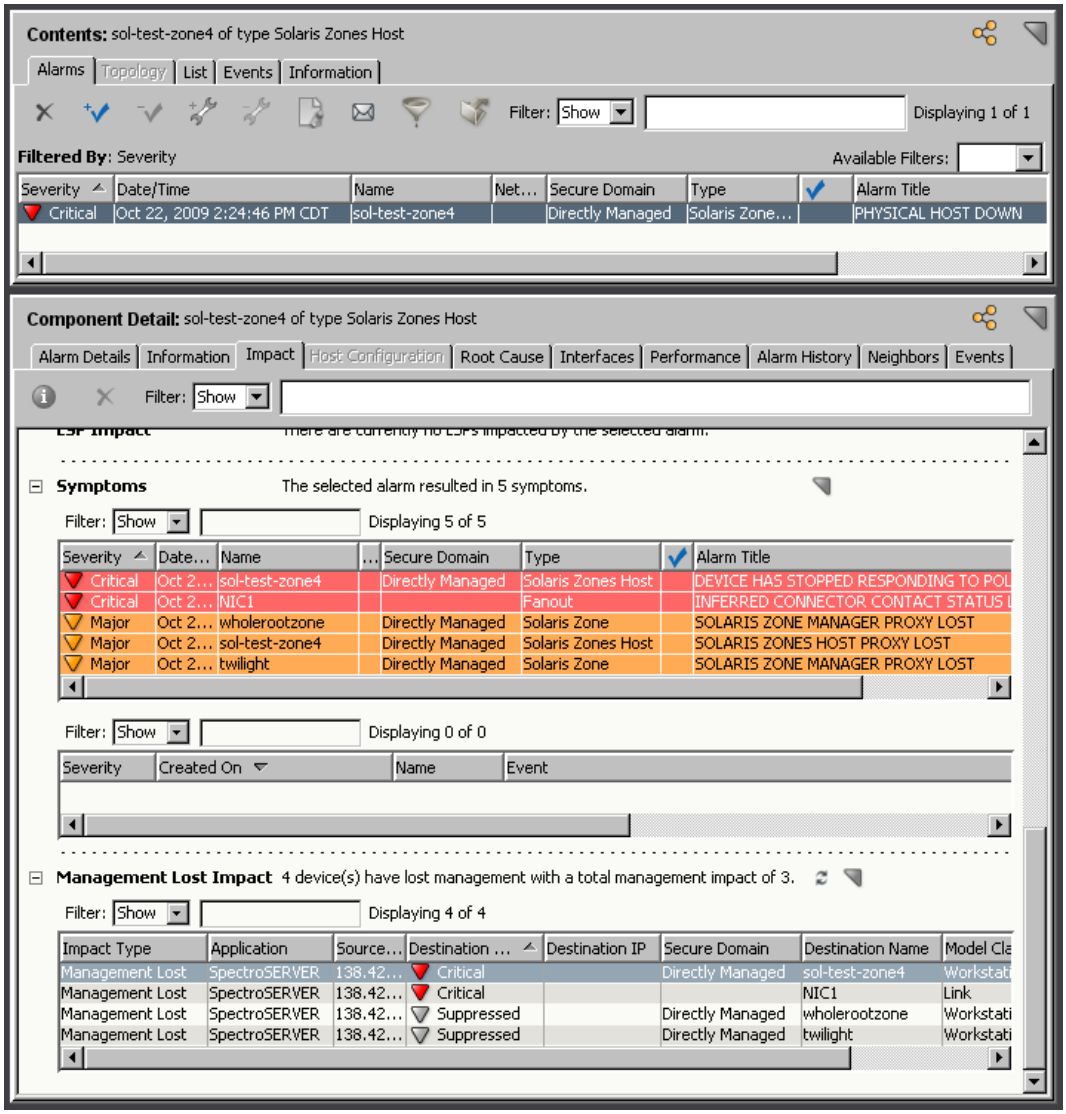
- All upstream devices for one or more Solaris zone instances or the Solaris Global Zone are unavailable—Standard CA Spectrum fault isolation techniques determine the root cause, as follows:
  - Device Stopped Responding to Polls alarm—Generated on the Solaris Zones Host when at least one upstream connected device for any Solaris zone or Solaris Global Zone is up.
  - Gateway Unreachable alarm—Generated on the Solaris Zones Host when *all* upstream connected devices are down.
- At least one upstream device is available for every Solaris zone instance and Solaris Global Zone model connected to the Solaris Zones Host—CA Spectrum infers that the Solaris Zones Host is the root cause and responds as follows:
  a. The Solaris Global Zone model and all Solaris zones, ports, and fanouts that are directly connected to the Solaris Global Zone model or Solaris zone models generate the standard fault isolation alarms.
  b. Virtual Host Manager creates a Physical Host Down alarm for the Solaris Zones Host model.

c. All fault isolation-related alarms that are created for the impacted devices (such as Solaris zones, ports, and fanouts) are correlated to the Physical Host Down alarm, making them symptoms of the Physical Host Down alarm. These symptom alarms appear in the Symptoms table on the Impact tab for the Physical Host Down alarm.

   Note: For each Solaris Zones Host model, Virtual Host Manager creates a "virtual fault domain." This domain includes the Solaris Zones Host, Solaris Global Zone, and Solaris zone instances, plus all ports and fanouts directly connected to the Solaris Global Zone model or Solaris zones. When the Solaris Zones Host generates the Physical Host Down alarm, all standard fault isolation alarms within the domain are correlated to it. Correlating these alarms as symptoms indicates that the Physical Host Down alarm on the Solaris Zone Host is the root cause.

d. All impacted devices are listed in the Management Lost Impact table on the Impact tab for the Physical Host Down alarm.

Note: Devices that are suppressed do not have a corresponding alarm in the Symptoms table, which is why the following example shows only two related symptom alarms but four impacted devices:



e. If all upstream devices for one or more Solaris zone instances or the Solaris Global Zone go down, CA Spectrum can no longer reliably state that the fault lies with the Solaris Zones Host. Therefore, CA Spectrum clears the Physical Host Down alarm and applies the standard CA Spectrum fault isolation techniques.

More information:

Determining Solaris Zones Affected by Solaris Zones Host Outages (see page 137)
How Fault Isolation Works when Proxy Management is Lost (see page 134)

How Fault Isolation Works when Proxy Management is Lost

The Solaris Zones virtualization technology used to create your virtual network provides CA Spectrum a unique management opportunity. CA Spectrum can use the standard methods to contact your virtual devices directly, plus CA Spectrum can simultaneously gather virtual device information from Solaris Zones technology. In this sense, the Solaris Zones technology is a "proxy" from which CA Spectrum gathers virtual device information. If CA Spectrum loses direct contact with a device, it generates alarms. Likewise, if Solaris Zones technology loses contact with a virtual device or if Virtual Host Manager loses contact with the Solaris Zones Manager, Virtual Host Manager generates alarms—Proxy Management Lost alarms (see definition on page 269).

In response, CA Spectrum attempts to isolate the cause of the proxy management failure. Proxy fault isolation is similar to the standard CA Spectrum fault isolation, except that these alarms alert you to the fact that *proxy* management of a virtual device is affected. Proxy management fault isolation cannot tell you whether a virtual device is up or down. However, it is important to know when contact through the proxy is lost, because you could be missing important virtual information about a device.

The type of proxy fault isolation Virtual Host Manager uses to discover the root cause depends on which devices are alarming and the type of events the devices generate. The following scenarios describe two unique proxy fault management situations and how Virtual Host Manager isolates the networking error in your virtual network.

Scenario 1: Contact between Solaris Zones Manager and Solaris Zones Host is lost

If the Solaris Zones Manager loses contact with one of the Solaris Zones Hosts it is managing, the Solaris Zones Manager data about that Solaris Zones Host and all hosted Solaris zone instances is lost. To isolate the problem, Virtual Host Manager determines the root cause as follows:

1. A Proxy Lost alarm is generated on the Solaris Zones Host, Solaris Global Zone, and all hosted Solaris zones.
2. The Solaris zone alarms are correlated to the Proxy Lost alarm for the Solaris Global Zone, making these Solaris zone alarms symptoms of the Solaris Global Zone alarm. The Solaris Global Zone alarm is correlated to the Proxy Lost alarm for the Solaris Zones Host, making it a symptom of the Solaris Zones Host alarm. Correlating these alarms as symptoms indicates that the Solaris Zones Host alarm is the root cause.
3. If CA Spectrum also loses contact with the Solaris Zones Host and generates a Physical Host Down alarm, the Proxy Lost alarm generated for the Solaris Zones Host is correlated to the Physical Host Down alarm. In this case, the Proxy Lost alarm becomes a symptom of the Physical Host Down alarm. Correlating this alarm as a symptom indicates that the Physical Host Down alarm on the Solaris Zones Host is the root cause.

Scenario 2: Contact between CA Spectrum and Solaris Zones Manager is lost

If CA Spectrum loses contact with or stops polling the Solaris Zones Manager model, CA Spectrum loses the Solaris Zones technology data about all virtual models managed by that Solaris Zones Manager. To isolate the problem, Virtual Host Manager determines the root cause as follows:

1. CA Spectrum generates Proxy Lost alarms for all virtual models managed by that Solaris Zones Manager, including Solaris zone instances, Solaris Global Zones, and Solaris Zones Hosts. CA Spectrum also generates a separate Proxy Unavailable alarm on the Solaris Zones Manager model.
2. The Solaris zone alarms are correlated to their corresponding Solaris Global Zone model alarms.
3. The Solaris Global Zone alarms are correlated to their corresponding Solaris Zones Host model alarm.

4. The Solaris Zones Host model alarms are correlated to a Proxy Unavailable alarm for the Solaris Zones Manager model.
5. This Proxy Unavailable alarm is then correlated to the root cause of the Solaris Zones Manager being down. The root cause is typically an alarm generated by standard CA Spectrum fault management, such as the alarms created for the following situations:
   - Lost management of Solaris Zones Manager (that is, a problem occurred with the CA SystemEDGE agent on the Solaris Zones Manager host)
   - Machine contact is lost
   - Solaris Zones Manager model is in maintenance mode

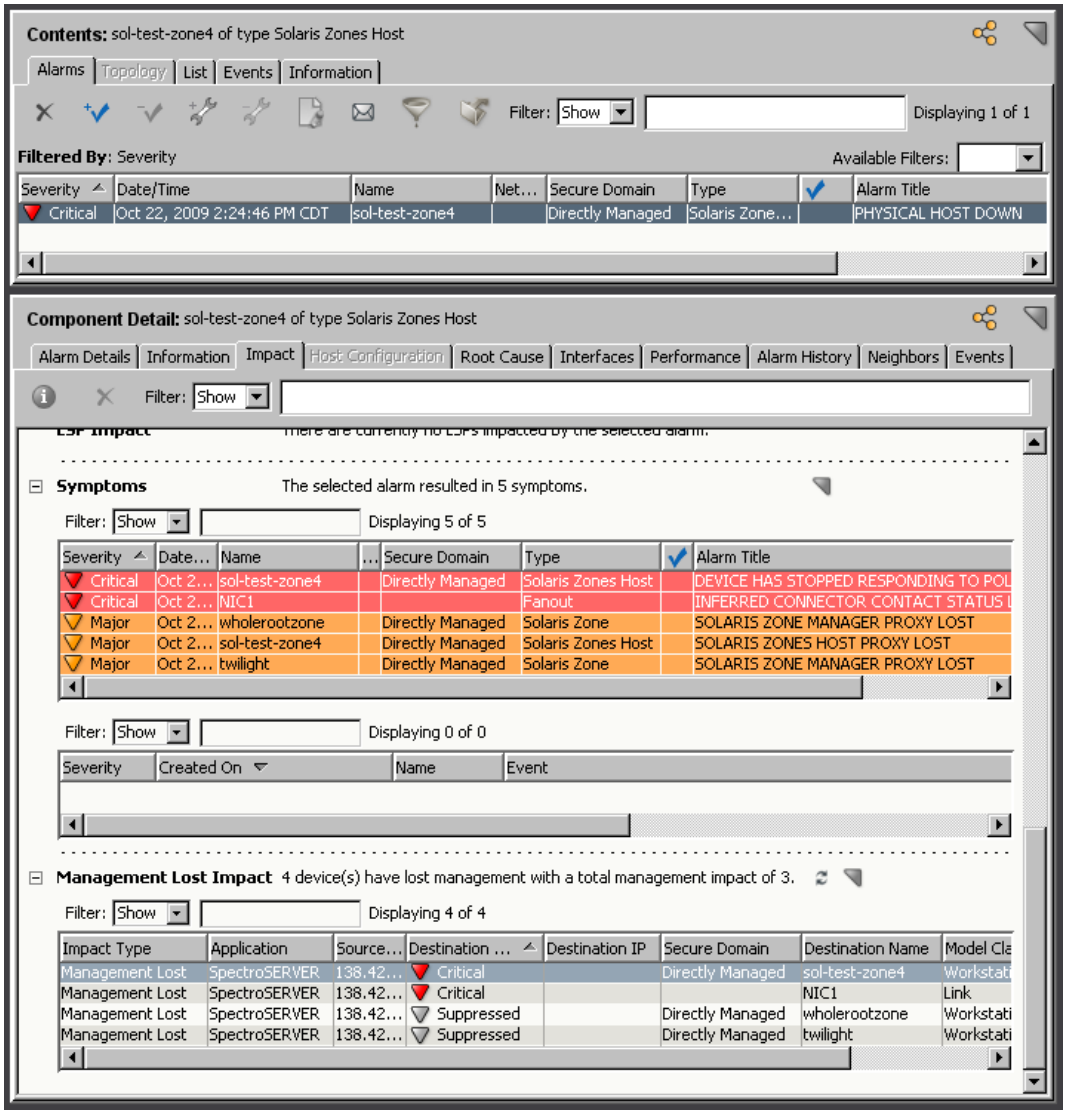
More information:

How Fault Isolation Works when Device Contact is Lost (see page 130)

Determining Solaris Zones Affected by Solaris Zones Host Outages

When contact with a Solaris Zones Host is interrupted or the Solaris Zones Host goes down, all Solaris zone instances hosted by the Solaris Zones Host are affected. Because Solaris Zones technology cannot communicate with the Solaris Zones Host to get usage information, you might not receive alarms for a critical Solaris zone hosted on that Solaris Zones Host. To find out if a critical Solaris zone is impacted, you can view a list of affected Solaris zone instances on the Impact tab of the alarm, as follows:

- Symptoms subview—displays all symptom alarms generated by the affected Solaris zone instances
- Management Lost Impact subview—lists the Solaris zone instances impacted by the alarm



More information:

How Fault Isolation Works when Device Contact is Lost (see page 130)

Chapter 5: Microsoft Hyper-V

This section is for Microsoft Hyper-V virtualization technology users and describes how to use Virtual Host Manager to manage your virtual entities created with Hyper-V.

This section contains the following topics:

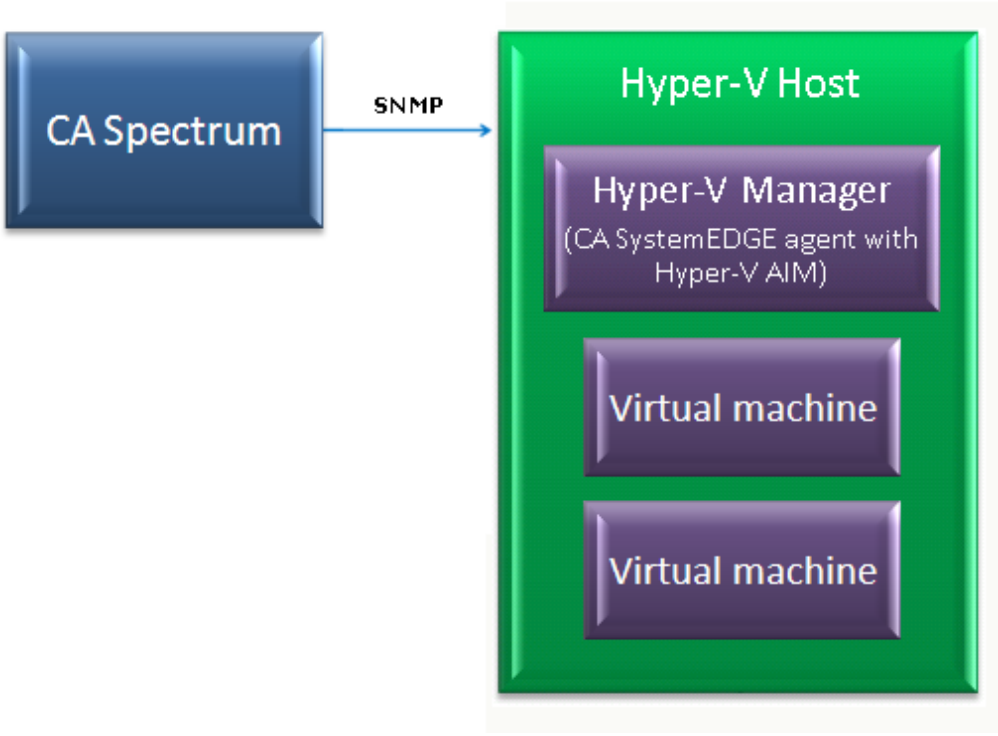
How Virtual Host Manager Works with Hyper-V

The Microsoft Hyper-V AIM collects the data of the monitored Hyper-V resources through server-internal queries without accessing the network. Therefore, the CA SystemEDGE agent and the Hyper-V AIM must run on each Microsoft Hyper-V Server that you want to monitor through CA Spectrum.

If your Microsoft Hyper-V virtual machine is a Windows platform virtual machine, we recommend installing the Microsoft Hyper-V integration services on each virtual machine in your Microsoft Hyper-V environment. The Hyper-V integration services optimize the virtualization of virtual machines. Without these tools, many features are not available.

The Microsoft Hyper-V Server provides functionality to create, run, and manage virtual machines. The Hyper-V AIM and CA SystemEDGE agent integrate with the Microsoft Hyper-V Server and collect data for Hyper-V monitoring through CA Spectrum.

The following diagram shows how CA Spectrum gathers information about your Microsoft Hyper-V virtual environment using the CA SystemEDGE agent with the Hyper-V AIM loaded:



As shown in the diagram, the process to gather information about your Microsoft Hyper-V virtual environment is as follows:

1. The Microsoft Hyper-V management operating system (see definition on page 269) resides on the Microsoft Hyper-V Host in your virtual environment, storing detailed data about each host and their virtual machines.
2. The Microsoft Hyper-V Manager, which contains the CA SystemEDGE agent with the Microsoft Hyper-V AIM loaded, resides on the Hyper-V Host server. With that AIM loaded, the CA SystemEDGE agent communicates with the Microsoft Hyper-V management operating system to gather the details about your virtual environment.
3. Periodically, CA Spectrum retrieves the information from the Hyper-V Manager and uses it to model and monitor your virtual entities.

More information:

How Virtual Host Manager Works (see page 11)
Viewing Your Hyper-V Virtual Network (see page 156)
How the Hyper-V Data is Updated in Virtual Host Manager (see page 158)

Models Created for Hyper-V

Virtual Host Manager provides several models to represent the components of your Microsoft Hyper-V virtual technology network. Understanding the following basic models can help you better understand Discovery and how the virtual environment interfaces with your physical environment.

Virtual Host Manager includes the following models and icons for Hyper-V devices:

Hyper-V Manager

Represents a server that contains the CA SystemEDGE agent with the Hyper-V AIM loaded. There can be only one Hyper-V Manager per Hyper-V Host.

Icon: 

Note: The Hyper-V management operating system is represented in the virtual topology as part of the Hyper-V Manager model. The *Hyper-V management operating system* is the original operating system running on the Hyper-V Host. Microsoft Hyper-V uses this operating system to configure the hosted Hyper-V virtual machines. As appropriate, this Hyper-V Manager model is repeated in the hierarchy and topology views to represent the Hyper-V management operating system.

Hyper-V Host

Represents a Hyper-V Host, as configured in your Hyper-V virtualization technology. A *Hyper-V Host* is a physical computer that uses Microsoft Hyper-V virtualization software to run virtual machines. Hosts provide the CPUs and memory resources that Hyper-V virtual machines use. They also give these virtual machines access to storage and network connectivity. These models serve as container models within the topology views, helping to group your virtual entities into a separate view while showing where the virtual environment interfaces with your physical network. The Hyper-V Host cannot be contacted directly for status information. Instead, the status of these models is inferred from the status of its contained items.

Icon: 

Hyper-V virtual machine

Represents a Hyper-V virtual machine, as configured in your Hyper-V virtualization technology. A Hyper-V *virtual machine* is a software computer that, like a physical computer, runs an operating system and applications. A virtual machine dynamically consumes resources on its physical host, depending on its workload.

Icon: 

More information:

Viewing Your Hyper-V Virtual Environment (see page 156)

Discovering Hyper-V Networks

This section describes the Discovery and modeling process for Virtual Host Manager. These tasks are typically performed by the Virtual Host Manager administrator.

How to Configure Discovery Options

After Virtual Host Manager is installed, you can configure Virtual Host Manager for Hyper-V Discovery. Configuring your preferences helps ensure that Virtual Host Manager models your virtual devices correctly.

To configure your installation of Virtual Host Manager for Hyper-V Discovery, select your preferences for the following options:

- Maintenance Mode for New Virtual Machines (see page 143)—Lets you decide which newly discovered virtual machines to place into maintenance mode until you are ready for CA Spectrum to manage them.
- Allow Device Model Deletes During Hyper-V Discovery (see page 144)—Controls how CA Spectrum handles Hyper-V host and Hyper-V virtual machine models when Microsoft Hyper-V no longer manages them.
- Search for Existing Models (see page 145)—Determines which secure domains Virtual Host Manager searches during a Hyper-V Discovery.

- Discover SNMP-Capable Devices (see page 146)—Controls how SNMP-capable devices are modeled during Hyper-V Discovery. By default, new models are initially created as VHM models only. But, this option lets you override the default and immediately create SNMP models for devices that meet the necessary criteria.
- Retain SNMP-enabled Virtual Machines During Hyper-V Manager Deletion (see page 147)—Controls how CA Spectrum handles SNMP-enabled virtual machine models when a Hyper-V Manager model is deleted.

Configure Maintenance Mode for New Hyper-V Virtual Machines

Virtual Host Manager automatically models the virtual machines that are managed by Microsoft Hyper-V. CA Spectrum attempts to manage all models discovered. However, some newly discovered Hyper-V virtual machines are not ready for CA Spectrum management when they are initially modeled. To prevent undesired alarms on new Hyper-V virtual machine models, you can decide which new models are immediately placed into maintenance mode. Later, you can manually disable maintenance mode on individual models when you are ready for CA Spectrum to manage these devices.

Follow these steps:

1. Open Virtual Host Manager in the Navigation panel (see page 115).

   A details page opens in the Contents panel for the selected Virtual Host Manager.
2. Click the Information tab.
3. Expand the Configuration, Hyper-V, Hyper-V Discovery subview.
4. Click Set in the 'Maintenance Mode for New Hyper-V Virtual Machines' field and select one of the following options:

   Place non-enabled VMs in Maintenance Mode

   (Default) Applies maintenance mode to only non-enabled Hyper-V virtual machine models on initial Hyper-V Discovery.

   Place all VMs in Maintenance Mode

   Applies maintenance mode to all newly discovered Hyper-V virtual machine models upon initial Hyper-V Discovery.

   Your setting is saved and newly discovered Hyper-V virtual machine models created by Virtual Host Manager are placed into maintenance mode per your selection.

More information:

How to Configure Discovery Options (see page 142)
Status Monitoring Options (see page 162)

Manage Device Models for Devices Deleted from Microsoft Hyper-V

The devices and the relationships among them change frequently in virtual environments. Maintaining accurate and timely data about your virtual environment in CA Spectrum is challenging. For example, when a Hyper-V virtual machine is removed, CA Spectrum removes the corresponding device models from Virtual Host Manager in the Navigation panel. However, should CA Spectrum keep or delete the model? You can select settings to control model deletion.

Important! When models are deleted, all notes or other customizations on those models are lost. Disable this option if models are likely to be recreated in your Hyper-V environment later.

Follow these steps:

1. Open Virtual Host Manager in the Navigation panel (see page 49).

   The main details page opens in the Contents panel for the selected Virtual Host Manager.

2. Click the Information tab.

3. Expand the Configuration, Hyper-V, Hyper-V Discovery subview.

4. Click Set in the 'Allow Device Model Deletes During Hyper-V Discovery' field and select one of the following options:

   Yes

   (Default) Deletes the models that correspond to entities no longer managed by your Microsoft Hyper-V environment.

   No

   Places Virtual Host Manager models in the LostFound container when their corresponding entity is no longer managed by your Hyper-V environment, but the models are not deleted from CA Spectrum.

   Note: Models with more associations, such as a model that is included in a Global Collection, are handled differently. These models are removed from the Universe, but they are not moved to the LostFound container.

   Your setting is saved, and device models are handled accordingly after the device is deleted from your Hyper-V environment.

More information:

How to Configure Discovery Options (see page 142)
Deleting Virtual Host Manager Models (see page 167)
Virtual Host Manager Alarms for Hyper-V (see page 168)
Traps Supported in Virtual Host Manager (see page 170)
Manage SNMP-Enabled Virtual Machine Models After Hyper-V Manager Deletion (see page 147)

Configure Model Searches Across Secure Domains

Before creating new models, Hyper-V Discovery attempts to locate models in the SpectroSERVER. In an environment with Secure Domain Manager deployed, Hyper-V Discovery searches for models within the same secure domain as your Hyper-V Manager. This domain is the "local" domain. However, some of your virtual environment devices can exist within a different secure domain. In this case, you can configure Hyper-V Discovery to search all secure domains for existing models.

Follow these steps:

1. Open Virtual Host Manager in the Navigation panel (see page 49).

   A details page opens in the Contents panel for the selected Virtual Host Manager.

2. Click the Information tab.

3. Expand the Configuration, Hyper-V, Hyper-V Discovery subview.

4. Click Set in the 'Search for Existing Models' field and select from the following options:

   In Hyper-V Manager's Secure Domain

   (Default) Searches for existing models within the same secure domain as the Hyper-V Manager server.

   In All Secure Domains

   Searches for existing models within all secure domains managed by the SpectroSERVER. Select this option only in the following situations:

   - All devices have unique IP addresses
   - When secure domains are used for security purposes or to isolate network traffic

   Note: Do not select this option for a NAT environment.

   Your setting is saved and Hyper-V Discovery searches for existing models in CA Spectrum according to your selection. If duplicate models (that is, models that share the same IP address) exist in multiple secure domains, Virtual Host Manager does the following:

   - Selects the model in the local secure domain, if available.
   - If a duplicate model does not exist in the local domain, Virtual Host Manager randomly selects a model from another secure domain.
   - In both cases, Virtual Host Manager generates a minor alarm for the duplicate IP addresses on the Hyper-V Manager model.

More information:

How to Configure Discovery Options (see page 142)

Configure SNMP Modeling Preferences

SNMP-capable virtual machines support enriched device monitoring, such as process and file system monitoring capabilities. However, SNMP agents can be costly and time-consuming to deploy. By default, Hyper-V Discovery creates virtual machines as VHM models (see definition on page 270), which you can later upgrade to SNMP models. However, you can configure Hyper-V Discovery to model all new SNMP-capable devices as SNMP models. Although Hyper-V Discovery may take longer to complete, initially modeling these as SNMP models avoids manually upgrading these models later.

Important! Enable SNMP modeling *before* you model your Hyper-V Manager servers. If you model the Hyper-V Manager servers first, all child models are created as VHM models, which must be manually upgraded to SNMP models.

Follow these steps:

1. Open Virtual Host Manager in the Navigation panel (see page 49).

   The main details page opens in the Contents panel for the selected Virtual Host Manager.

2. Click the Information tab.

3. Expand the Configuration, Hyper-V, Hyper-V Discovery, SNMP Discovery subview.

   Important! Follow the steps in the subview to prepare your devices and CA Spectrum for SNMP Discovery. If devices are not properly prepared before Hyper-V Discovery, Virtual Host Manager cannot create SNMP models.

4. Click Set in the 'Discover SNMP-Capable Devices' field and select from the following options:

   Yes

   Enables SNMP modeling during Hyper-V Discovery. Only devices that meet the criteria specified in the SNMP Discovery subview text are modeled as SNMP devices. Applies to *new* models only.

   No

   (Default) Models all new devices found during Hyper-V Discovery as VHM models. You can manually upgrade these models to SNMP models later.

   Your setting is saved and new devices are modeled in Virtual Host Manager according to your selection.

More information:

How to Discover and Model Your Virtual Environment (see page 148)
How Hyper-V Discovery Works (see page 150)
Adding SNMP Capabilities to VHM Models (see page 152)
Manage SNMP-Enabled Virtual Machine Models After Hyper-V Manager Deletion (see page 147)

Manage SNMP-Enabled Virtual Machine Models After Hyper-V Manager Deletion

By default, SNMP-enabled devices are deleted from CA Spectrum when the following items are deleted:

- Hyper-V Manager model for the device
- Hyper-V folder in the Navigation panel

SNMP-enabled device models can include significant customizations that you want to retain. You can adjust your settings to avoid deleting these models. They are placed into the LostFound container for later use.

Follow these steps:

1. Open Virtual Host Manager in the Navigation panel (see page 49).

   The main details page opens in the Contents panel for the selected Virtual Host Manager.

2. Click the Information tab.

3. Expand the Configuration, Hyper-V, Hyper-V Discovery subview.

4. Click Set in the 'Retain SNMP-enabled Virtual Machines During Hyper-V Manager Deletion' field and select one of the following options:

   Yes

   Retains SNMP-enabled virtual machine models in the LostFound container when their Hyper-V Manager or the Hyper-V folder is deleted.

   Note: Models with more associations, such as a model that is included in a Global Collection, are handled differently. These models are removed from the Universe, but they are not moved to the LostFound container.

   No

   (Default) Deletes all virtual machine models when their Hyper-V Manager or the Hyper-V folder is deleted.

   Your setting is saved. SNMP-enabled device models are handled according to your selection when Hyper-V Manager models or the Hyper-V folder is deleted.

More information:

How to Configure Discovery Options (see page 142)
Manage Device Models for Devices Deleted from Microsoft Hyper-V (see page 144)
Deleting Virtual Host Manager Models (see page 167)

How to Discover and Model Your Virtual Environment

To monitor your virtual environment, discover and model your virtual entities—Hyper-V Managers, Hyper-V Hosts, and Hyper-V virtual machines. Modeling these entities in Virtual Host Manager lets you view your complete network topology in one tool, showing the relationships between your physical and virtual components.

The main steps for modeling your virtual environment are as follows:

1. Run a standard CA Spectrum Discovery (see page 148).

   The purpose of this Discovery is to ensure that the upstream routers and switches are modeled before Hyper-V Discovery runs. Or, if the SNMP Modeling option is disabled, this step can also model the SNMP-capable virtual machines and Hyper-V servers. When modeling these entities, be sure that your modeling options are set correctly to support Virtual Host Manager.

2. Upgrade the CA SystemEDGE model (see page 150).

   This step is required only when your CA SystemEDGE agent on the Hyper-V server was modeled in a release before CA Spectrum Release 9.2.1.

3. Let Hyper-V Discovery run (see page 150).

   When you model the CA SystemEDGE agent (with the Hyper-V AIM) on the Hyper-V server, Hyper-V Discovery begins automatically. Each of these Hyper-V Server models has its own Hyper-V Discovery process. The purpose of Hyper-V Discovery is to find the virtual entities managed by Hyper-V, model the ones that do not exist, and place them in the Virtual Host Manager view of the Navigation panel.

More information:

Adding SNMP Capabilities to VHM Models (see page 152)
Move a Hyper-V Virtual Machine to a Different Hyper-V Host (see page 155)
How to Configure Management Options (see page 164)
Configure SNMP Modeling Preferences (see page 146)

Run CA Spectrum Discovery

To discover your Hyper-V environment, run the standard CA Spectrum Discovery. This Discovery ensures that the upstream routers and switches are modeled so that later connections from the virtual entities can be established. You can also model the SNMP-capable Hyper-V virtual machines during CA Spectrum Discovery.

Note: Modeling SNMP-capable Hyper-V virtual machines is necessary during CA Spectrum Discovery only when the SNMP Modeling option is disabled during Hyper-V Discovery.

Note: Only an administrator performs this task.

Follow these steps:

1. Open the Discovery console.

   Note: Before modeling, be sure that you know the correct community strings, IP addresses, and port numbers for any SNMP agents that run on a nonstandard port.

2. Click the  (Creates a new configuration) button in the Navigation panel.

3. Configure your options to support virtual network modeling, as follows:

   a. Click the Modeling Options button in the Modeling Options group.

      The Modeling Configuration dialog opens.

   b. Click the Protocol Options button.

      The Protocol Options dialog opens.

   c. Select the ARP Tables for Pingables option, and click OK.

      The Modeling Configuration dialog opens.

   d. (Optional) Click the Advanced Options button in the Advanced Options group. Add your nonstandard SNMP ports (such as, the CA SystemEDGE agent port), and click OK.

4. Enter individual IP addresses or the beginning and ending IP addresses in the IP Boundary List fields and click Add.

   Note: Be sure that the range of IP addresses includes all servers with CA SystemEDGE and Hyper-V AIM installed and the interconnecting switches and routers. Or you can include the SNMP-capable Hyper-V virtual machines that require SNMP models.

5. Enter any additional values in the Discovery console, and click Discover.

   The following models are created and added to your network topology in CA Spectrum:

   - Hyper-V Manager servers and the switches and routers that connect them to your network—Information about your virtual environment comes from the Hyper-V Manager. When these Hyper-V Manager models exist in CA Spectrum, Hyper-V Discovery can begin.
   - Hyper-V Hosts and Hyper-V virtual machines—If you decide not to model these entities with CA Spectrum Discovery, Hyper-V Discovery creates them as VHM models (see definition on page 270).

   Note: You can also manually model your virtual network by IP address. In this case, we recommend modeling the upstream devices first. Modeling in the correct order ensures that the relationships among these entities are built correctly in the topology. For more information about how to perform a Discovery, see the *Modeling and Managing Your IT Infrastructure Administrator Guide*.

More information:

Adding SNMP Capabilities to VHM Models (see page 152)
Move a Hyper-V Virtual Machine to a Different Hyper-V Host (see page 155)
How to Configure Management Options (see page 164)
Configure SNMP Modeling Preferences (see page 146)

Upgrade the CA SystemEDGE Model

The CA SystemEDGE agent could have been modeled in CA Spectrum before installing Virtual Host Manager or before the Hyper-V AIM was loaded on the agent. In this case, the existing CA SystemEDGE model is not compatible with Virtual Host Manager. Upgrade the model so that Virtual Host Manager can access the Hyper-V AIM capabilities in CA SystemEDGE. *This procedure is not required if the CA SystemEDGE agent with Hyper-V AIM is modeled after installing CA Spectrum.*

To upgrade the CA SystemEDGE model, right-click the model and select Reconfiguration, Reconfigure Model.

The CA SystemEDGE model is upgraded to support the Hyper-V AIM.

Note: You can also send a reconfigure model action to CA SystemEDGE using the CLI. For more information, see the *Modeling and Managing Your IT Infrastructure Administrator Guide*.

More information:

Adding SNMP Capabilities to VHM Models (see page 152)
Move a Hyper-V Virtual Machine to a Different Hyper-V Host (see page 155)
How to Configure Management Options (see page 164)

How Hyper-V Discovery Works

Hyper-V Discovery is a specialized discovery process that gathers detailed information about your virtual environment. The purpose of Hyper-V Discovery is to obtain the virtual entities managed by Microsoft Hyper-V, model the ones that do not exist in CA Spectrum, and place them under Virtual Host Manager in the Navigation panel.

A key benefit of Hyper-V Discovery is that it runs automatically in the background, continually keeping your virtual environment data updated in CA Spectrum. Understanding how Hyper-V Discovery works reinforces the importance of properly installing and modeling the various components of Virtual Host Manager.

The Hyper-V Discovery process works as follows:

1. Immediately after the CA SystemEDGE agent and Hyper-V AIM are installed, the Hyper-V AIM communicates with the Hyper-V Host to gather information about the virtual entities it manages. The Hyper-V AIM stores this information.

   Important! The CA SystemEDGE agent and Hyper-V AIM must be installed so that CA SystemEDGE, Hyper-V virtualization technology, and CA Spectrum can communicate. If they cannot, Hyper-V Discovery cannot run.

2. During CA Spectrum Discovery, CA Spectrum creates a Hyper-V Manager model for each server in Step 1 and enables CA Spectrum to handle communication between CA Spectrum and the CA SystemEDGE agent.

3. CA Spectrum polls the Hyper-V AIM to gather the Hyper-V information that is stored in Step 1.

4. CA Spectrum begins Hyper-V Discovery and uses this information from the AIM to update modeling in the CA Spectrum Topology tab and the Virtual Host Manager hierarchy in the Navigation panel, as follows:

   a. If you enable SNMP Discovery before Step 2, Virtual Host Manager Discovery creates SNMP models for all new SNMP-capable models that meet the SNMP Discovery criteria.

      Note: By default, SNMP Discovery is disabled during Hyper-V Discovery.

   b. VHM models (see definition on page 270) are created for the Hyper-V Managers.

   c. Previously existing Hyper-V virtual machine models are changed to VHM models.

   d. VHM models are created for the Hyper-V virtual machines that do not exist in CA Spectrum.

   e. VHM models are created for the Hyper-V Host models, and these models group their associated Hyper-V virtual machine models in the Navigation panel, under Virtual Host Manager and the Universe topology.

   f. All models for your virtual network are added to the Virtual Host Manager portion of the Navigation panel.

   Note: In a virtual environment, devices on separate ESX hosts can have the same IP address or MAC address. In this case, CA Spectrum creates duplicate models for each occurrence of an IP address or MAC address.

5. Hyper-V Discovery automatically repeats this process at each regularly scheduled Hyper-V polling interval.

   Note: By default, the Hyper-V polling interval is controlled by setting the polling interval on the Hyper-V Manager model. Or you can control Hyper-V polling by using the Hyper-V server application model.

More information:

Adding SNMP Capabilities to VHM Models (see page 152)
Move a Hyper-V Virtual Machine to a Different Hyper-V Host (see page 155)
How to Configure Management Options (see page 164)
Controlling Hyper-V AIM Polling (see page 165)
Configure Model Searches Across Secure Domains (see page 145)

Adding SNMP Capabilities to VHM Models

SNMP-capable virtual machines support enriched device monitoring, such as process and file system monitoring capabilities. However, SNMP agents can be costly and time-consuming to deploy. When an SNMP agent is not available or SNMP Discovery is disabled, Virtual Host Manager creates Hyper-V virtual machines as VHM models (see definition on page 270).

Later, you can install an SNMP agent on any virtual machine and upgrade its modeling in CA Spectrum. Options for upgrading to SNMP models are as follows:

- **Upgrade only selected devices**—This method works quickly when you have a small selection of models to upgrade. The VHM models and child models are deleted first. A drawback of this method is that after CA Spectrum deletes the models, you must wait for the next Hyper-V Discovery to create the new SNMP models and place them in Virtual Host Manager. Knowledge of the IP addresses for the models to upgrade is required.
- **Upgrade all SNMP-capable VHM models**—This method upgrades models in batch. It is preferred when upgrading Virtual Host Manager to a new release. For this method, knowledge of the IP addresses of individual models is not required. Another advantage is that after CA Spectrum deletes the VHM models, the upgraded SNMP models are immediately placed in the Virtual Host Manager hierarchy without waiting for the next polling cycle. Therefore, the child models are not left unmanaged.

  One drawback of this method is that it can take a long time to complete. The time required to complete this upgrade depends on how many community strings and SNMP ports Virtual Host Manager must search when locating SNMP-capable devices.

  Note: Virtual Host Manager attempts to identify SNMP agents on powered-up pingable virtual machines only.

Important! When models are deleted, all notes or other customizations on those models are lost.

More information:

How to Discover and Model Your Virtual Environment (see page 148)
Deleting Virtual Host Manager Models (see page 167)
Configure SNMP Modeling Preferences (see page 146)

Upgrade Selected VHM Models to SNMP Models

When an SNMP agent is not available or SNMP Discovery is disabled during Hyper-V Discovery, Virtual Host Manager creates Hyper-V virtual machines as VHM models (see definition on page 270). Later, you can install an SNMP agent on any virtual machine and upgrade its modeling in CA Spectrum. You must know the IP addresses for the device models to upgrade. Manually selecting models to upgrade works quickly, but all notes or customizations on these models are lost during the upgrade.

Follow these steps:

1. Deploy or enable an SNMP agent on the device, if required.
2. Model the device again using one of the following methods:
   - CA Spectrum Discovery
   - Model individual devices by IP address

   When the new SNMP-capable model is created, CA Spectrum removes the previous model from Virtual Host Manager and deletes it. At the next Hyper-V AIM polling cycle, CA Spectrum adds the SNMP-capable model to Virtual Host Manager in the Navigation panel.

   Important! When models are deleted, all notes or other customizations on those models are lost.

More information:

Manage Device Models for Devices Deleted from Microsoft Hyper-V (see page 144)
How to Discover and Model Your Virtual Environment (see page 148)
Deleting Virtual Host Manager Models (see page 167)

Upgrade All VHM Models to SNMP Models

When an SNMP agent is not available or SNMP Discovery is disabled during Hyper-V Discovery, Virtual Host Manager creates Hyper-V virtual machines as VHM models (see definition on page 270). Later, you can install an SNMP agent on any virtual machine and upgrade its modeling in CA Spectrum. When upgrading in batch, CA Spectrum searches all VHM models to find models that are now SNMP-capable devices. CA Spectrum converts them to SNMP models. This method can take a long time to complete, depending on how many community strings and ports Virtual Host Manager must search.

Follow these steps:

1. Deploy or enable an SNMP agent on your devices, as required.
2. Open Virtual Host Manager in the Navigation panel (see page 49).

   The main details page opens in the Contents panel for the selected Virtual Host Manager.
3. Select the Hyper-V Manager model in the Navigation panel that manages the models that you want to upgrade.
4. Click the Information tab.
5. Expand the Hyper-V Manager, CA Spectrum Modeling Control subview.
6. Click Upgrade ICMP-Only Devices.

   Important! When models are deleted, all notes or other customizations on those models are lost.

   Virtual Host Manager searches for VHM models managed by the Hyper-V AIM on the selected Hyper-V Manager device. Virtual Host Manager upgrades the ICMP-only devices that meet the criteria for SNMP devices and places them within the Virtual Host Manager hierarchy.

Move a Hyper-V Virtual Machine to a Different Hyper-V Host

Moving a Hyper-V virtual machine from one Hyper-V Host to another can result in lost data. The risk depends on your Virtual Host Manager configuration. The Hyper-V AIM does not support virtual machine migration. To Virtual Host Manager, a move is two events—the virtual machine is deleted from the original Hyper-V Host, and a new virtual machine is added to the new Hyper-V Host. In this case, Virtual Host Manager deletes the original virtual machine model and creates a new one. If you customized the original model, deleting it can result in lost data. You can avoid this data loss when you configure your Virtual Host Manager settings correctly before moving the virtual machine.

Follow these steps:

1. Change the 'Allow Device Model Deletes During Hyper-V Discovery' option to No (see page 144).

   Note: Disabling this option means that CA Spectrum does not delete the virtual machine model from CA Spectrum when the model is removed from Virtual Host Manager management.

2. Use the Microsoft Hyper-V virtualization technology to remove the virtual machine from the original Hyper-V Host.

3. Wait for Virtual Host Manager to reflect the changes in the Navigation panel.

4. Use the Microsoft Hyper-V virtualization technology to add the virtual machine to the other Hyper-V Host.

   When Hyper-V Discovery finds the new virtual machine, Virtual Host Manager reconciles it with the existing model. Virtual Host Manager places that model into Virtual Host Manager management.

5. (Optional) Change the 'Allow Device Model Deletes During Hyper-V Discovery' option back to Yes on the originating Hyper-V Manager model.

   The virtual machine is successfully moved.

More information:

How to Discover and Model Your Virtual Environment (see page 148)
Run CA Spectrum Discovery (see page 148)
Upgrade the CA SystemEDGE Model (see page 150)
How Hyper-V Discovery Works (see page 150)
How the Hyper-V Data is Updated in Virtual Host Manager (see page 158)

Viewing Your Hyper-V Virtual Environment

This section describes concepts for viewing your Hyper-V virtual environment and the associated alarms. The basic steps are no different from the standard CA Spectrum procedures. However, this section describes conceptual differences and details that only apply to the Hyper-V virtual technology.

Viewing Your Hyper-V Virtual Network

On the Explorer tab, the Virtual Host Manager node displays a hierarchical tree structure that helps you visualize the logical relationships among your virtual environment resources.

Using this information, you can see how resources are shared among your Hyper-V Managers. This information can help you identify opportunities to reorganize and optimize your virtual environment. The hierarchy also provides a quick way to monitor the performance of resources and troubleshoot alarms.

Because Virtual Host Manager is not aware of a DSS environment (see definition on page 268), it is located within a landscape hierarchy. The following example shows where Virtual Host Manager appears on the Explorer tab in the Navigation panel and illustrates the virtual environment hierarchy:

```
[-] SpectroSERVER host
    [+] Universe
    [-] Virtual Host Manager
        [-] Hyper-V
            [+] Hyper-V Manager 1
            [-] Hyper-V Manager 2
                [-] Hyper-V Host
                      .  Hyper-V Manager 2 (management operating system)
                      .  Hyper-V virtual machine 1
                      .  Hyper-V virtual machine 2
```

Note: The Hyper-V management operating system is represented in the virtual topology as part of the Hyper-V Manager model.

Virtual Host Manager is the root node for the entire virtual environment that is managed by this SpectroSERVER. Selecting this node in the Navigation panel displays Virtual Host Manager details in the Contents panel. You can view details such as events and alarms related to your virtual environment.

Directly under Virtual Host Manager, virtual environments are organized within folders that represent the associated technology. In the example hierarchy above, the Hyper-V folder contains the portion of the virtual environment that was created using Microsoft Hyper-V virtualization technology. In this folder, Virtual Host Manager lists all Hyper-V Manager hosts managed by this SpectroSERVER.

Each Hyper-V Manager contains only the portion of the entire virtual environment that it manages. Selecting a Hyper-V Manager in the Navigation panel displays details in the Contents panel, such as the Hyper-V Hosts or Hyper-V virtual machines managed by the selected Hyper-V Manager.

Under each Hyper-V Manager, the hierarchy represents the logical relationships between the following entities:

- **Hyper-V Hosts**

  A Hyper-V Host contains the Hyper-V virtual machines that it manages. Selecting a Hyper-V Host in the Navigation panel displays details in the Contents panel such as events and alarms related to the Hyper-V Host, memory usage, status, and more.

- **Hyper-V Management Operating System**

  The Hyper-V Management Operating System model appears as a child to its corresponding Hyper-V Host model and is always a leaf node on the Virtual Host Manager hierarchy tree. This model shares the name and model type of its parent. Although this model appears to be the same as the Hyper-V Manager model, the instance that appears under the Hyper-V Host model represents the management operating system running on the Hyper-V Host. Hyper-V uses this operating system to configure the hosted Hyper-V virtual machines. Selecting a Hyper-V Management Operating System model in the Navigation panel displays details in the Contents panel, including system status and CPU and memory usage.

- **Hyper-V Virtual Machines**

  A Hyper-V virtual machine is always a leaf node on the Virtual Host Manager hierarchy tree. Selecting a Hyper-V virtual machine in the Navigation panel displays details in the Contents panel, such as events and alarms that are related to the virtual machine, memory usage, and status.

More information:

How Virtual Host Manager Works with Hyper-V (see page 139)
Models Created for Hyper-V (see page 141)
Run CA Spectrum Discovery (see page 148)
Custom Subviews for Virtual Entity Types (see page 160)
Locater Tab for Hyper-V Searches (see page 161)

Understanding the Hyper-V Virtual Topology

The Hyper-V Manager/Management Operating System, Hyper-V Host, and Hyper-V virtual machine models created for your virtual environment are integrated into the topology view. Hyper-V Host models automatically group their associated Hyper-V virtual machines. The topology shows how these Hyper-V virtual machines are connected to your physical network entities.

Note: The Hyper-V management operating system is represented in the virtual topology as part of the Hyper-V Manager model.

The following example shows how these models can appear on the Explorer tab in the Navigation panel under the Universe group:

```
[-] Universe
     .  Physical switch 1
     .  Physical switch 2
    [-] Hyper-V Host
          .  Fanout 1
          .  Fanout 2
          .  Hyper-V Manager (management operating system)
          .  Hyper-V virtual machine 1
          .  Hyper-V virtual machine 2
          .  Hyper-V virtual machine 3
```

Selecting one of these models displays these relationships graphically on the Topology tab in the Contents panel.

How the Hyper-V Data is Updated in Virtual Host Manager

After CA Spectrum builds your initial Hyper-V hierarchy, your virtual network configuration can change. Virtual Host Manager continually works to keep this information accurate in CA Spectrum. For example, the following events can change your virtual network configuration:

- Creating or deleting a Hyper-V virtual machine on a Hyper-V Host
- Manually moving a Hyper-V virtual machine from one Hyper-V Host to another

To keep your information accurate, Virtual Host Manager detects these changes by polling the Hyper-V AIM. Therefore, your virtual network configuration changes, if any, are reflected in CA Spectrum at each polling cycle. CA Spectrum also receives traps from the AIM and generates the corresponding events. By reviewing the event log, you can find out when configuration changes occur, such as when a new virtual machine is created.

When a virtual machine is deleted, CA Spectrum removes the models from the Virtual Host Manager hierarchy on the Explorer tab. When the AIM detects an addition to your virtual network configuration, such as creating a new virtual machine or placing one into management, CA Spectrum performs the following tasks:

- Updates the placement of your virtual device models in the hierarchy of the Explorer tab
- *Automatically* rediscovers connections to the affected Hyper-V Manager and virtual machine models and associates them with the correct Hyper-V Host in the topology

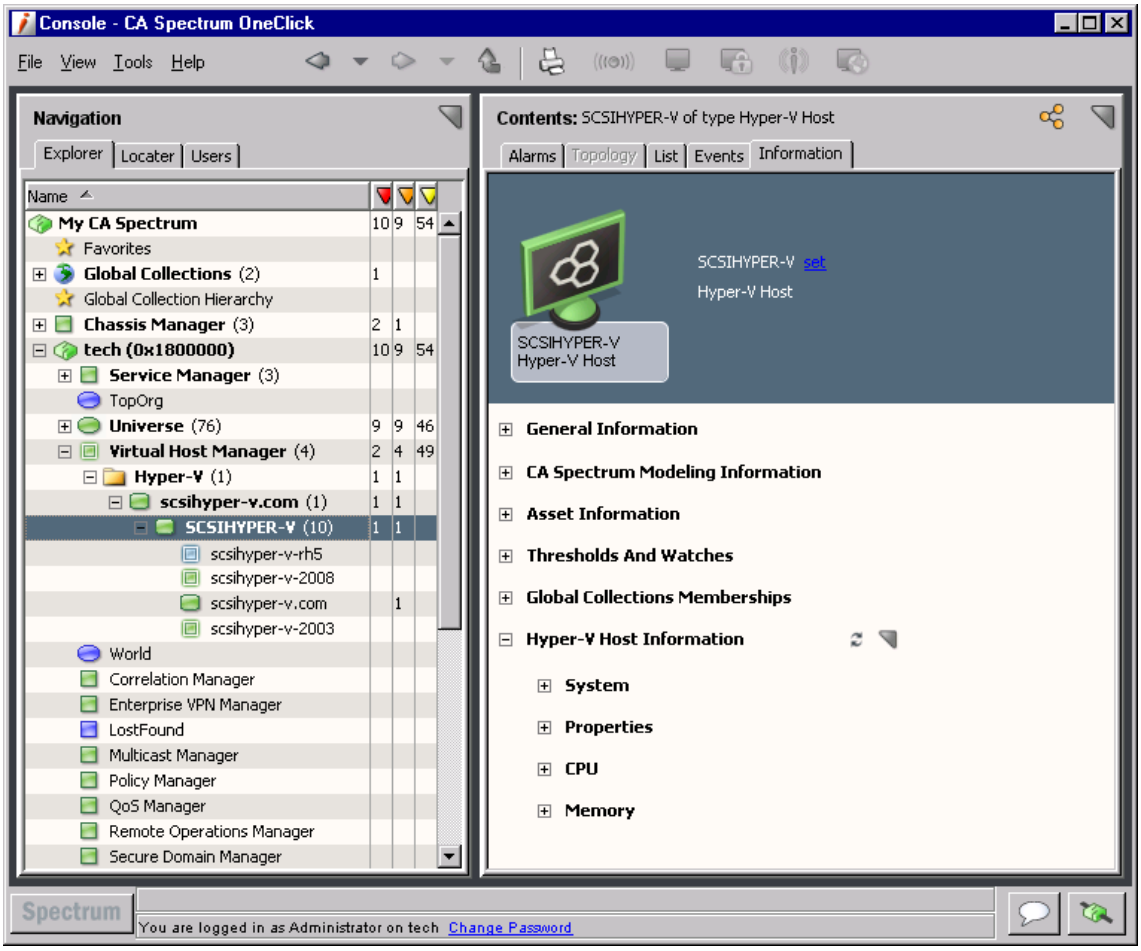
  Note: Although most components of your virtual environment are discovered automatically, the CA Spectrum administrator should initiate a new SNMP discovery to model *new* switches or routers. This discovery is necessary only when a new virtual host is configured that does not share connections with the existing virtual network models.

More information:

How Virtual Host Manager Works (see page 11)
Models Created for Hyper-V (see page 141)
Manage Device Models for Devices Deleted from Microsoft Hyper-V (see page 144)
Move a Hyper-V Virtual Machine to a Different Hyper-V Host (see page 155)
Viewing Your Hyper-V Virtual Network (see page 156)
Configure and Monitor Resource Status (see page 164)

Custom Subviews for Virtual Entity Types

Your Virtual Host Manager models collectively provide information about your virtual environment. Individually, each model provides unique information or configuration settings, depending on the virtual entity type it represents. This custom subview appears on the Information tab in the Contents panel. These subviews can contain real-time data, such as CPU status or memory utilization. For example, the custom subview for a Hyper-V Manager is the "Hyper-V Manager" subview, as shown:



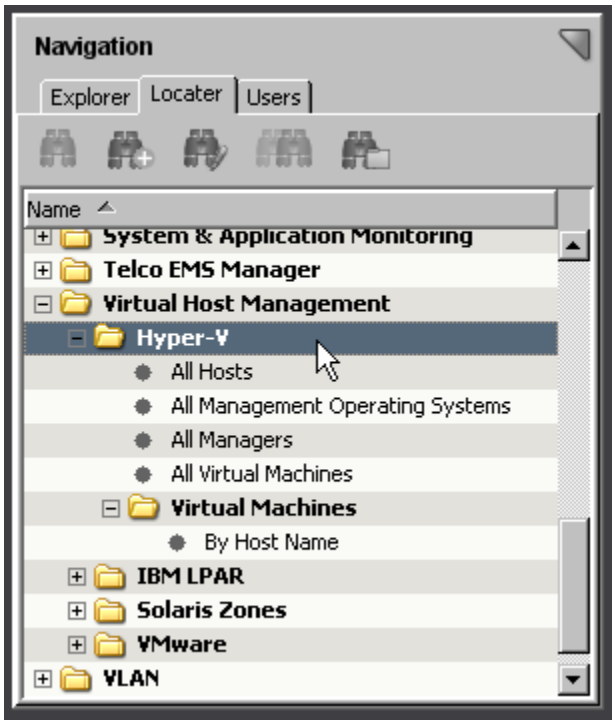
Note: The Hyper-V Manager model provides combined information for all virtual devices managed by the Hyper-V Manager. That is, selecting the Hyper-V Manager model in the Navigation panel displays information about the selected Hyper-V Manager host *and* combined information about all Hyper-V Hosts and Hyper-V virtual machines. This information is the same data displayed on the Information tab for each individual entity model. The combined view in the Hyper-V Manager model can provide a good overview about all of the virtual entities it manages.

More information:

Viewing Your Hyper-V Virtual Network (see page 156)
Configure and Monitor Resource Status (see page 164)

Locater Tab for Hyper-V Searches

In addition to viewing details about your virtual environment on the Explorer tab, you can also use the Locater tab to run preconfigured Virtual Host Manager searches. The search options are grouped under the Virtual Host Management, Hyper-V folder on the Locater tab, as shown:



These detailed searches can help you investigate information related to virtual entities only, such as locating all Hyper-V virtual machines within a landscape.

Note: Although Virtual Host Manager is not DSS (see definition on page 268) aware, these preconfigured searches let you select multiple landscapes to search in the search parameters.

The Locater tab in the Navigation panel includes the following searches for Virtual Host Manager information:

All Hosts

Locates all Hyper-V Host servers that have been modeled in the CA Spectrum database for your virtual network.

All Management Operating Systems

Locates all Hyper-V management operating systems (see definition on page 269) that have been modeled in the CA Spectrum database for your virtual network.

Note: The Hyper-V management operating system is represented in the virtual topology as part of the Hyper-V Manager model.

All Managers

Locates servers hosting the CA SystemEDGE agent with Hyper-V AIM enabled that have been modeled in the CA Spectrum database for your virtual network.

All Virtual Machines

Locates all Hyper-V virtual machines that have been modeled in the CA Spectrum database for your virtual network.

Virtual Machines, By Host Name

Locates virtual machines in the CA Spectrum database managed by only one or a select group of Hyper-V Hosts.

More information:

Viewing Your Hyper-V Virtual Network (see page 156)

Status Monitoring Options

CA Spectrum provides a wide range of options for monitoring the state of your virtual network resources. The status information available for a resource varies, depending on the type of virtual entity you are monitoring. Also, your ability to configure a status option depends on its type. For example, some status options are read-only, but others let you enable behaviors or select an alarm severity. Providing this range of options and levels of customization, CA Spectrum lets you decide how to best monitor the performance of your virtual network.

Status fields are located in the OneClick subviews. All status information for a given virtual environment is available on the Hyper-V Manager model in a tabular format. Also, each virtual entity type that has a unique model in CA Spectrum provides a subset of the same status information for easy viewing. Status-related settings, including the alert type and monitor settings, can be set from either view location.

The following tables outline the type of status information available for each virtual entity type. The Subview Locations column describes where the corresponding status fields are located in OneClick. For example, "memory" information for a Hyper-V virtual machine model is available on the Information tab in the following two locations:

- Virtual Machine Information subview for the Hyper-V virtual machine model
- Hyper-V Manager, Managed Environment, Virtual Machines subview for the Hyper-V Manager model

To explore the exact status options available for each status information type, locate the subview in OneClick.

Hyper-V Manager

Status Information Type	Subview Locations
Overall	Hyper-V Manager

Hyper-V Host

Status Information Type	Subview Locations
Overall	Hyper-V Host
CPU	Hyper-V Host, Hyper-V Manager
Memory	Hyper-V Host, Hyper-V Manager

Hyper-V Virtual Machine

Status Information Type	Subview Locations
Overall	Hyper-V virtual machine, Hyper-V Manager
Memory	Hyper-V virtual machine, Hyper-V Manager
CPU	Hyper-V virtual machine, Hyper-V Manager

More information:

Configure and Monitor Resource Status (see page 164)
Virtual Host Manager Alarms for Hyper-V (see page 168)
Traps Supported in Virtual Host Manager (see page 170)

How to Configure Management Options

After your virtual network is modeled, you can configure Virtual Host Manager options for viewing and managing your device models. Configuring your preferences helps ensure that Virtual Host Manager handles your virtual device models correctly and monitors only the information that is important to you.

To configure your installation of Virtual Host Manager, perform the following procedure after you discover and model your virtual network:

- Configure threshold values and other status monitoring options (see page 164)—These options let you determine which information you want to monitor and how CA Spectrum manages the various events that occur in your virtual network.

More information:

Upgrade the CA SystemEDGE Model (see page 150)
How the Hyper-V Data is Updated in Virtual Host Manager (see page 158)

Configure and Monitor Resource Status

You can monitor the status of virtual resources in OneClick. For example, you can view the total physical memory or used physical memory, and more. You can also set monitoring options, such as enabling alerts. This information can help you optimize your virtual network performance and troubleshoot alarms.

Note: Traps are set on and managed by the Hyper-V AIM.

You can view or configure resource status options and information for virtual devices on the Information tab.

Follow these steps:

1. Open Virtual Host Manager in the Navigation panel (see page 49).

   The main details page opens in the Contents panel for the selected Virtual Host Manager.

2. Locate and click the virtual device on the Explorer tab in the Navigation panel.

   The device details display in the Contents panel.

3. Click the Information tab.

   Multiple subviews are available for viewing. Generally, the subview at the bottom of the tab includes the resource allocation and utilization information for the selected model. For example, a Hyper-V Host model displays a subview named "Hyper-V Host Information" that includes details for the specific Hyper-V Host model you selected in the Navigation panel.

4. Expand the appropriate subview.

   All available resource status details and monitoring options for the selected device model are displayed.

   Note: The Hyper-V Manager model provides combined information for all virtual devices managed by the Hyper-V Manager. That is, selecting the Hyper-V Manager model in the Navigation panel displays information about the selected Hyper-V Manager host *and* combined information about all Hyper-V Hosts and Hyper-V virtual machines. This information is the same data displayed on the Information tab for each individual entity model. The combined view in the Hyper-V Manager model can provide a good overview about all of the virtual entities it manages.

More information:

Custom Subviews for Virtual Entity Types (see page 160)
Status Monitoring Options (see page 162)
How to Configure Management Options (see page 164)
Virtual Host Manager Alarms for Hyper-V (see page 168)

Controlling Hyper-V AIM Polling

When you are tuning Virtual Host Manager performance, you can change the Hyper-V Manager polling rate or disable Hyper-V technology polling. By default, the polling attributes on the Hyper-V Manager model control the Hyper-V polling behavior. Or you can change this Hyper-V polling behavior independently. The Hyper-V technology application model, HyperVAimApp, controls your Hyper-V polling.

The following two attribute values on the application specifically control the Hyper-V polling logic:

- PollingStatus
- Polling_Interval

Both the Hyper-V Manager model and the HyperVAimApp application model contain these attributes. PollingStatus disables and enables polling while Polling_Interval controls the polling frequency. If their values are different, the HyperVAimApp application model attribute values take precedence when determining Hyper-V technology polling behavior.

This ability to set the value for the device model and application model lets you fine-tune your Hyper-V technology polling. For both PollingStatus and Polling_Interval, modifying the attribute on the Hyper-V Manager device model also changes the corresponding application model attribute when their values are the same.

More information:

How Hyper-V Discovery Works (see page 150)

Configure the Hyper-V AIM Polling Interval

You can change the Hyper-V AIM polling rate. Configure the polling interval by setting the Polling_Interval attribute on the Hyper-V technology application model.

Follow these steps:

1. Open OneClick and click the Locater tab in the Navigation panel.
2. Expand the Application Models folder and double-click 'By Device IP Address.'

   A search dialog opens.
3. Enter the IP address for your Hyper-V Manager device in the Device IP Address field, and click OK.

   A list of application models for the Hyper-V Manager appears in the Contents panel.
4. Select the HyperVAimApp application model.

   The application model details appear in the Component Details panel.
5. Click the Information tab in the Component Details panel.
6. Open the Modeling Information subview.
7. Click set in the Polling Interval (sec) field, enter a new value.

   Note: Changing the Polling Interval value from any number to 0 also sets the Polling field to Off, disabling Hyper-V AIM polling. However, if you set the Polling Interval to 0 and set the Polling field to On, Hyper-V AIM polling continues, using the polling interval for the Hyper-V Manager device.

   The Hyper-V AIM polling interval setting is modified.

Disable Hyper-V AIM Polling

You can disable Hyper-V AIM polling. Disabling Hyper-V polling is the same as disabling Virtual Host Manager. Disable polling by setting the PollingStatus attribute on the Hyper-V virtual technology application model.

Follow these steps:

1. Open OneClick and click the Locater tab in the Navigation panel.
2. Expand the Application Models folder and double-click 'By Device IP Address.'

   A search dialog opens.
3. Enter the IP address for your Hyper-V Manager device in the Device IP Address field and click OK.

   A list of application models for the Hyper-V Manager appears in the Contents panel.
4. Select the HyperVAimApp application model.

   The application model details appear in the Component Details panel.
5. Click the Information tab in the Component Details panel.
6. Open the CA Spectrum Modeling Information subview.
7. Click set in the Polling field and select Off.

   Polling is disabled for the Hyper-V AIM on the selected Hyper-V Manager.

Deleting Virtual Host Manager Models

Models can be deleted from OneClick at any time for various reasons. However, Virtual Host Manager restricts your ability to delete models from the Virtual Host Manager hierarchy in the Navigation panel. To delete models manually, you have the following two options:

- Delete the Hyper-V folder or a Hyper-V Manager model in Virtual Host Manager
- Remove a virtual entity using your Microsoft Hyper-V virtualization technology

In Virtual Host Manager, models are sometimes deleted automatically. The following circumstances cause CA Spectrum to delete Virtual Host Manager models automatically:

- **Hyper-V folder deleted or Hyper-V Manager model removed from Virtual Host Manager**

  If you remove a Hyper-V Manager model or delete the Hyper-V folder from the Navigation panel, CA Spectrum deletes all related child models.

- **An entity removed from Hyper-V virtual environment**

  As you delete Hyper-V Hosts and the Hyper-V Manager using your Microsoft Hyper-V virtualization technology, CA Spectrum may also delete those models and their child models from Virtual Host Manager, according to your configuration settings.

- **Upgraded models exist**—In some cases, a Hyper-V Host is first modeled for Virtual Host Manager without SNMP capabilities. If SNMP capabilities are later added to a VHM model (see definition on page 270), the previous model is deleted and replaced with the new SNMP-capable model.

Note: Although the default setting is to delete the models, you can configure Virtual Host Manager to place the Hyper-V Host and Hyper-V virtual machine models in the LostFound container when they are removed from Virtual Host Manager. This setting is respected only when you remove an entity using your Microsoft Hyper-V virtual environment. However, this setting does not apply when you delete the Hyper-V folder, remove a Hyper-V Manager model, or upgrade a VHM model.

More information:

Manage Device Models for Devices Deleted from Microsoft Hyper-V (see page 144)
Adding SNMP Capabilities to VHM Models (see page 152)
Manage SNMP-Enabled Virtual Machine Models After Hyper-V Manager Deletion (see page 147)

Alarms and Fault Isolation for Hyper-V

This section describes the traps used by Virtual Host Manager and the resulting alarms. This section also explains how Virtual Host Manager fault isolation differs from basic CA Spectrum fault isolation.

Virtual Host Manager Alarms for Hyper-V

To alert you to problems within your virtual network, CA Spectrum generates alarms during polling. Polling generates four alarms: Hyper-V Proxy Lost, Hyper-V Host Proxy Lost, Hyper-V Manager Unavailable, and Hyper-V Virtual Machine Not Running.

More information:

Manage Device Models for Devices Deleted from Microsoft Hyper-V (see page 144)
Status Monitoring Options (see page 162)
Configure and Monitor Resource Status (see page 164)
Manage SNMP-Enabled Virtual Machine Models After Hyper-V Manager Deletion (see page 147)

How CA Spectrum Forwards Traps from CA SystemEDGE

CA Spectrum supports all traps that are sent by the Hyper-V AIM. These traps are initially sent to Hyper-V CA SystemEDGE model. If the destination for a trap is not the Hyper-V model, CA Spectrum forwards the trap to the correct virtual model.

Note: For specific event codes related to the traps, use the Event Configuration application and filter on "0x056e." Alternately, you can launch MIB tools to view the traps in the Trap Support table for the "CAHYPERV-AIM-MIB" MIB. For more information about using the Event Configuration application, see the *Event Configuration User Guide*. For more information about using MIB tools, see the *Modeling and Managing Your IT Infrastructure Administrator Guide*.

CA Spectrum determines where to forward the trap by using the following process:

1. When CA Spectrum receives a trap, it uses varbind information in the trap to identify the UID for the target device.
2. CA Spectrum uses this UID to look up and locate the CA Spectrum model that is tied to a given UID. The entity type of all traps is predetermined. Depending on the results of the look-up, CA Spectrum forwards the trap as follows:
   - If it finds a CA Spectrum model of a specific type with a given UID, CA Spectrum forwards the event and corresponding alarm to the destination model.
   - If it cannot find a CA Spectrum model for a given UID, CA Spectrum generates a new generic event on the Hyper-V Manager model. This new event includes details about the trap.

     Note: CA Spectrum often cannot find a related model when a trap is sent immediately after changing your virtual network entities in the Hyper-V virtualization technology. Hyper-V Discovery has not yet identified and created the corresponding model in CA Spectrum.

More information:

Traps Supported in Virtual Host Manager (see page 170)

Traps Supported in Virtual Host Manager

All traps generated by the Hyper-V AIM are supported in CA Spectrum. The traps are initially sent to the Hyper-V Manager model. Then, the traps are forwarded to a corresponding virtual entity type (that is, the "destination" entity), depending on the type of trap. Using these traps, you can monitor the performance of your virtual network, resolve any resulting alarms, or trigger events.

Note: For more information about traps generated by the Hyper-V AIM, see the *CA Virtual Assurance for Infrastructure Managers Administration Guide*.

The following tables list the traps for a specific destination entity type and specify whether the trap generates an alarm.

Hyper-V Manager Traps

Trap Name	Trap OID	Alarm?
hypervAimStatVMAddTrap	1.3.6.1.4.1.546.1.1.6.16501	No
hypervAimStatVMRemoveTrap	1.3.6.1.4.1.546.1.1.6.16502	No
hypervAimStatVMMigrateTrap	1.3.6.1.4.1.546.1.1.6.16505	No

Hyper-V Virtual Machine Traps

Trap Name	Trap OID	Alarm?
hypervAimStatVMEnabledTrap	1.3.6.1.4.1.546.1.1.6.16504	No

More information:

How the Hyper-V Data is Updated in Virtual Host Manager (see page 158)
Status Monitoring Options (see page 162)
How to Configure Management Options (see page 164)
Configure and Monitor Resource Status (see page 164)
How CA Spectrum Forwards Traps from CA SystemEDGE (see page 169)

Fault Management for Virtual Networks

The goal of fault isolation is to narrow down the root cause of a networking problem. Finding the root cause can help you to troubleshoot and quickly correct the problem or to correct the problem programmatically with automated scripts. Deciding which devices are the root cause of an alarm can be difficult, because problems with a single device can cause several devices in your network to generate events.

For example, losing contact with a Hyper-V Host often means that you have also lost contact with the Hyper-V virtual machines it manages. Therefore, the Hyper-V Host device model and all affected virtual machines generate alarms. Using fault isolation techniques, Virtual Host Manager correlates these alarms in an attempt to identify a single root cause.

Virtual networks provide a unique management opportunity, because they provide CA Spectrum an alternate management perspective. That is, CA Spectrum can gather information through direct contact with your virtual devices or through the virtual network management technology, Microsoft Hyper-V. This alternate management perspective enhances standard CA Spectrum fault management in two ways:

- **Enhanced Contact Lost alarms**—Two sources of information about a device means Virtual Host Manager can pinpoint the cause and more easily correlate events to a single root cause.
- **Proxy Failure alarms**—*Proxy management* is the act of managing network devices using an alternate management source in place of or in addition to the primary manager. For example, CA Spectrum can manage virtual network devices by contacting them directly or through the virtual technology application's contact with the devices. When Hyper-V virtualization technology loses contact with a virtual network device, Virtual Host Manager generates one of the Proxy Management Lost alarms for each device. These alarms are unique, because they are alerting you to the fact that *management* of the device through the *proxy* is affected, not the state of the device or direct (SNMP) management.

How Fault Isolation Works when Device Contact is Lost

To help you troubleshoot networking problems with your devices, CA Spectrum uses fault isolation to narrow down the root cause of an alarm. For virtual networks, Virtual Host Manager uses information from direct contact with the device plus information provided by Hyper-V virtualization technology through the Hyper-V AIM. In many cases, standard CA Spectrum fault management can pinpoint the root cause. But in special circumstances, the method for isolating problems in a virtual network go beyond the standard methods.

The type of fault isolation Virtual Host Manager uses to discover the root cause depends on which devices are alarming and the type of events the devices generate. The following scenarios describe two unique fault management situations and how CA Spectrum isolates the networking error in your virtual network.

Scenario 1: Hyper-V virtual machine is not running

In a virtual environment, the virtual management application can provide more details than CA Spectrum can discover through standard device monitoring. For example, the Hyper-V virtualization technology is aware when a Hyper-V virtual machine changes from the "running" state to something else, such as the "not running" state.

If a Hyper-V virtual machine is no longer running and CA Spectrum loses contact with it, but proxy management (see definition on page 269) of the Hyper-V Manager is uninterrupted, CA Spectrum determines the root cause as follows:

1. When CA Spectrum loses contact with a Hyper-V virtual machine, it generates a Contact Lost alarm.
2. During its next polling cycle, the Hyper-V Manager model polls the Hyper-V AIM to gather information about the virtual machine. Because Hyper-V technology manages the virtual machine, it can provide a unique view into the possible cause of alarms generated by a Hyper-V virtual machine.
3. If the Hyper-V virtualization technology finds that the virtual machine is in the not-running mode, it generates a Virtual Machine Not Running alarm.

   Note: This alarm is cleared upon the first Hyper-V AIM polling cycle after the virtual machine is running again.
4. Virtual Host Manager correlates the Contact Lost alarm to the corresponding Virtual Machine Not Running alarm created by CA Spectrum. Virtual Host Manager makes the Contact Lost alarm appear as a symptom of the Virtual Machine Not Running alarm.

Scenario 2: Hyper-V Host is down

If CA Spectrum loses contact with a modeled Hyper-V Manager and all Hyper-V virtual machines running on that host, CA Spectrum checks the status of the upstream routers and switches. Depending on their status, CA Spectrum determines the root cause as follows:

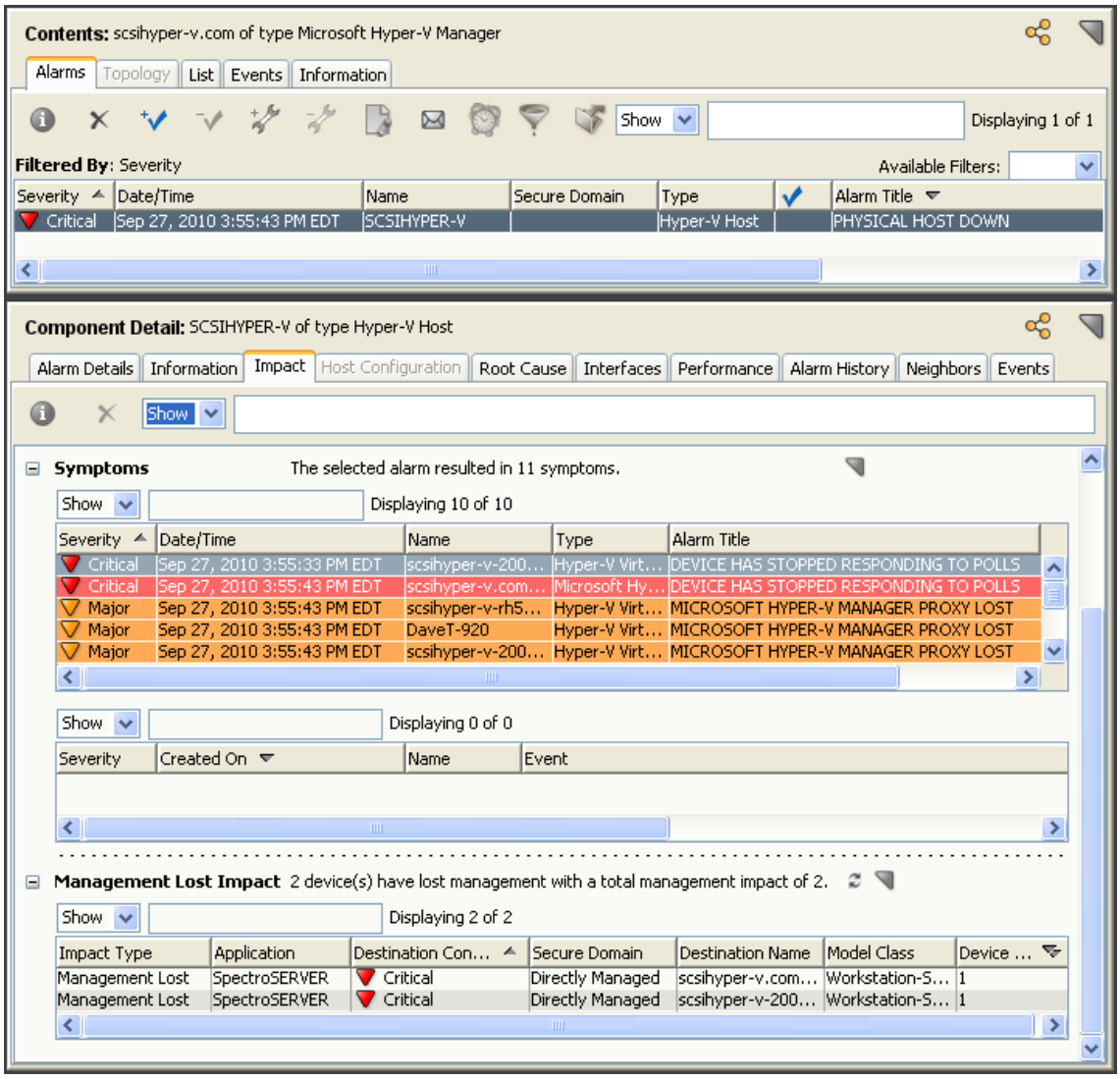
- All upstream devices for one or more virtual machines or the Hyper-V Manager are unavailable—Standard CA Spectrum fault isolation techniques determine the root cause, as follows:
  - Device Stopped Responding to Polls alarm—Generated on the Hyper-V Host when at least one upstream connected device for any virtual machine or Hyper-V Manager is up.
  - Gateway Unreachable alarm—Generated on the Hyper-V Host when *all* upstream connected devices are down.
- At least one upstream device is available for every virtual machine and Hyper-V Manager model connected to the Hyper-V Host—CA Spectrum infers that the Hyper-V Host is the root cause and responds as follows:
  a. The Hyper-V Manager model and all Hyper-V virtual machines, ports, and fanouts that are directly connected to the Hyper-V Manager model or virtual machine models generate the standard fault isolation alarms.
  b. Virtual Host Manager creates a Physical Host Down alarm for the Hyper-V Host model.

c. All fault isolation-related alarms that are created for the impacted devices (such as virtual machines, ports, and fanouts) are correlated to the Physical Host Down alarm, making them symptoms of the Physical Host Down alarm. These symptom alarms appear in the Symptoms table on the Impact tab for the Physical Host Down alarm.

   Note: For each Hyper-V Host model, Virtual Host Manager creates a "virtual fault domain." This domain includes the Hyper-V Host, Hyper-V Manager, and virtual machines, plus all ports and fanouts directly connected to the Hyper-V Manager model or virtual machines. When the Hyper-V Host generates the Physical Host Down alarm, all standard fault isolation alarms within the domain are correlated to it. Correlating these alarms as symptoms indicates that the Physical Host Down alarm on the Hyper-V Host is the root cause.

d. All impacted devices are listed in the Management Lost Impact table on the Impact tab for the Physical Host Down alarm.

Note: Devices that are suppressed do not have a corresponding alarm in the Symptoms table.



e. If all upstream devices for one or more virtual machines or the Hyper-V Manager go down, CA Spectrum can no longer reliably state that the fault lies with the Hyper-V Host. Therefore, CA Spectrum clears the Physical Host Down alarm and applies the standard CA Spectrum fault isolation techniques.

More information:

How Fault Isolation Works when Proxy Management is Lost (see page 175)
Determining Hyper-V Virtual Machines Affected by Hyper-V Host Outages (see page 177)

How Fault Isolation Works when Proxy Management is Lost

The Microsoft Hyper-V virtualization technology used to create your virtual network provides CA Spectrum a unique management opportunity. CA Spectrum can use the standard methods to contact your virtual devices directly, plus CA Spectrum can simultaneously gather virtual device information from Hyper-V technology. In this sense, the Hyper-V technology is a "proxy" from which CA Spectrum gathers virtual device information. If CA Spectrum loses direct contact with a device, it generates alarms. Likewise, if Hyper-V technology loses contact with a virtual device or if Virtual Host Manager loses contact with the Hyper-V Manager, Virtual Host Manager generates alarms—Proxy Management Lost alarms (see definition on page 269).

In response, CA Spectrum attempts to isolate the cause of the proxy management failure. Proxy fault isolation is similar to the standard CA Spectrum fault isolation, except that these alarms alert you to the fact that *proxy* management of a virtual device is affected. Proxy management fault isolation cannot tell you whether a virtual device is up or down. However, it is important to know when contact through the proxy is lost, because you could be missing important virtual information about a device.

The type of proxy fault isolation Virtual Host Manager uses to discover the root cause depends on which devices are alarming and the type of events the devices generate. The following scenario describes a unique proxy fault management situation and how Virtual Host Manager isolates the networking error in your virtual network.

Scenario: Contact between CA Spectrum and Hyper-V Manager is lost

If CA Spectrum loses contact with or stops polling the Hyper-V Manager model, CA Spectrum loses the Hyper-V virtualization technology data about all virtual models managed by that Hyper-V Manager. To isolate the problem, Virtual Host Manager determines the root cause as follows:

1. CA Spectrum generates Proxy Lost alarms for all virtual models managed by that Hyper-V Manager, including virtual machines and Hyper-V Hosts. CA Spectrum also generates a separate Proxy Unavailable alarm on the Hyper-V Manager model.
2. The virtual machine alarms are correlated to their corresponding Hyper-V Host model alarm.
3. The Hyper-V Host model alarms are correlated to a Proxy Unavailable alarm for the Hyper-V Manager model.
4. This Proxy Unavailable alarm is then correlated to the root cause of the Hyper-V Manager being down. The root cause is typically an alarm generated by standard CA Spectrum fault management, such as the alarms created for the following situations:
   - Lost management of Hyper-V Manager (that is, a problem occurred with the CA SystemEDGE agent on the Hyper-V Manager host)
   - Machine contact is lost
   - Hyper-V Manager model is in maintenance mode

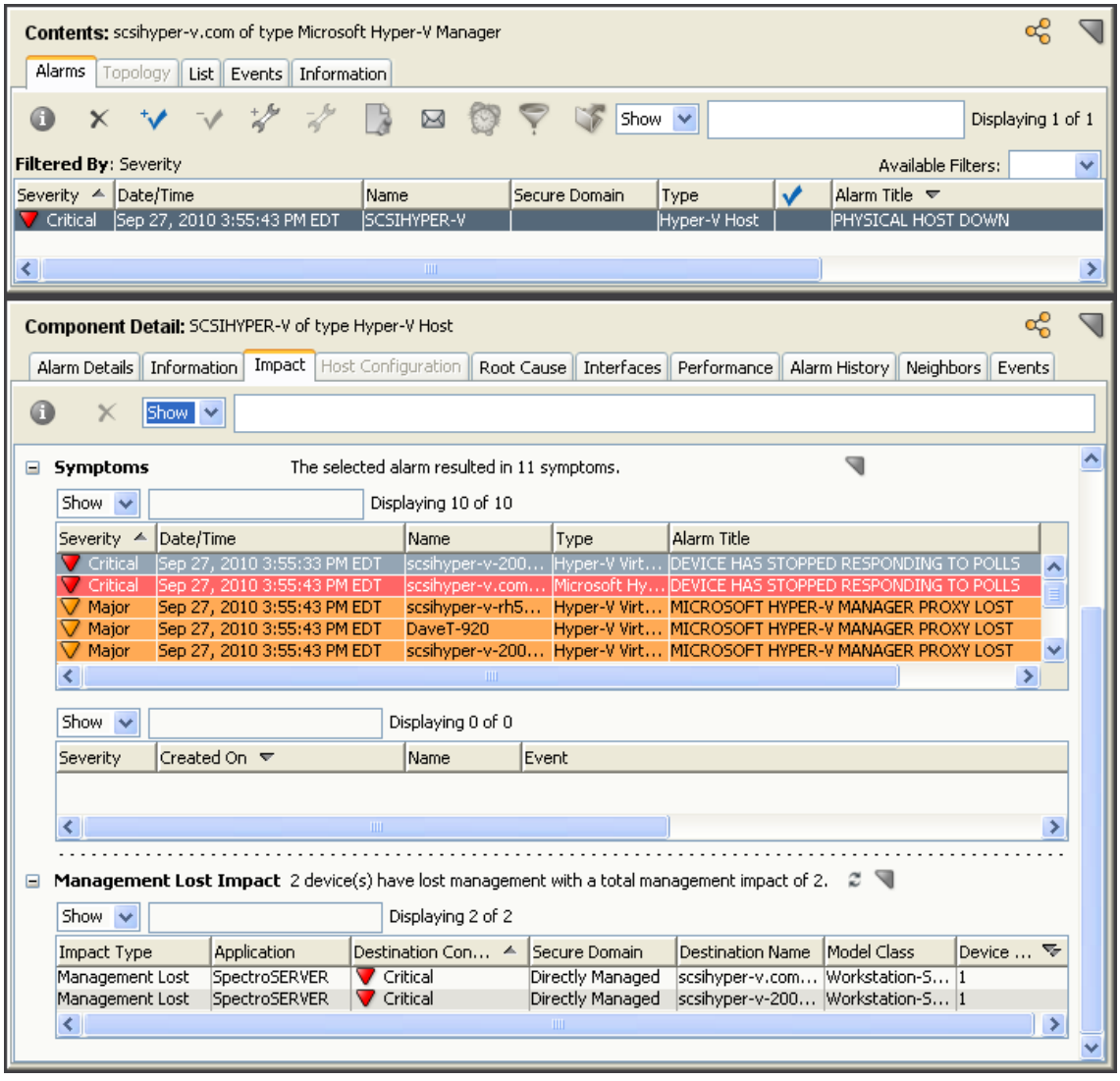
More information:

How Fault Isolation Works when Device Contact is Lost (see page 171)

Determining Hyper-V Virtual Machines Affected by Hyper-V Host Outages

When contact with a Hyper-V Host is interrupted or the Hyper-V Host goes down, all Hyper-V virtual machines hosted by the Hyper-V Host are affected. Because Hyper-V technology cannot communicate with the Hyper-V Host to get usage information, you might not receive alarms for a critical virtual machine on that Hyper-V Host. To find out if a critical virtual machine is impacted, you can view a list of affected virtual machines on the Impact tab of the alarm, as follows:

- Symptoms subview—displays all symptom alarms generated by the affected Hyper-V virtual machines
- Management Lost Impact subview—lists the Hyper-V virtual machines impacted by the alarm



More information:

How Fault Isolation Works when Device Contact is Lost (see page 171)

Chapter 6: IBM LPAR

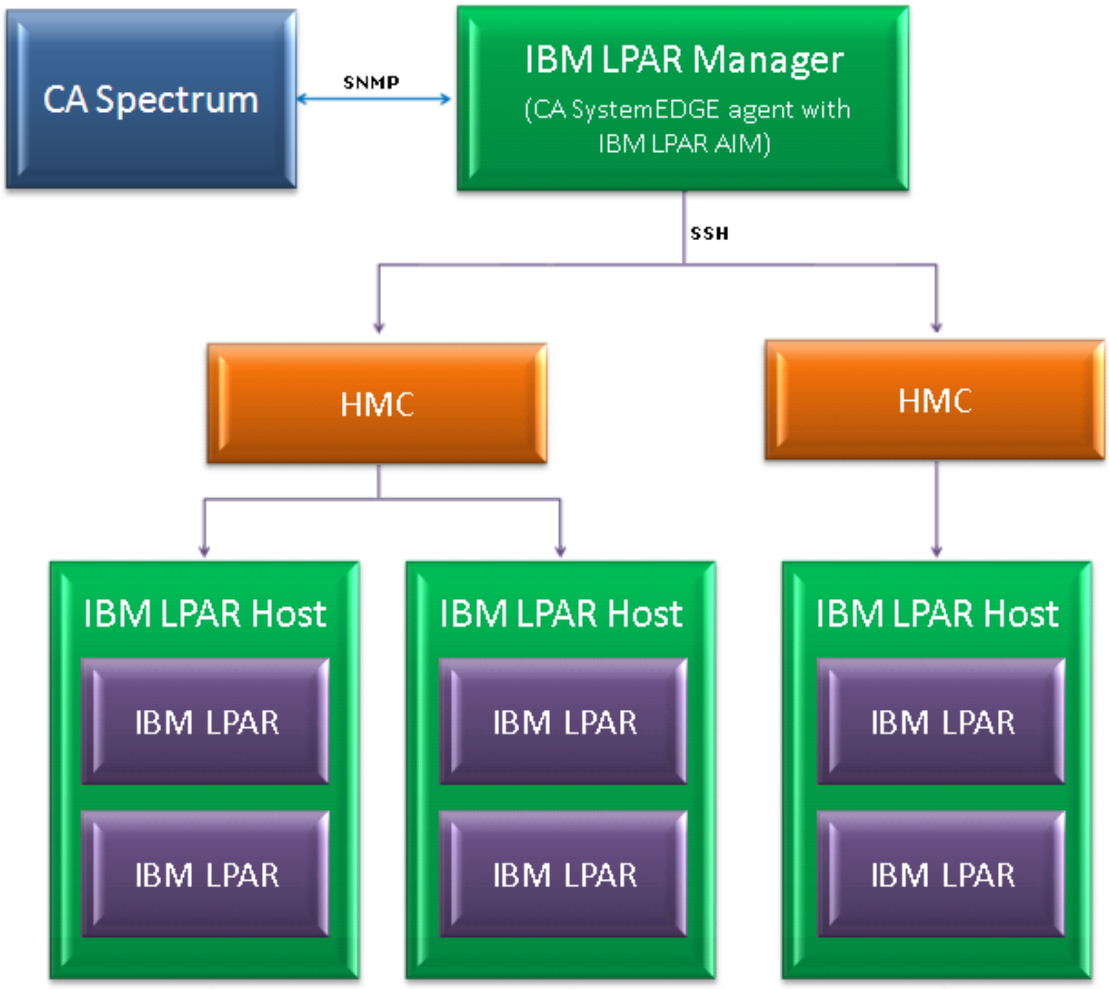
This section is for IBM LPAR virtualization technology users and describes how to use Virtual Host Manager to manage your virtual entities created with IBM LPAR technology.

This section contains the following topics:

How Virtual Host Manager Works with IBM LPARs

Virtual Host Manager monitors your virtual network entities seamlessly with your physical network entities. You get a full view of your network where you can troubleshoot networking issues for both types of entity. Although your virtual network entities behave like physical components, the process for monitoring those entities differs from the general CA Spectrum monitoring process. Understanding how this process works can help you locate and resolve networking issues related to your virtual network.

The *IBM LPAR Manager* in Virtual Host Manager is the CA SystemEDGE agent with the IBM LPAR AIM enabled. The IBM LPAR Managers are responsible for reporting on all of the configured IBM LPARs. Virtual Host Manager communicates with the IBM LPAR Managers to gather details about your IBM LPAR virtual environment. The following diagram shows how CA Spectrum gathers information about your IBM LPAR virtual environment using the IBM LPAR Manager:



As shown in the diagram, the process to gather information about your IBM LPAR virtual environment is as follows:

1. The HMC (see definition on page 268) communicates with each IBM LPAR Host that it manages.
2. The IBM LPAR Manager uses SSH to communicate with each of its managed HMCs to gather details about your virtual environment.

   Note: Monitor only one instance of the IBM LPAR Host with the IBM LPAR AIM. Do not manage a single IBM LPAR Host with multiple HMCs. Monitoring more than one instance can result in duplicate models in CA Spectrum.
3. Periodically, CA Spectrum communicates with the IBM LPAR Manager to retrieve these details. The IBM LPAR Manager has the CA SystemEDGE agent installed with the IBM LPAR AIM enabled. CA Spectrum uses SNMP to communicate with the CA SystemEDGE agent and uses the information to model and monitor your virtual environment in CA Spectrum.

More information:

How Virtual Host Manager Works (see page 11)
Viewing Your IBM LPAR Virtual Network (see page 197)
How the IBM LPAR Data is Updated in Virtual Host Manager (see page 199)

Models Created for IBM LPARs

Virtual Host Manager provides several models to represent the components of your IBM LPAR virtual technology network. Understanding the following basic models can help you better understand Discovery and how the virtual environment interfaces with your physical environment.

Virtual Host Manager includes the following models and icons for IBM LPAR devices:

IBM LPAR Manager

Represents a server that contains the CA SystemEDGE agent with the IBM LPAR AIM loaded.

Icon: 

IBM LPAR Host

Represents an IBM LPAR Host, as configured in the HMC (see definition on page 268). An *IBM LPAR Host* is a physical computer that uses IBM LPAR virtualization software to host IBM LPAR instances. IBM LPAR Hosts provide the CPU and memory resources that IBM LPARs use. They also give these IBM LPARs access to storage and network connectivity. These models serve as container models within the Universe topology, helping to group your virtual entities into a separate view while showing where the virtual environment interfaces with your physical network. The IBM LPAR Host cannot be contacted directly for status information. Instead, the status of these models is inferred from the status of its contained items.

Icon: 

IBM LPAR

Represents an IBM LPAR, as configured in the HMC. An *IBM LPAR* is a logical partition instance configured on the IBM LPAR Host that, like a physical computer, runs an operating system and applications. An IBM LPAR dynamically consumes resources on its physical host, depending on its workload and configuration.

Icon: 

More information:

Viewing Your IBM LPAR Virtual Environment (see page 197)

Discovering IBM LPAR Networks

This section describes the Discovery and modeling process for Virtual Host Manager. These tasks are typically performed by the Virtual Host Manager administrator.

How to Configure Discovery Options

After Virtual Host Manager is installed, you can configure Virtual Host Manager for IBM LPAR Discovery. Configuring your preferences helps ensure that Virtual Host Manager models your virtual devices correctly.

To configure your installation of Virtual Host Manager for IBM LPAR Discovery, select your preferences from the following options:

- Maintenance Mode for New IBM LPARs (see page 183)—Lets you decide which newly discovered IBM LPAR instances to place into maintenance mode until you are ready for CA Spectrum to manage them.
- Allow Device Model Deletes During IBM LPAR Discovery (see page 184)—Controls how CA Spectrum handles IBM LPAR virtualization technology models when Virtual Host Manager no longer manages them.
- Search for Existing Models (see page 185)—Determines which secure domains Virtual Host Manager searches during an IBM LPAR Discovery.
- Discover SNMP-Capable Devices (see page 187)—Controls how SNMP-capable devices are modeled during IBM LPAR Discovery. By default, new models are initially created as VHM models only. But, this option lets you override the default and immediately create SNMP models for devices that meet the necessary criteria.
- Retain SNMP-enabled LPARs During IBM LPAR Manager Deletion (see page 188)—Controls how CA Spectrum handles SNMP-enabled LPAR models when an IBM LPAR Manager model is deleted.

Configure Maintenance Mode for New IBM LPARs

Virtual Host Manager automatically models the IBM LPAR instances in your IBM LPAR virtual environment. CA Spectrum attempts to manage all models that are discovered. However, some new IBM LPARs are not ready for CA Spectrum management when they are initially modeled. For example, a non-running IBM LPAR causes CA Spectrum to generate a Contact Lost alarm. To prevent undesired alarms on new IBM LPAR models, you can decide which new models are immediately placed into maintenance mode. Later, you can manually disable maintenance mode when you are ready for CA Spectrum to manage these devices.

Follow these steps:

1. Open Virtual Host Manager in the Navigation panel (see page 115).

   A details page opens in the Contents panel for the selected Virtual Host Manager.
2. Click the Information tab.
3. Expand the Configuration, IBM LPAR, IBM LPAR Discovery subview.

4. Click Set in the 'Maintenance Mode for New IBM LPARs' field and select one of the following options:

   Place non-enabled LPARs in Maintenance Mode

   (Default) Applies maintenance mode to only non-enabled IBM LPAR models upon initial IBM LPAR Discovery.

   Place all LPARs in Maintenance Mode

   Applies maintenance mode to all new IBM LPAR models upon initial IBM LPAR Discovery.

   Your setting is saved and new IBM LPAR instances created by Virtual Host Manager are placed into maintenance mode per your selection.

More information:

How to Configure Discovery Options (see page 183)
Status Monitoring Options (see page 203)

Manage Device Models for Devices Deleted from IBM LPAR Manager

The devices and the relationships among them change frequently in virtual environments. Maintaining accurate and timely data about your virtual environment in CA Spectrum is challenging. For example, when an IBM LPAR Host or IBM LPAR instance is removed, CA Spectrum knows to remove the corresponding device models from Virtual Host Manager in the Navigation panel. However, should CA Spectrum keep or delete the model? You can select settings to control model deletion.

Important! When models are deleted, all notes or other customizations on those models are lost. You can disable this option if your models are likely to be recreated in your IBM LPAR environment later.

Follow these steps:

1. Open Virtual Host Manager in the Navigation panel (see page 115).

   The main details page opens in the Contents panel for the selected Virtual Host Manager.

2. Click the Information tab.

3. Expand the Configuration, IBM LPAR, IBM LPAR Discovery subview.

4. Click Set in the 'Allow Device Model Deletes During IBM LPAR Discovery' field and select one of the following options:

   Yes

   (Default) Deletes the Virtual Host Manager models that correspond to entities no longer managed by your IBM LPAR environment.

   No

   Places Virtual Host Manager models in the LostFound container if their corresponding entity is no longer managed by your IBM LPAR environment.

   Note: Models with more associations, such as a model that is included in a Global Collection, are handled differently. These models are removed from the Universe, but they are not moved to the LostFound container.

   Your setting is saved, and device models are handled accordingly after the device is deleted from your IBM LPAR environment.

More information:

How to Configure Discovery Options (see page 183)
Deleting Virtual Host Manager Models (see page 210)
Virtual Host Manager Alarms for IBM LPAR (see page 211)
Traps Supported in Virtual Host Manager (see page 213)
Manage SNMP-Enabled LPAR Models After IBM LPAR Manager Deletion (see page 188)

Configure Model Searches Across Secure Domains

Rather than creating new models, IBM LPAR Discovery attempts to locate models in the SpectroSERVER. In an environment with Secure Domain Manager deployed, IBM LPAR Discovery searches for models within the same secure domain as your IBM LPAR Manager. This domain is the "local" domain. However, some of your virtual environment devices can exist within a different secure domain. In this case, you can configure IBM LPAR Discovery to search all secure domains for existing models.

Follow these steps:

1. Open Virtual Host Manager in the Navigation panel (see page 49).

   The main details page opens in the Contents panel for the selected Virtual Host Manager.

2. Click the Information tab.

3. Expand the Configuration, IBM LPAR, IBM LPAR Discovery subview.

4. Click Set in the 'Search for Existing Models' field and select from the following options:

   In IBM LPAR Manager's Secure Domain

   (Default) Searches for existing models within the same secure domain as the IBM LPAR Manager server.

   In All Secure Domains

   Searches for existing models within all secure domains managed by the SpectroSERVER. Select this option only in the following situations:

   - All devices have unique IP addresses
   - When secure domains are used for security purposes or to isolate network traffic

   Note: Do not select this option for a NAT environment.

   Your setting is saved and IBM LPAR Discovery searches for existing models in CA Spectrum according to your selection. If duplicate models (that is, models that share the same IP address) exist in multiple secure domains, Virtual Host Manager does the following:

   - Selects the model in the local secure domain, if available.
   - If a duplicate model does not exist in the local domain, Virtual Host Manager randomly selects a model from another secure domain.
   - In both cases, Virtual Host Manager generates a minor alarm for the duplicate IP addresses on the IBM LPAR Manager model.

More information:

How to Configure Discovery Options (see page 183)

Configure SNMP Modeling Preferences

SNMP-capable devices support enriched device monitoring, such as process and file system monitoring capabilities. However, SNMP agents can be costly and time-consuming to deploy. By default, IBM LPAR Discovery creates IBM LPAR instances as VHM models (see definition on page 270). You can later upgrade them to SNMP models. However, you can also configure IBM LPAR Discovery to model all new SNMP-capable devices as SNMP models. Although IBM LPAR Discovery can take longer to complete, initially modeling these as SNMP models avoids manually upgrading these models later.

Important! Enable SNMP modeling *before* you model your IBM LPAR Hosts. If you model the IBM LPAR Hosts first, all child models are created as VHM models, which must be manually upgraded to SNMP models.

Follow these steps:

1. Open Virtual Host Manager in the Navigation panel (see page 49).

   The main details page opens in the Contents panel for the selected Virtual Host Manager.

2. Click the Information tab.

3. Expand the Configuration, IBM LPAR, IBM LPAR Discovery, SNMP Discovery subview.

   Important! Follow the steps in the subview to prepare your devices and CA Spectrum for SNMP Discovery. If devices are not properly prepared prior to IBM LPAR Discovery, Virtual Host Manager cannot create SNMP models.

4. Click Set in the 'Discover SNMP-Capable Devices' field and select from the following options:

   Yes

   Enables SNMP modeling during IBM LPAR Discovery. Only devices that meet the criteria specified in the SNMP Discovery subview text are modeled as SNMP devices. Applies to *new* models only.

   No

   (Default) Models all new devices found during IBM LPAR Discovery as VHM models. You can manually upgrade these models to SNMP models later.

   Your setting is saved and new devices are modeled in Virtual Host Manager according to your selection.

More information:

How vCenter Discovery Works (see page 43)
How to Discover and Model Your Virtual Environment (see page 189)
Adding SNMP Capabilities to VHM Models (see page 193)
Manage SNMP-Enabled LPAR Models After IBM LPAR Manager Deletion (see page 188)

Manage SNMP-Enabled LPAR Models After IBM LPAR Manager Deletion

By default, SNMP-enabled devices are deleted from CA Spectrum when the following items are deleted:

- IBM LPAR Manager model for the device
- IBM LPAR folder in the Navigation panel

SNMP-enabled device models can include significant customizations that you want to retain. You can adjust your settings to avoid deleting these models. They are placed into the LostFound container for later use.

Follow these steps:

1. Open Virtual Host Manager in the Navigation panel (see page 49).

   The main details page opens in the Contents panel for the selected Virtual Host Manager.

2. Click the Information tab.
3. Expand the Configuration, IBM LPAR, IBM LPAR Discovery subview.
4. Click Set in the 'Retain SNMP-enabled LPARs During IBM LPAR Manager Deletion' field and select one of the following options:

   Yes

   Retains SNMP-enabled LPAR models in the LostFound container when their IBM LPAR Manager or the IBM LPAR folder is deleted.

   Note: Models with more associations, such as a model that is included in a Global Collection, are handled differently. These models are removed from the Universe, but they are not moved to the LostFound container.

   No

   (Default) Deletes all LPAR models when their IBM LPAR Manager or the IBM LPAR folder is deleted.

   Your setting is saved, and SNMP-enabled device models are handled accordingly when IBM LPAR Manager models or the IBM LPAR folder is deleted.

More information:

How to Configure Discovery Options (see page 183)
Manage Device Models for Devices Deleted from IBM LPAR Manager (see page 184)
Deleting Virtual Host Manager Models (see page 210)

How to Discover and Model Your Virtual Environment

To monitor your virtual environment, you must discover and model your virtual entities—IBM LPAR Hosts and IBM LPAR instances. Modeling these entities in Virtual Host Manager lets you view your complete network topology in one tool, showing the relationships between your physical and virtual components.

The main steps for modeling your virtual environment are as follows:

1. Run a standard CA Spectrum Discovery (see page 190).

   The purpose of this Discovery is to help ensure the upstream routers and switches are modeled before IBM LPAR Discovery runs. Optionally, if the SNMP Modeling option is disabled, this step can also model the SNMP-capable IBM LPAR Managers. When modeling these entities, be sure that your modeling options are set correctly to support Virtual Host Manager.

2. Upgrade the CA SystemEDGE model (see page 191).

   This step is required only when your CA SystemEDGE agent on the IBM LPAR Manager host was modeled in a release before CA Spectrum Release 9.2.1.

3. Let IBM LPAR Discovery run (see page 192).

   When you model the CA SystemEDGE agent with IBM LPAR AIM on the IBM LPAR Manager host, IBM LPAR Discovery begins automatically. Each of these IBM LPAR Manager models has its own IBM LPAR Discovery process. The purpose of IBM LPAR Discovery is to find the virtual entities in your IBM LPAR environment, model the ones that do not exist, and place them in the Virtual Host Manager view of the Navigation panel.

More information:

Adding SNMP Capabilities to VHM Models (see page 193)
Move IBM LPAR to a Different Host (see page 196)
How to Configure Management Options (see page 204)
Configure SNMP Modeling Preferences (see page 187)

Run CA Spectrum Discovery

To discover your IBM LPAR environment, run the standard CA Spectrum Discovery. This Discovery ensures that the upstream routers and switches are modeled so that later connections from the virtual entities can be established. You can also model the SNMP-capable IBM LPAR Hosts and IBM LPAR instances during CA Spectrum Discovery.

Note: Modeling SNMP-capable IBM LPAR Hosts and IBM LPAR instances is necessary during CA Spectrum Discovery only when the SNMP Modeling option is disabled during IBM LPAR Discovery.

Note: Only an administrator performs this task.

Follow these steps:

1. Open the Discovery console.

   Note: Before modeling, be sure that you know the correct community strings, IP addresses, and port numbers for any SNMP agents that run on a nonstandard port.

2. Click the  (Creates a new configuration) button in the Navigation panel.

3. Configure your options to support virtual network modeling, as follows:

   a. Click the Modeling Options button in the Modeling Options group.

      The Modeling Configuration dialog opens.

   b. Click the Protocol Options button.

      The Protocol Options dialog opens.

   c. Select the ARP Tables for Pingables option, and click OK.

      The Modeling Configuration dialog opens.

   d. (Optional) Click the Advanced Options button in the Advanced Options group, add your nonstandard SNMP ports (such as, the CA SystemEDGE agent port), and click OK.

4. Enter individual IP addresses or the beginning and ending IP addresses in the IP Boundary List fields and click Add.

   Note: Be sure that the range of IP addresses includes all servers with CA SystemEDGE and the IBM LPAR AIM installed and the interconnecting switches and routers. Or you can include the SNMP-capable IBM LPAR Hosts and IBM LPAR instances that require SNMP models.

5. Enter any additional values in the Discovery console, and click the Discover button.

   The following models are created and are added to your network topology in CA Spectrum:

   - IBM LPAR Managers and the switches and routers that connect them to your network—Information about your virtual environment comes from the IBM LPAR Manager. When these IBM LPAR Manager models exist in CA Spectrum, IBM LPAR Discovery can begin.
   - IBM LPAR instances—If you decide not to model these entities with CA Spectrum Discovery, IBM LPAR Discovery creates them as VHM models (see definition on page 270).

   Note: You can also manually model your virtual network by IP address. In this case, we recommend modeling the upstream devices first. Modeling in the correct order ensures that the relationships among these entities are built correctly in the topology. For more information about how to perform a Discovery, see the *Modeling and Managing Your IT Infrastructure Administrator Guide*.

More information:

Adding SNMP Capabilities to VHM Models (see page 193)
Move IBM LPAR to a Different Host (see page 196)
How to Configure Management Options (see page 204)
Configure SNMP Modeling Preferences (see page 187)

Upgrade the CA SystemEDGE Model

The CA SystemEDGE agent could have been modeled in CA Spectrum before installing Virtual Host Manager or before the IBM LPAR AIM was loaded on the agent. In this case, the existing CA SystemEDGE model is not compatible with Virtual Host Manager. Upgrade the model so Virtual Host Manager can access the IBM LPAR AIM capabilities in CA SystemEDGE. *This procedure is not required if the CA SystemEDGE agent with IBM LPAR AIM is loaded and is modeled after installing CA Spectrum.*

To upgrade the CA SystemEDGE model, right-click the model and select Reconfiguration, Reconfigure Model.

The CA SystemEDGE model is upgraded to support the IBM LPAR AIM.

Note: You can also send a reconfigure model action to CA SystemEDGE using the CLI. For more information, see the *Modeling and Managing Your IT Infrastructure Administrator Guide*.

More information:

Adding SNMP Capabilities to VHM Models (see page 193)
Move IBM LPAR to a Different Host (see page 196)
How to Configure Management Options (see page 204)

How IBM LPAR Discovery Works

IBM LPAR Discovery is a specialized discovery process that gathers detailed information about your virtual environment. The purpose of IBM LPAR Discovery is to obtain the virtual entities managed by the HMC (see definition on page 268), model the ones that do not exist in CA Spectrum, and place them under Virtual Host Manager in the Navigation panel.

A key benefit of IBM LPAR Discovery is that it runs automatically in the background, keeping your virtual environment data updated in CA Spectrum. Understanding how IBM LPAR Discovery works reinforces the importance of properly installing and modeling the various components of Virtual Host Manager.

The IBM LPAR Discovery process works as follows:

1. Immediately after the IBM LPAR Manager is configured (the CA SystemEDGE agent is installed with the IBM LPAR AIM enabled), the IBM LPAR Manager uses SSH to contact each HMC that it monitors. The IBM LPAR Manager gathers and stores information from the HMC about your virtual environment.

   Note: Monitor only one instance of the IBM LPAR Host with the IBM LPAR AIM. Do not manage a single IBM LPAR Host with multiple HMCs. Monitoring more than one instance can result in duplicate models in CA Spectrum.

   Important! The CA SystemEDGE agent and IBM LPAR AIM must be installed so that CA SystemEDGE, the HMCs, and CA Spectrum can communicate. If they cannot, IBM LPAR Discovery cannot run.

2. During CA Spectrum Discovery, CA Spectrum creates a model for each IBM LPAR Manager in Step 1 and enables CA Spectrum to handle communication between CA Spectrum and the CA SystemEDGE agent.

3. CA Spectrum polls the IBM LPAR AIM to gather the IBM LPAR Manager information that is stored in Step 1.

4. CA Spectrum begins IBM LPAR Discovery and uses this information from the AIM to update modeling in the CA Spectrum Topology tab and the Virtual Host Manager hierarchy in the Navigation panel, as follows:

   a. If you enable SNMP Discovery before Step 2, Virtual Host Manager Discovery creates SNMP models for all new SNMP-capable models that meet the SNMP Discovery criteria.

      Note: By default, SNMP Discovery is disabled during IBM LPAR Discovery.

   b. VHM models (see definition on page 270) are created for the remaining non-SNMP IBM LPAR Hosts and IBM LPAR instances, as follows:

      - Previously existing IBM LPAR models are changed to VHM models.
      - VHM models are created for the IBM LPAR instances that *do not* previously exist in CA Spectrum.
      - VHM models are created for the IBM LPAR Host models, and these models group their associated IBM LPAR instance models in the Navigation panel, under Virtual Host Manager and the Universe topology.

   c. All models for your virtual network are added to the Virtual Host Manager portion of the Navigation panel.

   Note: In a virtual environment, devices on separate IBM LPAR Hosts can have the same IP address or MAC address. In this case, CA Spectrum creates duplicate models for each occurrence of an IP address or MAC address.

5. IBM LPAR Discovery automatically repeats this process at each regularly scheduled IBM LPAR technology polling interval.

   Note: By default, the IBM LPAR polling interval is controlled by setting the polling interval on the IBM LPAR Manager model. Or you can control IBM LPAR polling independently using the IBM LPAR virtualization technology application model.

More information:

Adding SNMP Capabilities to VHM Models (see page 193)
Move IBM LPAR to a Different Host (see page 196)
How to Configure Management Options (see page 204)
Controlling IBM LPAR AIM Polling (see page 208)
Configure Model Searches Across Secure Domains (see page 185)

Adding SNMP Capabilities to VHM Models

SNMP-capable devices support enriched device monitoring, such as process and file system monitoring capabilities. However, SNMP agents can be costly and time-consuming to deploy. When an SNMP agent is not available or SNMP Discovery is disabled, Virtual Host Manager creates IBM LPARs as VHM models (see definition on page 270).

Later, you can install an SNMP agent on any IBM LPAR Host or IBM LPAR and upgrade its modeling in CA Spectrum. Options for upgrading to SNMP models are as follows:

- **Upgrade only selected devices**—This method works quickly when you have a small selection of models to upgrade. The VHM models are deleted first. One drawback of this method is that after CA Spectrum deletes the models, you must wait for the next IBM LPAR Discovery to create the SNMP models and place them in Virtual Host Manager. Knowledge of the IP addresses for the models to upgrade is required.
- **Upgrade all SNMP-capable VHM models**—This method upgrades models in batch. It is preferred when upgrading Virtual Host Manager to a new release. Knowledge of the IP addresses of individual models is not required. Another advantage is that after CA Spectrum deletes the VHM models, the upgraded SNMP models are immediately placed in the Virtual Host Manager hierarchy without waiting for the next polling cycle. Therefore, Virtual Host Manager manages the models more quickly. The drawback to this method is that it can take a long time to complete. The time required to complete this upgrade depends on how many community strings and SNMP ports Virtual Host Manager must search when locating SNMP-capable devices.

  Note: Virtual Host Manager attempts to identify SNMP agents on powered-up pingable devices only.

Important! When models are deleted, all notes or other customizations on those models are lost.

More information:

How to Discover and Model Your Virtual Environment (see page 189)
Deleting Virtual Host Manager Models (see page 210)
Configure SNMP Modeling Preferences (see page 187)

Upgrade Selected VHM Models to SNMP Models

When an SNMP agent is not available or SNMP Discovery is disabled during IBM LPAR Discovery, Virtual Host Manager creates IBM LPAR instances as VHM models (see definition on page 270). Later, you can install an SNMP agent on these devices and upgrade their modeling in CA Spectrum. You must know the IP addresses for the device models to upgrade. Manually selecting models to upgrade works quickly, but all notes or customizations on these models are lost during the upgrade.

Follow these steps:

1. Deploy or enable an SNMP agent on the device, if required.
2. Model the device again using one of the following methods:
   - CA Spectrum Discovery
   - Model individual devices by IP address

When the new SNMP-capable model is created, CA Spectrum removes the previous model from Virtual Host Manager and deletes it. At the next IBM LPAR AIM polling cycle, CA Spectrum adds the SNMP-capable model to Virtual Host Manager in the Navigation panel.

Important! When models are deleted, all notes or other customizations on those models are lost.

More information:

Manage Device Models for Devices Deleted from IBM LPAR Manager (see page 184)
How to Discover and Model Your Virtual Environment (see page 189)
Deleting Virtual Host Manager Models (see page 210)

Upgrade All VHM Models to SNMP Models

When an SNMP agent is not available or SNMP Discovery is disabled during IBM LPAR Discovery, Virtual Host Manager creates IBM LPAR instances as VHM models (see definition on page 270). Later, you can install an SNMP agent on any IBM LPAR and upgrade its modeling in CA Spectrum. When upgrading in batch, CA Spectrum searches your VHM models and locates models that are now SNMP-capable devices. Then, CA Spectrum converts these to SNMP models. This method can take a long time to complete, depending on how many community strings and ports Virtual Host Manager must search.

Follow these steps:

1. Deploy or enable an SNMP agent on your devices, as required.
2. Open Virtual Host Manager in the Navigation panel (see page 49).

   The main details page opens in the Contents panel for the selected Virtual Host Manager.
3. Select the IBM LPAR Manager model in the Navigation panel that manages the models you want to upgrade.
4. Click the Information tab.
5. Expand the IBM LPAR Manager, CA Spectrum Modeling Control subview.
6. Click the Upgrade ICMP-Only Devices button.

   Important! When models are deleted, all notes or other customizations on those models are lost.

   Virtual Host Manager searches for VHM models managed by the IBM LPAR AIM on the selected IBM LPAR Manager device. Virtual Host Manager upgrades the ICMP-only devices that meet the criteria for SNMP devices and places them within the Virtual Host Manager hierarchy.

Move IBM LPAR to a Different Host

Moving an IBM LPAR from one IBM LPAR Host to another can potentially result in lost data, depending on your configuration settings in Virtual Host Manager and the HMC (see definition on page 268). The IBM LPAR AIM does not support IBM LPAR migration. To Virtual Host Manager, a move is treated as two events—an IBM LPAR is deleted in the HMC and a new IBM LPAR is created. Based on your Virtual Host Manager configuration, CA Spectrum can delete the original IBM LPAR model and create a new one. If you customized the original model, deleting it can result in lost data. You can avoid this data loss when you configure your Virtual Host Manager settings correctly before moving the IBM LPAR in the HMC.

Follow these steps:

1. Change the 'Allow Device Model Deletes During IBM LPAR Discovery' option to No (see page 184).

   Note: With this option disabled, CA Spectrum does not delete the IBM LPAR model from CA Spectrum, even though the model is removed from Virtual Host Manager management.

2. Using the HMC, remove the IBM LPAR from the original IBM LPAR Host.

3. Wait for Virtual Host Manager in the Navigation panel to reflect the changes.

   CA Spectrum places the IBM LPAR model into the LostFound container.

   Important! For Virtual Host Manager to reconcile the new IBM LPAR with the existing model in the LostFound container, the IBM LPAR name, MAC address, *and* IP address must remain the same after migrating the IBM LPAR in the HMC. If any of these values change, Virtual Host Manager cannot use the existing model.

4. Using the HMC, add the IBM LPAR to the other IBM LPAR Host.

   When IBM LPAR Discovery finds the new IBM LPAR, Virtual Host Manager reconciles it with the existing model, removes it from the LostFound container, and places that model into Virtual Host Manager management.

5. (Optional) Change the 'Allow Device Model Deletes During IBM LPAR Discovery' option back to Yes on the originating IBM LPAR Manager model.

   The IBM LPAR is moved from one IBM LPAR Host to another.

More information:

How to Discover and Model Your Virtual Environment (see page 189)
Run CA Spectrum Discovery (see page 190)
Upgrade the CA SystemEDGE Model (see page 191)
How IBM LPAR Discovery Works (see page 192)
How the IBM LPAR Data is Updated in Virtual Host Manager (see page 199)

Viewing Your IBM LPAR Virtual Environment

This section describes concepts for viewing your IBM LPAR virtual environment and the associated alarms. The basic steps are no different from the standard CA Spectrum procedures. However, this section describes conceptual differences and details that only apply to the IBM LPAR virtual technology.

Viewing Your IBM LPAR Virtual Network

On the Explorer tab, the Virtual Host Manager node displays a hierarchical tree structure that helps you visualize the logical relationships among your virtual environment resources.

Using this information, you can see how resources are shared among your IBM LPAR Managers, which can help you identify opportunities to reorganize and optimize your virtual environment. This hierarchy also provides a quick way to monitor the performance of your resources and troubleshoot their alarms.

Because Virtual Host Manager is not aware of a DSS environment (see definition on page 268), it is located within a landscape hierarchy. The following example shows where Virtual Host Manager appears on the Explorer tab in the Navigation panel and illustrates the virtual environment hierarchy:

```
[-] SpectroSERVER host
    [+] Universe
    [-] Virtual Host Manager
        [-] IBM LPAR
            [+] IBM LPAR Manager 1
            [-] IBM LPAR Manager 2
                [-] IBM LPAR Host 1
                      .  IBM LPAR 1
                      .  IBM LPAR 2
                [+] IBM LPAR Host 2
                [+] IBM LPAR Host 3
```

Virtual Host Manager is the root node for the entire virtual environment managed by this SpectroSERVER. Selecting this node in the Navigation panel displays Virtual Host Manager details in the Contents panel. You can view details such as events and alarms that are related to your virtual environment.

Directly under Virtual Host Manager, virtual environments are organized within folders that represent the associated technology. In the example hierarchy above, the IBM LPAR folder contains the portion of the virtual environment that was created using IBM LPAR virtualization technology. In this folder, Virtual Host Manager lists all IBM LPAR Manager hosts that are managed by this SpectroSERVER.

Each IBM LPAR Manager contains only the portion of the entire virtual environment that it manages. Selecting an IBM LPAR Manager in the Navigation panel displays details in the Contents panel, such as the IBM LPAR Hosts or IBM LPAR instances that are managed by the selected IBM LPAR Manager. You can also view general statistics and view details about other components that are not modeled in CA Spectrum, such as the following:

- System profiles
- Profiles
- Slots
- Virtual Ethernet devices
- Virtual SCSI devices
- Virtual serial devices
- Physical disks

Under each IBM LPAR Manager, the hierarchy represents the logical relationships between the following entities:

- **IBM LPAR Hosts**

  An IBM LPAR Host contains the IBM LPAR instances that it manages. Selecting an IBM LPAR Host in the Navigation panel displays details in the Contents panel, such as events and alarms that are related to the IBM LPAR Host and CPU usage.

- **IBM LPAR instances**

  An IBM LPAR instance is always a leaf node on the Virtual Host Manager hierarchy tree. Selecting an IBM LPAR in the Navigation panel displays details in the Contents panel, including events and alarms, memory usage, and status.

More information:

How Virtual Host Manager Works with IBM LPARs (see page 179)
Models Created for IBM LPARs (see page 181)
Run CA Spectrum Discovery (see page 190)
Custom Subviews for Virtual Entity Types (see page 201)
Locater Tab for IBM LPAR Searches (see page 202)

Understanding the IBM LPAR Virtual Topology

The IBM LPAR Manager, IBM LPAR Host, and IBM LPAR instance models created for your virtual environment are integrated into the topology view. IBM LPAR Host models automatically group their associated IBM LPAR instances. The topology shows how these IBM LPARs are connected to your physical network entities.

The following example shows how these models can appear on the Explorer tab in the Navigation panel under the Universe group:

```
[-] Universe
     .  Physical switch 1
     .  Physical switch 2
     .  IBM LPAR Manager
    [-] IBM LPAR Host
          .  Fanout A
          .  Fanout B
          .  IBM LPAR A
          .  IBM LPAR B
          .  IBM LPAR C
```

Selecting one of these models displays these relationships graphically on the Topology tab in the Contents panel.

More information:

Models Created for IBM LPARs (see page 181)
How the IBM LPAR Data is Updated in Virtual Host Manager (see page 199)
Locater Tab for IBM LPAR Searches (see page 202)

How the IBM LPAR Data is Updated in Virtual Host Manager

During your initial IBM LPAR Discovery, CA Spectrum populates Virtual Host Manager hierarchy in the Navigation panel with your virtual device models. After CA Spectrum builds this initial hierarchy, your virtual network configuration can change, and Virtual Host Manager must continually work to keep this information accurate in CA Spectrum. For example, the following events can change your virtual network configuration:

- Creating or deleting an IBM LPAR on an IBM LPAR Host
- Moving an IBM LPAR from one IBM LPAR Host to another

To keep your information accurate, Virtual Host Manager detects these changes by polling the IBM LPAR AIM. Therefore, your virtual network configuration is updated in CA Spectrum at each polling cycle. CA Spectrum also receives traps from the AIM and generates the corresponding events. By reviewing the event log, you can find out when configuration changes occur, such as when a new IBM LPAR is created.

When an IBM LPAR is deleted, CA Spectrum removes the models from the Virtual Host Manager hierarchy in the Navigation panel. When the AIM detects an addition to your virtual network configuration, such as provisioning a new IBM LPAR or placing one into management, CA Spectrum performs the following tasks:

- Updates the placement of your virtual device models in the Virtual Host Manager hierarchy of the Navigation panel
- *Automatically* rediscovers connections to the affected IBM LPAR models and associates them with the correct IBM LPAR Host in the Universe topology.

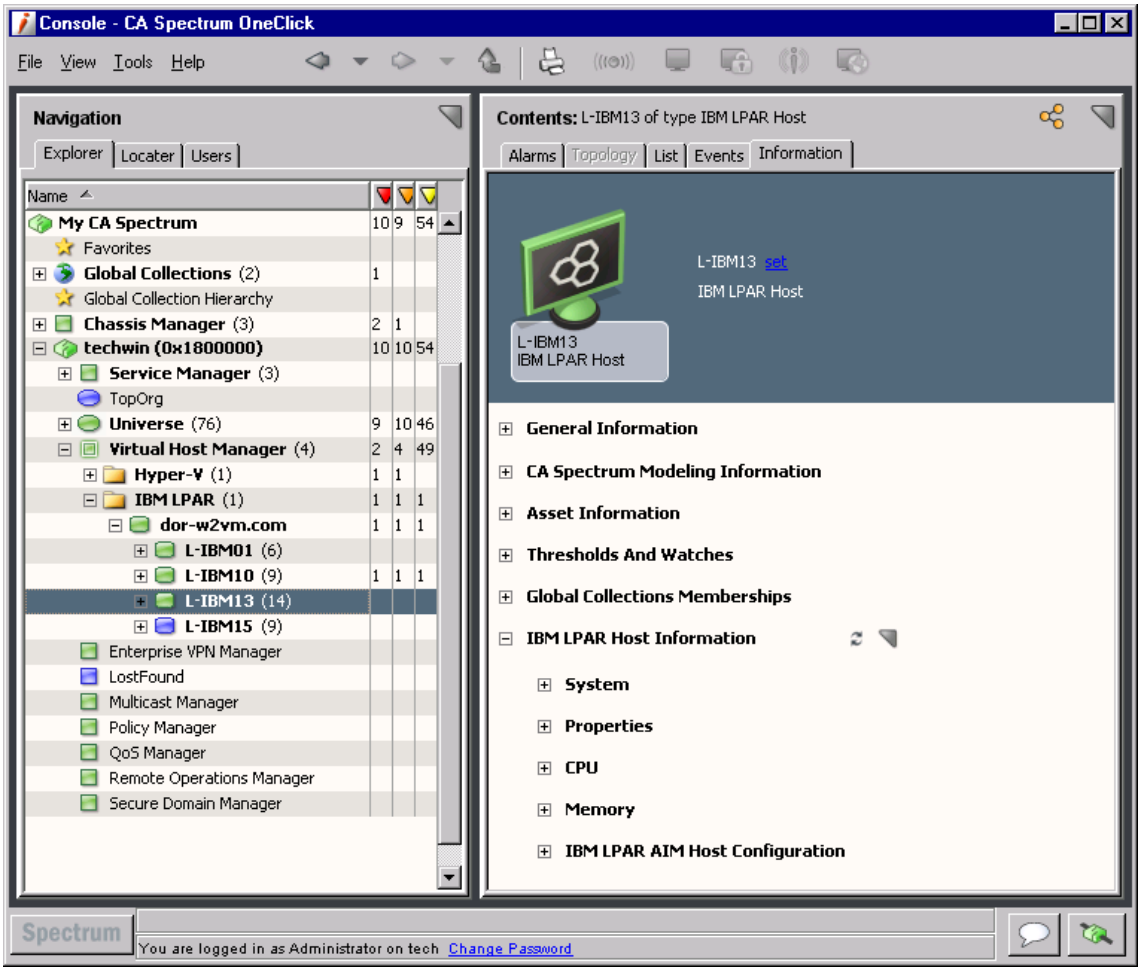
  Important! To reestablish connections to your virtual models correctly, all interconnecting routers and switches in your physical network must be modeled. If these models do not exist before connections to your virtual devices are rediscovered, CA Spectrum cannot resolve those connections and display the information correctly in the Universe topology view. The IBM LPAR Hosts are placed in the same LAN container as the CA SystemEDGE model.

More information:

How Virtual Host Manager Works (see page 11)
Models Created for IBM LPARs (see page 181)
Manage Device Models for Devices Deleted from IBM LPAR Manager (see page 184)
Move IBM LPAR to a Different Host (see page 196)
Viewing Your IBM LPAR Virtual Network (see page 197)
Configure and Monitor Resource Status (see page 207)

Custom Subviews for Virtual Entity Types

Your Virtual Host Manager models collectively provide information about your virtual environment. Individually, each model provides unique information or configuration settings, depending on the virtual entity type it represents. This custom subview appears on the Information tab in the Contents panel. These subviews can contain real-time data, such as CPU status or memory utilization, and provide access to threshold settings. For example, the custom subview for IBM LPAR Host is the "IBM LPAR Host Information" subview, as shown:



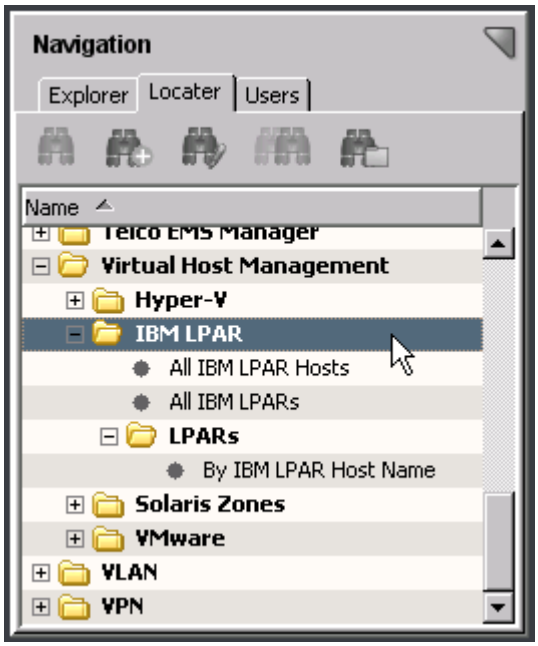
Note: The IBM LPAR Manager model provides combined information for all virtual devices managed by the IBM LPAR Manager. That is, selecting the IBM LPAR Manager model in the Navigation panel displays information about the selected IBM LPAR Manager host *and* combined information about all IBM LPAR Hosts, IBM LPAR instances, system profiles, virtual Ethernet devices, and more. This information contains the same data displayed on the Information tab for each individual entity model. The combined view in the IBM LPAR Manager model can provide a good overview about all of the virtual entities it manages.

More information:

Viewing Your IBM LPAR Virtual Network (see page 197)
Configure and Monitor Resource Status (see page 207)

Locater Tab for IBM LPAR Searches

In addition to viewing details about your virtual environment on the Explorer tab, you can also use the Locater tab to run preconfigured Virtual Host Manager searches. The search options are grouped under the Virtual Host Management, IBM LPAR folder on the Locater tab, as shown:



These detailed searches can help you investigate information related to virtual entities only, such as locating all IBM LPAR instances within a landscape.

Note: Although Virtual Host Manager is not DSS (see definition on page 268) aware, these preconfigured searches let you select multiple landscapes to search in the search parameters.

The Locater tab in the Navigation panel includes the following searches for Virtual Host Manager information:

All IBM LPAR Hosts

Locates all IBM LPAR Hosts that have been modeled in the CA Spectrum database for your virtual network.

All IBM LPARs

Locates all IBM LPAR instances that have been modeled in the CA Spectrum database for your virtual network.

LPARs, By IBM LPAR Host Name

Locates all IBM LPAR instances that have been modeled in the CA Spectrum database for your virtual network, limited to only those IBM LPARs managed by a selected IBM LPAR Host.

More information:

Viewing Your IBM LPAR Virtual Network (see page 197)

Status Monitoring Options

CA Spectrum provides a wide range of options for monitoring the state of your virtual network resources. The status information available for a resource varies, depending on the type of virtual entity you are monitoring. Also, your ability to configure a status option depends on its type. For example, some status options are read-only, but others let you configure threshold values, enable behaviors, or select an alarm severity. Providing this range of options and levels of customization, CA Spectrum lets you decide how to best monitor the performance of your virtual network.

Status fields are located in the OneClick subviews. All status information for a given virtual environment is available on the IBM LPAR Manager model in a tabular format. Also, each virtual entity type that has a unique model in CA Spectrum provides a subset of the same status information for easy viewing. Status-related settings, including the alert type, monitor, and thresholds, can be set from either view location.

The following tables outline the type of status information available for each virtual entity type. The Subview Locations column describes where the corresponding status fields are located in OneClick. For example, "memory" information for your IBM LPAR models is available on the Information tab in the following two locations:

- IBM LPAR Information, Memory subview for the IBM LPAR model
- IBM LPAR Manager, Managed Environment, LPARs subview for the IBM LPAR Manager model

To explore the exact status options available for each status information type, locate the subview in OneClick.

IBM LPAR Host

Status Information Type	Subview Locations
Overall	IBM LPAR Host, IBM LPAR Manager
CPU	IBM LPAR Host, IBM LPAR Manager

IBM LPAR

Status Information Type	Subview Locations
System	IBM LPAR, IBM LPAR Manager
CPU	IBM LPAR, IBM LPAR Manager
Memory	IBM LPAR, IBM LPAR Manager

More information:

Configure and Monitor Resource Status (see page 207)
Virtual Host Manager Alarms for IBM LPAR (see page 211)
Traps Supported in Virtual Host Manager (see page 213)

How to Configure Management Options

After your virtual network is modeled, you can configure Virtual Host Manager options for viewing and managing your device models. Configuring your preferences helps ensure that Virtual Host Manager handles your virtual device models correctly and monitors only the information that is important to you.

To configure your installation of Virtual Host Manager, perform the following procedures after you discover and model your virtual network:

- Configure the IBM LPAR AIM options (see page 205)—These options let you select settings for the CA SystemEDGE IBM LPAR AIM, such as the AIM polling interval and various traps.
- Configure threshold values and other status monitoring options (see page 207)—These options let you determine which information you want to monitor and how CA Spectrum manages the various events that occur in your virtual environment.

Configure the IBM LPAR AIM

The IBM LPAR AIM communicates with the IBM LPAR Manager to manage and collect information about your virtual environment. In Virtual Host Manager, you can configure the AIM to determine how it handles polling, traps, and events. The IBM LPAR AIM configuration settings let you determine the right balance of information to gather against the amount of required resources.

Follow these steps:

1. Open Virtual Host Manager in the Navigation panel (see page 115).

   The main details page opens in the Contents panel for the selected Virtual Host Manager.

2. Locate and click your IBM LPAR Manager on the Explorer tab in the Navigation panel.

   The tabs in the Contents panel are populated with details about your IBM LPAR Manager.

3. Click the Information tab.

4. Expand the IBM LPAR Manager, IBM LPAR AIM, Configuration subview.

5. Click set to change the settings for the following fields, as needed:

   Polling Interval (Seconds)

   Specifies the time interval (in seconds) when the IBM LPAR AIM polls and caches status and modeling information from the configured IBM LPAR Hosts. This polling retrieves status and modeling updates, such as an IBM LPAR not-running status, IBM LPAR Host disconnected, new IBM LPAR available, new IBM LPAR Host, and more.

   Default: 300

   Limits: Values greater than or equal to 300.

   Note: For best results, we recommend setting this interval lower than the CA Spectrum poll cycle interval.

   Log Level

   Specifies the level of information written to the IBM LPAR AIM log file. The levels are cumulative (for example, log level 4 writes all messages at levels 0 through 4). The log levels are as follows:

   - 0: Fatal
   - 1: Critical
   - 2: Warning
   - 3: Info
   - 4: Debug

- 5: Debug Low
- 6: Debug Lower
- 7: Debug Lowest

Default: 2

Note: Specifying a debug level greater than 4 is discouraged.

Events Max

Specifies the maximum number of events to store in the Events table. When the maximum rows are reached, CA Spectrum begins overwriting event rows, beginning with the oldest recorded events.

Default: 500

Limits: 1–2147483647

History (days)

Specifies the amount of history information that is available in the Events table, in days. Events older than the specified number of days are purged from the Events table.

Note: The value in the Events Max field also affects this setting. When the max is reached, the Events table cannot always store events that span the number of days that you specify in the History (days) field. For example, 800 events occur in the past 30 days. The most recent 500 events occurred within the past 10 days. If the Events Max field specifies 500, only 10 days of history are available in the Events table.

Default: 30

Limits: 1–365

Clear Events

Determines whether to clear events from the Events table. Select from the following options:

do-not-clear

(Default) Retains all events in the Event table until the Events Max or History (days) values are reached.

clear

Clears all events from the Event table when you start the IBM LPAR AIM.

Your IBM LPAR AIM is configured with your selections.

More information:

How to Configure Management Options (see page 204)

Configure and Monitor Resource Status

Yu can monitor the status of virtual resources in OneClick. For example, you can view the total memory, used memory, percent of CPU usage, and more. Also, you can set monitoring options, such as enabling alerts and setting threshold values for traps. This information can help you optimize your virtual network performance and troubleshoot alarms.

Note: Traps are set on and managed by the IBM LPAR AIM, but you can configure these threshold values from the OneClick subviews. A read/write community string is required to change any threshold values or settings.

You can view or configure resource status options and information for virtual devices on the Information tab.

Follow these steps:

1. Open Virtual Host Manager in the Navigation panel (see page 115).

   The main details page opens in the Contents panel for the selected Virtual Host Manager.

2. Locate and click the virtual device on the Explorer tab in the Navigation panel.

   The device details display in the Contents panel.

3. Click the Information tab.

   Multiple subviews are available for viewing. Generally, the subview at the bottom of the tab includes the resource allocation and utilization information for the selected model. For example, an IBM LPAR Host model displays a subview named "IBM LPAR Host Information" that includes details for the specific model you selected in the Navigation panel.

4. Expand the appropriate subview.

   All available resource status details and monitoring options for the selected device model are displayed.

   Note: The IBM LPAR Manager model provides combined information for all virtual devices managed by the IBM LPAR Manager. That is, selecting the IBM LPAR Manager model in the Navigation panel displays information about the selected IBM LPAR Manager host *and* combined information about all IBM LPAR Hosts, IBM LPAR instances, system profiles, virtual Ethernet devices, and more. This information contains the same data displayed on the Information tab for each individual entity model. The combined view in the IBM LPAR Manager model can provide a good overview about all of the virtual entities it manages.

More information:

Custom Subviews for Virtual Entity Types (see page 201)
Status Monitoring Options (see page 203)
How to Configure Management Options (see page 204)
Virtual Host Manager Alarms for IBM LPAR (see page 211)

Controlling IBM LPAR AIM Polling

When tuning Virtual Host Manager performance, you can change the IBM LPAR Manager polling rate or disable IBM LPAR technology polling. By default, the polling attributes on the IBM LPAR Manager model control the IBM LPAR-related polling behavior. Or you can change this IBM LPAR-related polling behavior independently. The IBM LPAR virtual technology application model, IBMLPARAIMApp, controls your IBM LPAR-related polling.

The following two attribute values on the application specifically control the IBM LPAR technology polling logic:

- PollingStatus
- Polling_Interval

Both the IBM LPAR Manager device model and the IBMLPARAIMApp application model contain these attributes. PollingStatus disables and enables polling, while Polling_Interval controls the polling frequency. If the values are different, the IBMLPARAIMApp application model attribute values take precedence.

This ability to set the value for the device model and application model lets you fine-tune your IBM LPAR-related polling. For both PollingStatus and Polling_Interval, modifying the attribute on the IBM LPAR Manager device model also changes the corresponding application model attribute if their values are the same.

More information:

How IBM LPAR Discovery Works (see page 192)

Configure the IBM LPAR Polling Interval

You can change the IBM LPAR AIM polling rate. Configure the polling interval by setting the Polling_Interval attribute on the IBM LPAR virtual technology application model.

Follow these steps:

1. Open OneClick and click the Locater tab in the Navigation panel.
2. Expand the Application Models folder and double-click 'By Device IP Address.'

   A search dialog opens.
3. Enter the IP address for your IBM LPAR Manager in the Device IP Address field and click OK.

   A list of application models for the IBM LPAR Manager appears in the Contents panel.
4. Select the IBMLPARAIMApp application model.

   The application model details appear in the Component Details panel.
5. Click the Information tab in the Component Details panel.
6. Click the Modeling Information subview.
7. Click set in the Poll Interval (sec) field, enter a new value.

   Note: Changing the Poll Interval (sec) value from any number to 0 also sets the Polling field to Off, disabling IBM LPAR AIM polling. However, if you set the Poll Interval (sec) to 0 and set the Polling field to On, IBM LPAR AIM polling continues, using the polling interval set for the IBM LPAR Manager device.

   The IBM LPAR AIM polling interval setting is configured.

Disable IBM LPAR Polling

You can disable IBM LPAR AIM polling. Disabling IBM LPAR polling is the same as disabling Virtual Host Manager. Disable polling by setting the PollingStatus attribute on the IBM LPAR virtual technology application model.

Follow these steps:

1. Open OneClick and click the Locater tab in the Navigation panel.
2. Expand the Application Models folder and double-click 'By Device IP Address.'

   A search dialog opens.
3. Enter the IP address for your IBM LPAR Manager in the Device IP Address field and click OK.

   A list of application models for the IBM LPAR Manager appears in the Contents panel.

4. Select the IBMLPARAIMApp application model.

   The application model details appear in the Component Details panel.

5. Click the Information tab in the Component Details panel.

6. Click the CA Spectrum Modeling Information subview.

7. Click set in the Polling field and select Off.

   Polling is disabled for the IBM LPAR AIM on the selected IBM LPAR Manager.

Deleting Virtual Host Manager Models

Models can be deleted from OneClick at any time for various reasons. However, Virtual Host Manager restricts your ability to delete models from the Virtual Host Manager hierarchy in the Navigation panel. To delete models manually, you have the following two options:

- Delete the IBM LPAR folder or an IBM LPAR Manager model in Virtual Host Manager
- Remove a virtual entity using the HMC (see definition on page 268)

In Virtual Host Manager, models are sometimes deleted automatically. The following circumstances cause CA Spectrum to automatically delete Virtual Host Manager models:

- **IBM LPAR folder deleted or IBM LPAR Manager model removed from Virtual Host Manager**

  If you remove an IBM LPAR Manager model or delete the IBM LPAR folder from the Navigation panel, CA Spectrum deletes all related child models.

- **An entity removed from IBM LPAR virtual environment**

  As you delete IBM LPAR Hosts and IBM LPAR instances using the HMC, CA Spectrum also deletes those models and their child models from Virtual Host Manager.

- **Upgraded models exist**—In some cases, an IBM LPAR instance is first modeled for Virtual Host Manager without SNMP capabilities. If SNMP capabilities are later added to a VHM model (see definition on page 270), the previous model is deleted and replaced with the new SNMP-capable model.

Note: Although the default setting is to delete the models, you can configure Virtual Host Manager to place the IBM LPAR Host and IBM LPAR instances in the LostFound container when they are removed from Virtual Host Manager. This configuration setting applies only when you remove devices using your HMC. However, this setting does not apply when you delete the IBM LPAR folder, remove an IBM LPAR Manager model, or upgrade a VHM model.

More information:

Manage Device Models for Devices Deleted from IBM LPAR Manager (see page 184)
Adding SNMP Capabilities to VHM Models (see page 193)
Manage SNMP-Enabled LPAR Models After IBM LPAR Manager Deletion (see page 188)

Alarms and Fault Isolation for IBM LPAR

This section describes the traps used by Virtual Host Manager and the resulting alarms. This section also explains how Virtual Host Manager fault isolation differs from basic CA Spectrum fault isolation.

Virtual Host Manager Alarms for IBM LPAR

To alert you to problems within your virtual network, CA Spectrum generates alarms. Alarms are created in two ways:

- Traps sent from the CA SystemEDGE agent
- Polling

Polling generates four alarms: IBM LPAR Proxy Lost, IBM LPAR Host Proxy Lost, IBM LPAR Manager Unavailable, and IBM LPAR Not Running. However, several traps can generate alarms on your virtual devices. CA Spectrum supports all traps sent by the IBM LPAR AIM from the CA SystemEDGE agent. To get the greatest value from these traps when monitoring your devices, you can configure the threshold values for each virtual device individually.

If a trap breaches your threshold value and generates an alarm, CA Spectrum uses the value of the “state” varbind passed with the trap to determine the alarm severity. All state varbinds have the following possible values, which CA Spectrum alarms on the same way:

- 0: Unknown
- 1: OK
- 2: Warning
- 3: Critical

The "Unknown" state does not have an associated alarm severity and does not change the alarm severity of a device. CA Spectrum maps the other IBM LPAR technology states to a CA Spectrum alarm severity:

IBM LPAR State	CA Spectrum Alarm Severity
1: OK	Normal (Green)
2: Warning	Minor (Yellow)
3: Critical	Major (Orange)

More information:

Manage Device Models for Devices Deleted from IBM LPAR Manager (see page 184)
Status Monitoring Options (see page 203)
Configure and Monitor Resource Status (see page 207)
Manage SNMP-Enabled LPAR Models After IBM LPAR Manager Deletion (see page 188)

How CA Spectrum Forwards Traps from CA SystemEDGE

CA Spectrum supports all traps sent by the IBM LPAR AIM. These traps are initially sent to the IBM LPAR CA SystemEDGE model. If the destination for a trap is not this model, CA Spectrum forwards the trap to the correct virtual model.

Note: For specific event codes related to the traps, use the Event Configuration application and filter on “0x056e.” Or you can launch MIB tools to view the traps in the Trap Support table for the “EMPIRE-CALPARA-MIB” MIB. For more information about using the Event Configuration application, see the *Event Configuration User Guide*. For more information about using MIB tools, see the *Modeling and Managing Your IT Infrastructure Administrator Guide*.

CA Spectrum determines where to forward the trap by using the following process:

1. When CA Spectrum receives a trap, it uses varbind information in the trap to locate the correct virtual entity, as follows:
   - For traps that are forwarded to an IBM LPAR Host, CA Spectrum uses the UID to locate the correct host.
   - For traps that are forwarded to an IBM LPAR instance, CA Spectrum uses the UID to determine first the correct IBM LPAR Host. Based on the UID or the IBM LPAR name, CA Spectrum locates the correct IBM LPAR instance within the list of IBM LPARs managed by this IBM LPAR Host.

2. CA Spectrum uses this UID to look up and locate the CA Spectrum model that is tied to a given UID. The entity type of all traps is predetermined. Depending on the results of the look-up, CA Spectrum forwards the trap as follows:

   - If it finds a CA Spectrum model of a specific type with a given UID and in some cases an IBM LPAR name, CA Spectrum forwards the event and corresponding alarm to the destination model.
   - If it cannot find a CA Spectrum model for a given UID and in some cases an IBM LPAR name, CA Spectrum generates a new generic event on the IBM LPAR Manager model. This new event includes details about the trap.

     Note: CA Spectrum often cannot find a related model when a trap is sent immediately after changing your virtual network entities in the HMC (see definition on page 268). IBM LPAR Discovery has not yet identified and created the corresponding model in CA Spectrum.

More information:

Traps Supported in Virtual Host Manager (see page 213)

Traps Supported in Virtual Host Manager

All traps generated by the IBM LPAR AIM are supported in CA Spectrum. The traps are initially sent to the IBM LPAR Manager model. Then, the traps are forwarded to a corresponding virtual entity type (that is, the "destination" entity), depending on the type of trap. Using these traps, you can monitor the performance of your virtual network, resolve any resulting alarms, or trigger events.

Note: For more information about traps generated by the IBM LPAR AIM, see the *CA Virtual Assurance for Infrastructure Managers Implementation Guide*.

The following tables list the traps for a specific destination entity type and specify whether the trap generates an alarm.

IBM LPAR Manager Traps

Trap Name	Trap OID	Alarm?
lparAimSysAdded	1.3.6.1.4.1.546.1.1.0.165317	No
lparAimSysRemove	1.3.6.1.4.1.546.1.1.0.165316	No

IBM LPAR Host Traps

Trap Name	Trap OID	Alarm?
lparAimLPAdded	1.3.6.1.4.1.546.1.1.0.165321	No
lparAimLPDeleted	1.3.6.1.4.1.546.1.1.0.165322	No
lparAimSlotAdd	1.3.6.1.4.1.546.1.1.0.165340	No

Trap Name	Trap OID	Alarm?
lparAimSlotDelete	1.3.6.1.4.1.546.1.1.0.165341	No
lparAimSlotLPChange	1.3.6.1.4.1.546.1.1.0.165342	No
lparAimSlotMonitorChange	1.3.6.1.4.1.546.1.1.0.165343	No
lparAimSysCfgAlertChange	1.3.6.1.4.1.546.1.1.0.165312	No
lparAimSysCfgMonitorChange	1.3.6.1.4.1.546.1.1.0.165311	No
lparAimSysCPUThresholdChange	1.3.6.1.4.1.546.1.1.0.165313	No
lparAimSysDown	1.3.6.1.4.1.546.1.1.0.165315	No
lparAimSysMEMThresholdChange	1.3.6.1.4.1.546.1.1.0.165314	No
lparAimSysProfAdd	1.3.6.1.4.1.546.1.1.0.165360	No
lparAimSysProfChange	1.3.6.1.4.1.546.1.1.0.165362	No
lparAimSysProfDelete	1.3.6.1.4.1.546.1.1.0.165361	No
lparAimSysStateChangeTrap	1.3.6.1.4.1.546.1.1.0.165310	Yes
lparAimSysCpuStateChange	1.3.6.1.4.1.546.1.1.0.165318	Yes

IBM LPAR Traps

Trap Name	Trap OID	Alarm?
lparAimLPAlert	1.3.6.1.4.1.546.1.1.0.165324	No
lparAimLPCPUCritThreshold	1.3.6.1.4.1.546.1.1.0.165329	No
lparAimLPCPULagSetting	1.3.6.1.4.1.546.1.1.0.165327	No
lparAimLPCPUMonitor	1.3.6.1.4.1.546.1.1.0.165325	No
lparAimLPCPUState	1.3.6.1.4.1.546.1.1.0.165333	Yes
lparAimLPCPUWarnThreshold	1.3.6.1.4.1.546.1.1.0.165328	No
lparAimLPMemoryCritThreshold	1.3.6.1.4.1.546.1.1.0.165331	No
lparAimLPMemoryMonitor	1.3.6.1.4.1.546.1.1.0.165326	No
lparAimLPMemoryState	1.3.6.1.4.1.546.1.1.0.165332	Yes
lparAimLPMemoryWarnThreshold	1.3.6.1.4.1.546.1.1.0.165330	No
lparAimLPMonitor	1.3.6.1.4.1.546.1.1.0.165323	No
lparAimLPStateChange	1.3.6.1.4.1.546.1.1.0.165320	Yes
lparAimProfAdd	1.3.6.1.4.1.546.1.1.0.165350	No
lparAimProfDelete	1.3.6.1.4.1.546.1.1.0.165351	No
lparAimVIOvEthernetAdd	1.3.6.1.4.1.546.1.1.0.165373	No

Trap Name	Trap OID	Alarm?
lparAimVIOvEthernetRemoved	1.3.6.1.4.1.546.1.1.0.165374	No
lparAimVIOvSCSIAdd	1.3.6.1.4.1.546.1.1.0.165370	No
lparAimVIOvSCSIRemoved	1.3.6.1.4.1.546.1.1.0.165371	No
lparAimVIOvSerialAdd	1.3.6.1.4.1.546.1.1.0.165375	No
lparAimVIOvSerialRemoved	1.3.6.1.4.1.546.1.1.0.165376	No

More information:

How the IBM LPAR Data is Updated in Virtual Host Manager (see page 199)
Status Monitoring Options (see page 203)
How to Configure Management Options (see page 204)
Configure and Monitor Resource Status (see page 207)
How CA Spectrum Forwards Traps from CA SystemEDGE (see page 212)

Fault Management for Virtual Networks

The goal of fault isolation is to narrow down the root cause of a networking problem. Finding the root cause can help you to troubleshoot and quickly correct the problem or to correct the problem programmatically with automated scripts. Deciding which devices are the root cause of an alarm can be difficult, because problems with a single device can cause several devices in your network to generate events.

For example, losing contact with an IBM LPAR Host often means that you have also lost contact with the IBM LPAR instances it manages. Therefore, the IBM LPAR Host device model and all affected IBM LPAR instances generate alarms. Using fault isolation techniques, Virtual Host Manager correlates these alarms in an attempt to identify a single root cause.

Virtual networks provide a unique management opportunity, because they provide CA Spectrum an alternate management perspective. That is, CA Spectrum can gather information through direct contact with your virtual devices or through the virtual network management technology, IBM LPAR. This alternate management perspective enhances standard CA Spectrum fault management in two ways:

- **Enhanced Contact Lost alarms**—Two sources of information about a device means Virtual Host Manager can pinpoint the cause and more easily correlate events to a single root cause.
- **Proxy Failure alarms**—*Proxy management* is the act of managing network devices using an alternate management source in place of or in addition to the primary manager. For example, CA Spectrum can manage virtual network devices by contacting them directly or through the virtual technology application's contact with the devices. When IBM LPAR virtualization technology loses contact with a virtual network device, Virtual Host Manager generates one of the Proxy Management Lost alarms for each device. These alarms are unique, because they are alerting you to the fact that *management* of the device through the *proxy* is affected, not the state of the device or direct (SNMP) management.

How Fault Isolation Works when Device Contact is Lost

To help you troubleshoot networking problems with your devices, CA Spectrum uses fault isolation to narrow down the root cause of an alarm. For virtual networks, Virtual Host Manager uses information from direct contact with the device plus information provided by IBM LPAR technology through the IBM LPAR AIM. In many cases, standard CA Spectrum fault management can pinpoint the root cause. But in special circumstances, the method for isolating problems in a virtual network go beyond the standard methods.

The type of fault isolation Virtual Host Manager uses to discover the root cause depends on which devices are alarming and the type of events the devices generate. The following scenarios describe two unique fault management situations and how CA Spectrum isolates the networking error in your virtual network.

Scenario 1: IBM LPAR instance is not running

In a virtual environment, the virtual management application can provide more details than CA Spectrum can discover through standard device monitoring. For example, the IBM LPAR virtualization technology is aware when an IBM LPAR changes from the "running" state to something else, such as the "open-firmware" state.

If an IBM LPAR is no longer running and CA Spectrum loses contact with it, but proxy management (see definition on page 269) of the IBM LPAR Manager is uninterrupted, CA Spectrum determines the root cause as follows:

1. When CA Spectrum loses contact with an IBM LPAR, it generates a Contact Lost alarm.
2. During its next polling cycle, the IBM LPAR Manager model polls the IBM LPAR AIM to gather information about the IBM LPAR instance. Because IBM LPAR technology manages the IBM LPAR instances, it can provide a unique view into the possible cause of alarms generated by an IBM LPAR.
3. If the IBM LPAR technology finds that the IBM LPAR is in the not-running mode, it generates an IBM LPAR Not Running alarm.

   Note: This alarm is cleared upon the first IBM LPAR AIM polling cycle after the IBM LPAR is running again.
4. Virtual Host Manager correlates the Contact Lost alarm to the corresponding IBM LPAR Not Running alarm created by CA Spectrum. Virtual Host Manager makes the Contact Lost alarm appear as a symptom of the IBM LPAR Not Running alarm.

Scenario 2: IBM LPAR Host is down

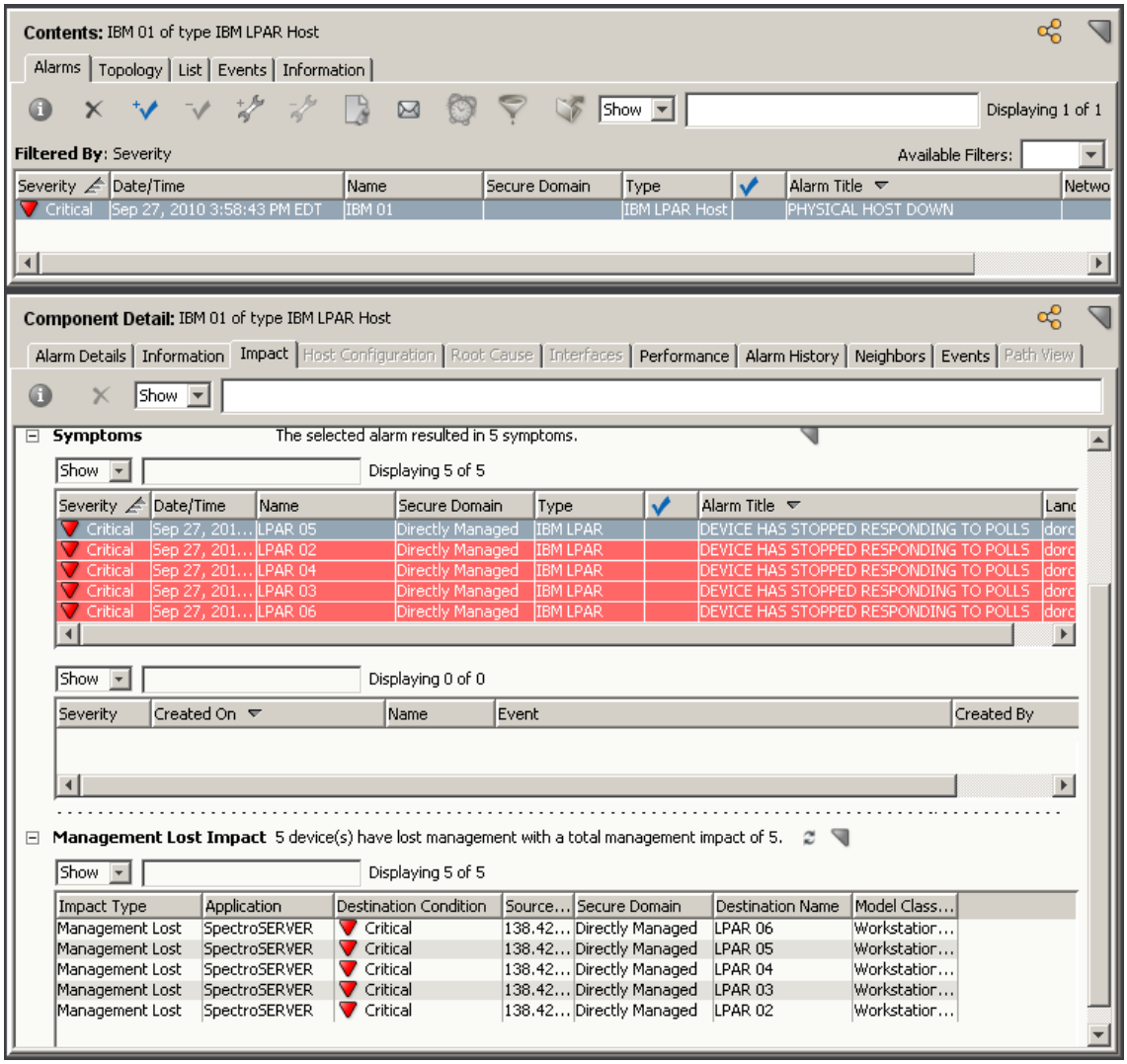
If CA Spectrum loses contact with all IBM LPARs running on an IBM LPAR Host, CA Spectrum checks the status of the upstream routers and switches. Depending on their status, CA Spectrum determines the root cause as follows:

- All upstream devices for one or more IBM LPAR instances are unavailable—Standard CA Spectrum fault isolation techniques determine the root cause, as follows:
  - Device Stopped Responding to Polls alarm—Generated on the IBM LPAR Host when at least ne upstream connected device for any IBM LPAR is up.
  - Gateway Unreachable alarm—Generated on the IBM LPAR Host when *all* upstream connected devices are down.
- At least one upstream device is available for every IBM LPAR instance connected to the IBM LPAR Host—CA Spectrum infers that the IBM LPAR Host is the root cause and responds as follows:
  a. All IBM LPARs, ports, and fanouts that are directly connected to the IBM LPAR models generate the standard fault isolation alarms.
  b. Virtual Host Manager creates a Physical Host Down alarm for the IBM LPAR Host model.
  c. All fault isolation-related alarms that are created for the impacted devices (such as IBM LPARs, ports, and fanouts) are correlated to the Physical Host Down alarm, making them symptoms of the Physical Host Down alarm. These symptom alarms appear in the Symptoms table on the Impact tab for the Physical Host Down alarm.

Note: For each IBM LPAR Host model, Virtual Host Manager creates a "virtual fault domain." This domain includes the IBM LPAR Host and IBM LPAR instances, plus all ports and fanouts directly connected to the IBM LPARs. When the IBM LPAR Host generates the Physical Host Down alarm, all standard fault isolation alarms within the domain are correlated to it. Correlating these alarms as symptoms indicates that the Physical Host Down alarm on the IBM LPAR Host is the root cause.

d. All impacted devices are listed in the Management Lost Impact table on the Impact tab for the Physical Host Down alarm.

Note: Devices that are suppressed do not have a corresponding alarm in the Symptoms table.



e. If all upstream devices for one or more IBM LPAR instances go down, CA Spectrum can no longer reliably state that the fault lies with the IBM LPAR Host. Therefore, CA Spectrum clears the Physical Host Down alarm and applies the standard CA Spectrum fault isolation techniques.

More information:

How Fault Isolation Works when Proxy Management is Lost (see page 219)
Determining IBM LPARs Affected by Host Outages (see page 222)

How Fault Isolation Works when Proxy Management is Lost

The IBM LPAR virtualization technology used to create your virtual network provides CA Spectrum a unique management opportunity. CA Spectrum can use the standard methods to contact your virtual devices directly, plus CA Spectrum can simultaneously gather virtual device information from IBM LPAR technology. In this sense, the IBM LPAR technology is a "proxy" from which CA Spectrum gathers virtual device information. If CA Spectrum loses direct contact with a device, it generates alarms. Likewise, if IBM LPAR technology loses contact with a virtual device or if Virtual Host Manager loses contact with the IBM LPAR Manager, Virtual Host Manager generates alarms—Proxy Management Lost alarms (see definition on page 269).

In response, CA Spectrum attempts to isolate the cause of the proxy management failure. Proxy fault isolation is similar to the standard CA Spectrum fault isolation, except that these alarms alert you to the fact that *proxy* management of a virtual device is affected. Proxy management fault isolation cannot tell you whether a virtual device is up or down. However, it is important to know when contact through the proxy is lost, because you could be missing important virtual information about a device.

The type of proxy fault isolation Virtual Host Manager uses to discover the root cause depends on which devices are alarming and the type of events the devices generate. The following scenarios describe two unique proxy fault management situations and how Virtual Host Manager isolates the networking error in your virtual network.

Scenario 1: Contact between IBM LPAR Manager and HMC is lost

If the IBM LPAR Manager loses contact with an HMC and all IBM LPAR Hosts and IBM LPARs the HMC is managing, the IBM LPAR Manager data about the IBM LPAR Hosts and all hosted IBM LPAR instances is lost. To isolate the problem, Virtual Host Manager determines the root cause as follows:

1. A Proxy Lost alarm is generated on the IBM LPAR Hosts and all hosted IBM LPARs.
2. The IBM LPAR alarms are correlated to the Proxy Lost alarm for the IBM LPAR Host, making these IBM LPAR alarms symptoms of the IBM LPAR Host alarm. Correlating these alarms as symptoms indicates that the IBM LPAR Host alarm is the root cause.
3. If CA Spectrum also loses contact with the IBM LPAR Host and generates a Physical Host Down alarm, the Proxy Lost alarm generated for the IBM LPAR Host is correlated to the Physical Host Down alarm. In this case, the Proxy Lost alarm becomes a symptom of the Physical Host Down alarm. Correlating this alarm as a symptom indicates that the Physical Host Down alarm on the IBM LPAR Host is the root cause.

Scenario 2: Contact between CA Spectrum and IBM LPAR Manager is lost

If CA Spectrum loses contact with or stops polling the IBM LPAR Manager model, CA Spectrum loses the IBM LPAR technology data about all virtual models managed by that IBM LPAR Manager. To isolate the problem, Virtual Host Manager determines the root cause as follows:

1. CA Spectrum generates Proxy Lost alarms for all virtual models managed by that IBM LPAR Manager, including IBM LPAR instances and IBM LPAR Hosts. CA Spectrum also generates a separate Proxy Unavailable alarm on the IBM LPAR Manager model.
2. The IBM LPAR alarms are correlated to their corresponding IBM LPAR Host model alarm.
3. The IBM LPAR Host model alarms are correlated to a Proxy Unavailable alarm for the IBM LPAR Manager model.
4. This Proxy Unavailable alarm is then correlated to the root cause of the IBM LPAR Manager being down. The root cause is typically an alarm generated by standard CA Spectrum fault management, such as the alarms created for the following situations:
   - Lost management of IBM LPAR Manager (that is, a problem occurred with the CA SystemEDGE agent on the IBM LPAR Manager host)
   - Machine contact is lost
   - IBM LPAR Manager model is in maintenance mode

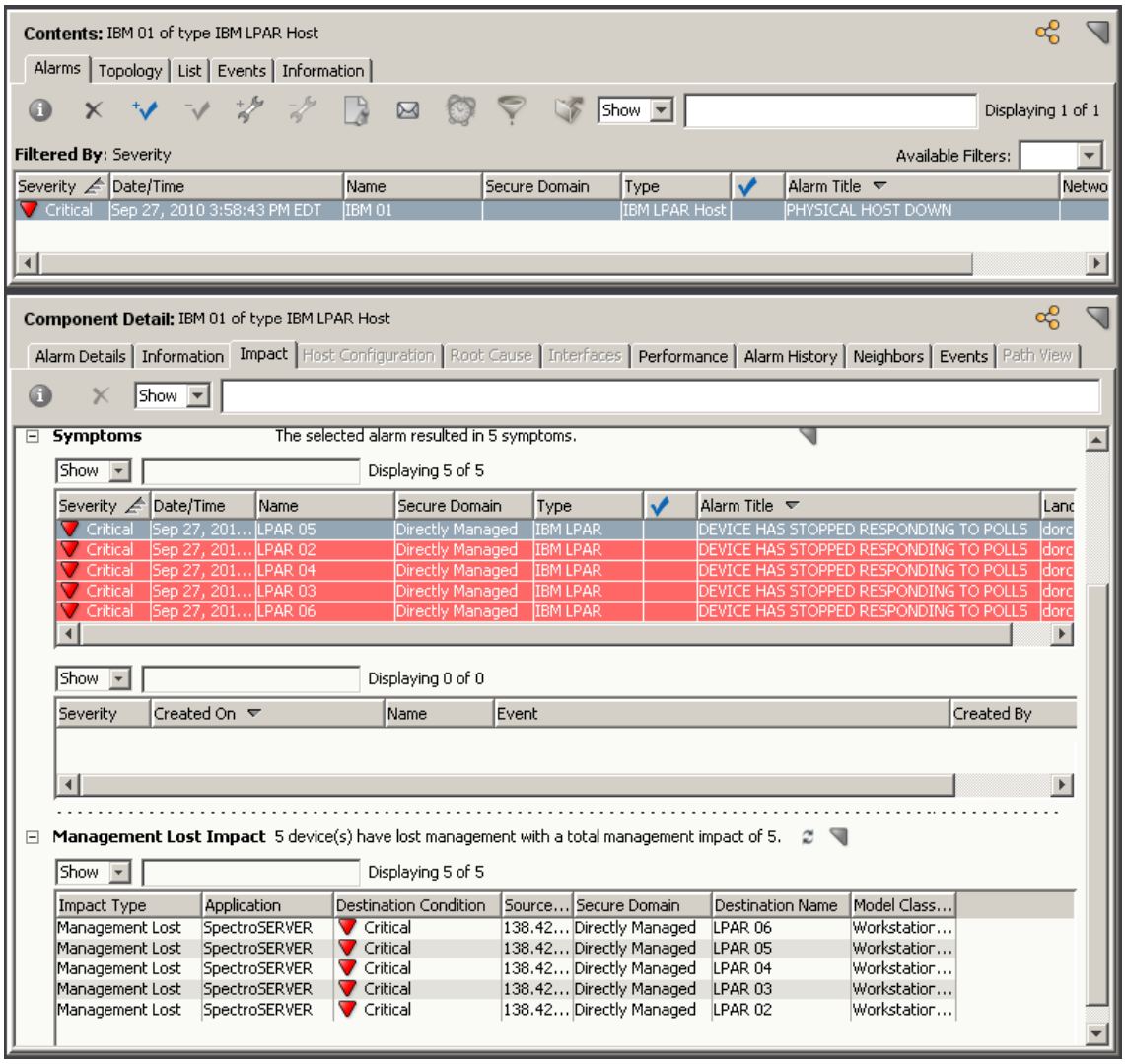
More information:

How Fault Isolation Works when Device Contact is Lost (see page 216)

Determining IBM LPARs Affected by Host Outages

When contact with an IBM LPAR Host is interrupted or the IBM LPAR Host goes down, all IBM LPAR instances hosted by the IBM LPAR Host are affected. Because IBM LPAR technology cannot communicate with the IBM LPAR Host to get usage information, you might not receive alarms for a critical IBM LPAR hosted on that IBM LPAR Host. To find out if a critical IBM LPAR is impacted, you can view a list of affected IBM LPAR instances on the Impact tab of the alarm, as follows:

- Symptoms subview—displays all symptom alarms generated by the affected IBM LPAR instances
- Management Lost Impact subview—lists the IBM LPAR instances impacted by the alarm



More information:

How Fault Isolation Works when Device Contact is Lost (see page 216)

Chapter 7: Huawei SingleCLOUD

This section is for Huawei SingleCLOUD virtualization technology users and describes how to use Virtual Host Manager to manage the virtual entities in your Huawei SingleCLOUD platform.

This section contains the following topics:

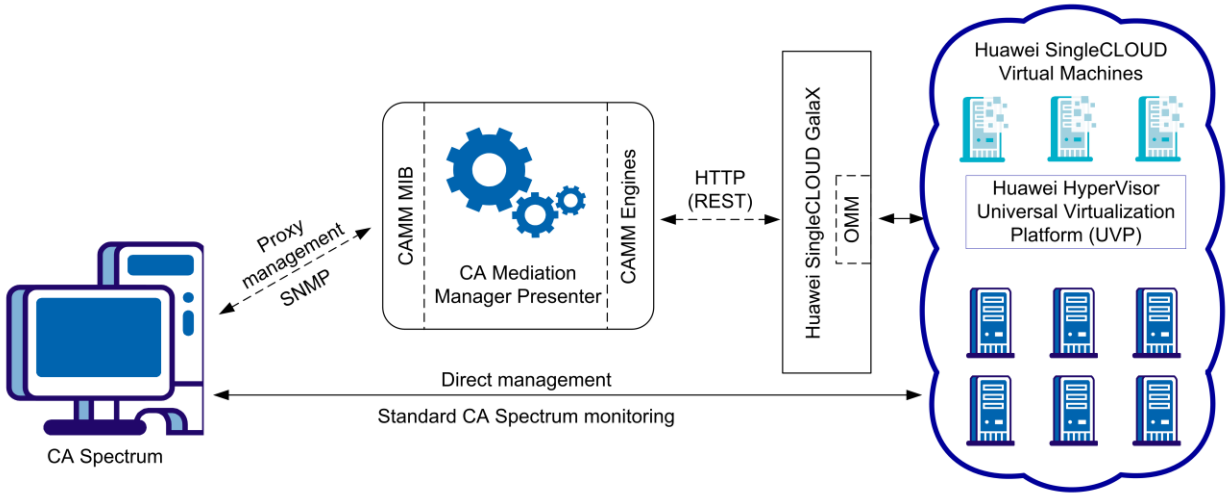
How Virtual Host Manager Works with Huawei SingleCLOUD

Virtual Host Manager monitors your virtual network entities seamlessly with your physical network entities. You get a full view of your network where you can troubleshoot networking issues for both types of entity. Although your virtual network entities behave like physical components, the process for monitoring those entities differs from the general CA Spectrum monitoring process. Understanding how this process works can help you locate and resolve networking issues related to your virtual network.

The Huawei SingleCLOUD platform consists of a complete system of network, storage, servers, and software for creating private or public clouds. Virtual Host Manager helps you to manage and monitor your Huawei SingleCLOUD virtual environment.

CA Spectrum gathers information about your Huawei SingleCLOUD virtual environment by two different methods. As with other CA Spectrum managed devices, Virtual Host Manager uses standard CA Spectrum monitoring methods. In addition, Virtual Host Manager for Huawei SingleCLOUD also retrieves specialized information from an alternate (proxy) manager, CA Mediation Manager (CAMM).

The following diagram shows how CA Spectrum gathers information about your Huawei SingleCLOUD environment:



CA Mediation Manager resides on its own host and obtains information from the Huawei SingleCLOUD environment by using HTTP (REST) services to communicate with Huawei SingleCLOUD GalaX, a software suite that collectively manages Huawei SingleCLOUD.

CAMM uses the following components:

- The Engine. The Engine is CAMM's polling engine which gathers information from the Huawei SingleCLOUD platform. The CAMM Engine communicates directly with the Huawei SingleCLOUD GalaX Operation and Management Module (OMM) to obtain information about the Huawei HyperVisor Universal Virtualization Platform (UVP).
- The Presenter. The Presenter receives the information from the Engine and uses it to populate a CA-developed MIB (CAMEDIATIONMANAGER-ENTERPRISES-HUAWEI-SINGLECLOUD-MIB).

CA Spectrum uses SNMP to retrieve data from the CAMM MIB and uses this information to model and monitor your Huawei SingleCLOUD environment in OneClick.

Models Created for Huawei SingleCLOUD

Virtual Host Manager provides several models to represent the components of your Huawei SingleCLOUD virtual network. Understanding the following basic models can help you better understand Discovery and how the virtual environment interfaces with your physical environment.

Virtual Host Manager includes the following models and icons for Huawei SingleCLOUD entities:

Huawei SingleCLOUD CAMM Presenter

Represents a CA Mediation Manager (CAMM) Presenter. The CAMM Presenter model allows configuration of the virtual IP addresses used by the CAMM Engines to communicate with Huawei SingleCLOUD GalaX. Each CAMM Presenter can support multiple virtual IP addresses.

Icon: 

Huawei SingleCLOUD Manager

Represents a virtual IP address on the CAMM Presenter. CAMM communicates with Huawei SingleCLOUD GalaX, which is responsible for managing the Huawei SingleCLOUD virtual platform. Information for each Huawei SingleCLOUD GalaX being monitored by CAMM is provided through a virtual IP address on the CAMM Presenter and is represented by a Huawei SingleCLOUD Manager model.

Icon: 

Huawei SingleCLOUD Cloud

Represents a collection of physical and virtual hosts that make up a private or public cloud network.

Icon: 

Huawei SingleCLOUD Host

Represents the Computing Node Agent (CNA) that hosts the virtual machines. In the Universe topology, these models group your virtual entities into a separate view while showing where the virtual environment interfaces with your physical network. The Huawei SingleCLOUD Host cannot be contacted directly for status information. Instead, the status of this model is inferred from the status of its contained items.

Icon: 

Huawei SingleCLOUD CNA FIP

Represents the management interface of the CNA that is hosting the virtual machines. This model is assigned the IP address of the CNA FIP and lives within the host container.

Icon: 

Huawei SingleCLOUD Virtual Machine

Represents a virtual machine, as configured in your Huawei SingleCLOUD platform.

Icon: 

Discovering Huawei SingleCLOUD Networks

Before you can use Virtual Host Manager to monitor your Huawei SingleCLOUD virtual environment, you have to discover and model any network elements that are to be managed. This section describes the discovery and modeling process for Virtual Host Manager for Huawei SingleCLOUD. These tasks are typically performed by the Virtual Host Manager administrator.

Follow these steps:

1. Perform the following pre-Discovery steps:
   a. Define CA Mediation Manager Presenters. (see page 229)
   b. Configure Discovery Options. (see page 230)
2. Discover and model your Huawei SingleCLOUD network. (see page 235)

Define CA Mediation Manager Presenters

After Virtual Host Manager is installed, you define the CA Mediation Manager Presenters to CA Spectrum. The Huawei SingleCLOUD CAMM Presenter model allows configuration of the virtual IP addresses associated with Huawei SingleCLOUD GalaX. Defining a CAMM Presenter creates a container model that will later be used to organize and contain Huawei SingleCLOUD Manager models.

Note: Creating a Huawei SingleCLOUD CAMM Presenter model does not trigger Discovery.

Follow these steps:

1. Select the Virtual Host Manager node in the Explorer tab in the Navigation panel.

   The Contents panel displays information for the Virtual Host Manager feature.
2. Select the Information tab.
3. Expand the Configuration, Huawei SingleCLOUD, CA Mediation Manager Presenters subview.

   The CA Mediation Manager Presenters table appears.
4. Click Add.

   The 'Create Model Of Type HuaweiSCCAMMPresenter' dialog appears.
5. Enter a Name and Description, and click OK.

   The Huawei SingleCLOUD CAMM Presenter model is created and appears in the table.

More information:

Models Created for Huawei SingleCLOUD (see page 226)

Configure Discovery Options

Before you perform Discovery to create models for your Huawei SingleCLOUD entities, specify options to control aspects of the Discovery process. Configuring your preferences helps Virtual Host Manager model your virtual devices as expected.

To configure your installation of Virtual Host Manager for Huawei SingleCLOUD Discovery, select your preferences from the following options:

- Maintenance Mode for New Huawei SingleCLOUD Virtual Machines (see page 230)—Lets you decide whether to place newly discovered virtual machines into maintenance mode until you are ready for CA Spectrum to manage them.
- Allow Device Model Deletes During Huawei SingleCLOUD Discovery (see page 231)—Controls how CA Spectrum handles Huawei SingleCLOUD models when Virtual Host Manager no longer manages them.
- Search for Existing Models (see page 232)—Determines which secure domains Virtual Host Manager searches during a Huawei SingleCLOUD Discovery.
- Retain SNMP-enabled Virtual Machines During Huawei SingleCLOUD Manager Deletion (see page 233)—Controls how CA Spectrum handles SNMP-enabled Huawei SingleCLOUD models when a Huawei SingleCLOUD Manager model is deleted.
- Discover SNMP-Capable Devices (see page 235)—Controls how SNMP-capable devices are modeled during Huawei SingleCLOUD Discovery. By default, new models are initially created as VHM models (see definition on page 270) only. But this option lets you override the default and immediately create SNMP models for devices that meet the criteria.

Configure Maintenance Mode for New Huawei SingleCLOUD Devices

areVirtual Host Manager automatically models the virtual machines that make up the Huawei SingleCLOUD virtual environment. CA Spectrum attempts to manage all models that are discovered. However, some newly discovered Huawei SingleCLOUD virtual machines are not ready for CA Spectrum management when they are initially modeled. To prevent undesired alarms on new Huawei SingleCLOUD Virtual Machine models, you can decide which new models are immediately placed into maintenance mode. Later, you can manually disable maintenance mode when you are ready for CA Spectrum to manage these devices.

Follow these steps:

1. Click the Virtual Host Manager node in the Explorer tab in the Navigation panel.

   The Contents panel displays information for the Virtual Host Manager feature.

2. Click the Information tab.

3. Expand the Configuration, Huawei SingleCLOUD, Huawei SingleCLOUD Discovery subview.

   Configurable Discovery options appear.

4. Click Set in the 'Maintenance Mode for New Huawei SingleCLOUD Virtual Machines' field and select one of the following options:

   Place non-enabled VMs in Maintenance Mode

   (Default) Applies maintenance mode to only non-enabled Huawei SingleCLOUD Virtual Machine models upon initial Huawei SingleCLOUD Discovery.

   Place all VMs in Maintenance Mode

   Applies maintenance mode to all newly discovered Huawei SingleCLOUD Virtual Machine models upon initial Huawei SingleCLOUD Discovery.

   Your setting is saved and newly discovered Huawei SingleCLOUD Virtual Machine models created by Virtual Host Manager are placed into maintenance mode per your selection.

Manage Device Models for Deleted Huawei SingleCLOUD Devices

The devices and the relationships among them change frequently in virtual environments. Maintaining accurate and timely data about your virtual environment in CA Spectrum is challenging. For example, when a Huawei SingleCLOUD virtual machine is removed, CA Spectrum knows to remove the corresponding device models from Virtual Host Manager in the Navigation panel. However, should CA Spectrum keep or delete the model? You can select settings to control model deletion.

Important! When models are deleted, all notes or other customizations on those models are lost. You can disable this option if your models are likely to be recreated in your Huawei SingleCLOUD environment later.

Follow these steps:

1. Click the Virtual Host Manager node in the Explorer tab in the Navigation panel.

   The Contents panel displays information for the Virtual Host Manager feature.

2. Click the Information tab.

3. Expand the Configuration, Huawei SingleCLOUD, Huawei SingleCLOUD Discovery subview.

   Configurable Discovery options appear.

4. Click Set in the 'Allow Device Model Deletes During Huawei SingleCLOUD Discovery' field and select one of the following options:

   Yes

   (Default) Deletes the Virtual Host Manager models that correspond to entities no longer managed in your Huawei SingleCLOUD environment.

   No

   Places Virtual Host Manager models in the LostFound container if their corresponding entity is no longer managed by your Huawei SingleCLOUD environment, but the models are not deleted from CA Spectrum.

   Note: Models with more associations, such as a model that is included in a Global Collection, are handled differently. These models are removed from the Universe, but they are not moved to the LostFound container.

   Your setting is saved, and device models are handled accordingly after the device is deleted from your Huawei SingleCLOUD environment.

Configure Model Searches Across Secure Domains

Rather than creating new models, Huawei SingleCLOUD Discovery attempts to locate models in the SpectroSERVER. In an environment with Secure Domain Manager deployed, Huawei SingleCLOUD Discovery searches for models within the same secure domain as your Huawei SingleCLOUD Manager. This domain is the "local" domain. However, some of your devices can exist within a different secure domain. In this case, you can configure Huawei SingleCLOUD Discovery to search all secure domains for existing models.

Follow these steps:

1. Click the Virtual Host Manager node in the Explorer tab in the Navigation panel.

   The Contents panel displays information for the Virtual Host Manager feature.

2. Click the Information tab.

3. Expand the Configuration, Huawei SingleCLOUD, Huawei SingleCLOUD Discovery subview.

   Configurable Discovery options appear.

4. Click Set in the 'Search for Existing Models' field and select from the following options:

   In Huawei SingleCLOUD Manager's Secure Domain

   (Default) Searches for models within the same secure domain as the Huawei SingleCLOUD Manager server.

   In All Secure Domains

   Searches for models within all secure domains managed by the SpectroSERVER. Select this option only in the following situations:

   - All devices have unique IP addresses
   - When secure domains are used for security purposes or to isolate network traffic

   Note: Do not select this option for a NAT environment.

   Your setting is saved, and Huawei SingleCLOUD Discovery searches for existing models in CA Spectrum according to your selection. If duplicate models (that is, models that share the same IP address) exist in multiple secure domains, Virtual Host Manager does the following:

   - Selects the model in the local secure domain, if available.
   - If a duplicate model does not exist in the local domain, Virtual Host Manager randomly selects a model from another secure domain.

   In both cases, Virtual Host Manager generates a minor alarm for the duplicate IP addresses on the Huawei SingleCLOUD Manager model.

Manage Deletion of SNMP-Enabled Huawei SingleCLOUD Models

By default, SNMP-enabled devices are deleted from CA Spectrum when the following items are deleted:

- Huawei SingleCLOUD folder in the Explorer tab
- Huawei SingleCLOUD CAMM Presenter model
- Huawei SingleCLOUD Manager model

SNMP-enabled device models can include significant customizations that you want to retain. You can adjust your settings to avoid deleting these models. They can be placed into the LostFound container for later use.

Follow these steps:

1. Click the Virtual Host Manager node in the Explorer tab in the Navigation panel.

   The Contents panel displays information for the Virtual Host Manager feature.

2. Click the Information tab.

3. Expand the Configuration, Huawei SingleCLOUD, Huawei SingleCLOUD Discovery subview.

   Configurable Discovery options appear.

4. Click Set in the ‘Retain SNMP-enabled Virtual Machines During Huawei SingleCLOUD Manager Deletion' field and select one of the following options:

   Yes

   Retains SNMP-enabled virtual machine models in the LostFound container when their Huawei SingleCLOUD folder, Huawei SingleCLOUD CAMM Presenter model, or Huawei SingleCLOUD Manager model is deleted.

   Note: Models with more associations, such as a model that is included in a Global Collection, are handled differently. These models are removed from the Universe, but they are not moved to the LostFound container.

   No

   (Default) Deletes all Huawei SingleCLOUD models when their Huawei SingleCLOUD folder, Huawei SingleCLOUD CAMM Presenter model, or Huawei SingleCLOUD Manager model is deleted.

   Your setting is saved, and SNMP-enabled device models are handled accordingly when the Huawei SingleCLOUD folder, Huawei SingleCLOUD CAMM Presenter model, or Huawei SingleCLOUD Manager model is deleted.

Configure SNMP Modeling Preferences

SNMP-capable devices support enriched device monitoring, such as process and file system monitoring capabilities. However, SNMP agents can be costly and time-consuming to deploy. By default, Huawei SingleCLOUD Discovery creates Huawei SingleCLOUD virtual machines as VHM models (see definition on page 270). You can later upgrade them to SNMP models. However, you can also configure Huawei SingleCLOUD Discovery to model all new SNMP-capable devices as SNMP models. Although Huawei SingleCLOUD Discovery may take longer to complete, initially modeling these as SNMP models spares you from manually upgrading these models later.

Important! Enable SNMP modeling *before* modeling Huawei SingleCLOUD components. If you model the Huawei SingleCLOUD components first, any child models are created as VHM models, which must be manually upgraded to SNMP models.

Follow these steps:

1. Click the Virtual Host Manager node in the Explorer tab in the Navigation panel.

   The Contents panel displays information for the Virtual Host Manager feature.

2. Click the Information tab.

3. Expand the Configuration, Huawei SingleCLOUD, Huawei SingleCLOUD Discovery, SNMP Discovery subview.

4. Click Set in the 'Discover SNMP-Capable Devices' field and select from the following options:

   Yes

   Enables SNMP modeling during Huawei SingleCLOUD Discovery. Only devices that meet the criteria in the SNMP Discovery subview text are modeled as SNMP devices. Applies to *new* models only.

   No

   (Default) Models all new devices found during Huawei SingleCLOUD Discovery as VHM models (see definition on page 270). You can manually upgrade these models to SNMP models later.

   Your setting is saved and new devices are modeled in Virtual Host Manager per your selection.

Discover and Model Your Huawei SingleCLOUD Environment

To monitor your virtual environment, you must discover and model your virtual entities—Huawei SingleCLOUD Managers, Clouds, Hosts, and Virtual Machines. Modeling these entities in Virtual Host Manager lets you view your complete network topology in one tool, showing the relationships between your physical and virtual components.

The main steps for modeling your virtual environment are as follows:

1. Run a standard CA Spectrum Discovery (see page 236).

   The purpose of this Discovery is to model the upstream routers and switches before Huawei SingleCLOUD Discovery runs. When modeling these entities, be sure that your modeling options are set correctly to support Virtual Host Manager.

2. Define Huawei SingleCLOUD Managers (see page 237).

   This step discovers and models the virtual IP addresses that CAMM uses to communicate with Huawei SingleCLOUD GalaX, the management application for the Huawei SingleCLOUD virtual platform. CA Spectrum uses these models to retrieve information about the Huawei SingleCLOUD architecture and its virtual machines.

3. Let Huawei SingleCLOUD Discovery run (see page 238).

   When you model the Huawei SingleCLOUD Manager, Huawei SingleCLOUD Discovery begins automatically, discovering and modeling the virtual entities in your Huawei SingleCLOUD environment.

4. (Optional) Add SNMP Capabilities to VHM Models (see page 239).

   If you modeled Huawei SingleCLOUD entities as VHM models. you can upgrade them to SNMP models.

5. (Optional) Move a Huawei SingleCLOUD Host to a Different Huawei SingleCLOUD GalaX (see page 241).

   When moving a Huawei SingleCLOUD Host from management by one Huawei SingleCLOUD GalaX to another, steps should be performed in a certain order to accurately reflect the changes in the modeled CA Spectrum environment.

Each of these steps is described in detail in the following sections.

Run CA Spectrum Discovery

To accurately reflect your complete Huawei SingleCLOUD environment, run standard CA Spectrum Discovery to locate any connecting devices. Upstream routers and switches are modeled so that later connections from the virtual entities can be established.

Note: Only an administrator performs this task.

Follow these steps:

1. Open the Discovery console.

   Note: Before modeling, be sure that you know the correct community strings, IP addresses, and port numbers for any SNMP agents that run on a nonstandard port.

2. Click  (Creates a new configuration) in the Navigation panel.

   The Configuration dialog opens.

3. Specify a name and location for the new configuration, and click OK.

   The Configuration dialog closes.

4. Enter individual IP addresses or the beginning and ending IP addresses in the IP/Host Name Boundary List fields and click Add.

   Note: Be sure that the range of IP addresses includes all the interconnecting switches and routers.

5. Configure your Modeling Options as follows:

   a. Select the 'Discover and automatically model to CA Spectrum' option.

   b. Click the Modeling Options button.

      The Modeling Configuration dialog opens.

   c. Click the Protocol Options button.

      The Protocol Options dialog opens.

   d. Select the ARP Tables for Pingables option, and click OK.

      The Protocol Options dialog closes.

   e. Click OK to close the Modeling Configuration dialog.

6. (Optional) Click the Advanced Options button in the Advanced Options group, add your nonstandard SNMP ports (such as the CAMM port), and click OK.

7. Enter any additional values in the Discovery console, and click Discover.

   Models are created and added to your network topology in CA Spectrum for the switches and routers that connect your Huawei SingleCLOUD entities to your network.

Define Huawei SingleCLOUD Managers

After the Huawei SingleCLOUD CAMM Presenter (see definition on page 267) has been defined and you have modeled your connecting devices, you can model and discover your Huawei SingleCLOUD Managers (see definition on page 268). Successful creation of the Huawei SingleCLOUD Manager model automatically triggers Huawei SingleCLOUD Discovery.

Follow these steps:

1. Select the Huawei SingleCLOUD CAMM Presenter in the Huawei SingleCLOUD folder in the Virtual Host Manager hierarchy in the Explorer tab in the Navigation panel.

   The Component Detail panel displays information for the CAMM Presenter.

2. In the Information tab in the Component Detail panel, expand the Huawei SingleCLOUD Managers subview.

   The Huawei SingleCLOUD Managers table appears.

3. Click Add.

   The 'Create Model Of Type HuaweiSCManager' dialog appears.

4. Enter the information for your Huawei SingleCLOUD Manager, and click OK. Notice the following field:

   Network Address

   Enter the virtual IP address used by the CAMM Presenter to communicate with Huawei SingleCLOUD GalaX.

   Important! This value should not be the same as the primary IP address of the device or virtual machine where the CAMM Presenter is installed.

   A Huawei SingleCLOUD Manager model is created and appears in the table. Information about your Huawei SingleCLOUD environment comes from the Huawei SingleCLOUD Manager. When this model is created, Huawei SingleCLOUD Discovery begins.

More information:

Models Created for Huawei SingleCLOUD (see page 226)

Huawei SingleCLOUD Discovery

Huawei SingleCLOUD Discovery is a specialized discovery process that gathers detailed information about your virtual environment. The purpose of Discovery is to discover and model the virtual entities in the Huawei SingleCLOUD platform. Understanding how Huawei SingleCLOUD Discovery works reinforces the importance of installing and modeling the various components of Virtual Host Manager properly.

A key benefit of Huawei SingleCLOUD Discovery is that it runs automatically in the background, continually updating virtual environment data in CA Spectrum. Because of this automated capability, portions of Huawei SingleCLOUD Discovery have already occurred in previous steps. The following description explains the Huawei SingleCLOUD Discovery in its entirety and is provided for reference. No action is required.

The Huawei SingleCLOUD Discovery process works as follows:

1. Immediately after CAMM and the Huawei SingleCLOUD Device Pack are installed correctly, the CAMM Engine starts communicating with Huawei SingleCLOUD GalaX. Information is processed by the CAMM Presenter and is made available to CA Spectrum.

   Important! CA Mediation Manager and the Huawei SingleCLOUD Device Pack must be installed and configured so that CA Spectrum, CAMM, and Huawei SingleCLOUD GalaX can communicate. If they cannot, Huawei SingleCLOUD Discovery cannot run.

2. During CA Spectrum Discovery, CA Spectrum creates models for connecting devices so that later connections from the virtual entities can be established.
3. Huawei SingleCLOUD CAMM Presenter and Huawei SingleCLOUD Manager models are created. Creation of the Huawei SingleCLOUD Manager enables CA Spectrum to handle communication between CA Spectrum and CAMM.
4. The Huawei SingleCLOUD Manager polls CAMM to gather information about the Huawei SingleCLOUD environment, which was gathered in Step 1.
5. CA Spectrum begins Huawei SingleCLOUD Discovery. CA Spectrum uses this information to update modeling in the CA Spectrum Topology tab and the Virtual Host Manager hierarchy in the Navigation panel, as follows:
   a. If you enable SNMP Discovery before Step 2, Virtual Host Manager Discovery creates SNMP models for all new SNMP-capable models that meet the SNMP Discovery criteria.

      Note: By default, SNMP Discovery is disabled during Huawei SingleCLOUD Discovery.

   b. VHM models are created for the remaining non-SNMP Huawei SingleCLOUD entities.

   Note: In a virtual environment, devices on separate Huawei SingleCLOUD Hosts can have the same IP or MAC address. In this case, CA Spectrum creates duplicate models for each occurrence of an IP address or MAC address.
6. Huawei SingleCLOUD Discovery repeats this process at each regularly scheduled Huawei SingleCLOUD Manager polling interval.

Add SNMP Capabilities to VHM Models

SNMP-capable devices support enriched device monitoring, such as process and file system monitoring capabilities. However, SNMP agents can be costly and time-consuming to deploy. When an SNMP agent is not available or SNMP Discovery is disabled, Virtual Host Manager creates Huawei SingleCLOUD entities as VHM models (see definition on page 270).

Later, you can install an SNMP agent on any Huawei SingleCLOUD Host or virtual machine and upgrade its modeling in CA Spectrum. Options for upgrading to SNMP models are as follows:

- Upgrade only selected devices (see page 240)—This method works quickly when you have a small selection of models to upgrade. The VHM models are deleted first. One drawback of this method is that after CA Spectrum deletes the models, you must wait for the next Huawei SingleCLOUD Discovery to create the new SNMP models and place them in Virtual Host Manager. Knowledge of the IP addresses for the models to upgrade is required.

- Upgrade all SNMP-capable VHM models (see page 241)—This method upgrades models in batch, and this method is preferred when upgrading Virtual Host Manager to a new release. Knowledge of the IP addresses of individual models is not required. Another advantage is that after CA Spectrum deletes the VHM models, the upgraded SNMP models are immediately placed in the Virtual Host Manager hierarchy without waiting for the next polling cycle. Therefore, Virtual Host Manager manages the models more quickly.

  One drawback of this method is that it can take a long time to complete. The time required to complete this upgrade depends on how many community strings and SNMP ports Virtual Host Manager must search when locating SNMP-capable devices.

  Note: Virtual Host Manager attempts to identify SNMP agents on powered-up pingable devices only.

Important! When models are deleted, all notes or other customizations on those models are lost.

Upgrade Selected VHM Models to SNMP Models

When an SNMP agent is not available or SNMP Discovery is disabled during Huawei SingleCLOUD Discovery, Virtual Host Manager creates Huawei SingleCLOUD Hosts and Virtual Machines as VHM models (see definition on page 270). Later, you can install an SNMP agent on these devices and upgrade their modeling in CA Spectrum. You must know the IP addresses for the device models to upgrade. Manually selecting models to upgrade works quickly, but all notes or customizations on these models are lost during the upgrade.

Follow these steps:

1. Deploy or enable an SNMP agent on the device, if required.
2. Model the device again using one of the following methods:
   - CA Spectrum Discovery
   - Model individual devices by IP address

   When the new SNMP-capable model is created, CA Spectrum removes the previous model from Virtual Host Manager and deletes it. At the next Huawei SingleCLOUD Manager polling cycle, CA Spectrum adds the SNMP-capable model to Virtual Host Manager in the Navigation panel.

   Important! When models are deleted, all notes or other customizations on those models are lost.

Upgrade All VHM Models to SNMP Models

When an SNMP agent is not available or SNMP Discovery is disabled during Huawei SingleCLOUD Discovery, Virtual Host Manager creates Huawei SingleCLOUD Hosts and Virtual Machines as VHM models (see definition on page 270). Later, you can install an SNMP agent on these devices and upgrade their modeling in CA Spectrum. When upgrading in batch, CA Spectrum searches your VHM models, and locates SNMP-capable devices. Then CA Spectrum converts these to SNMP models. This method can take a long time to complete, depending on how many community strings and ports Virtual Host Manager must search.

Follow these steps:

1. Deploy or enable an SNMP agent on your devices, as required.
2. Open Virtual Host Manager in the Navigation panel.

   The main details page opens in the Contents panel for the selected Virtual Host Manager.
3. Select the Huawei SingleCLOUD Manager model in the Navigation panel that manages the models to upgrade.
4. Click the Information tab.
5. Expand the Huawei SingleCLOUD Manager, CA Spectrum Modeling Control subview.
6. Click the Upgrade ICMP-Only Devices button.

   Important! When models are deleted, all notes or other customizations on those models are lost.

   Virtual Host Manager searches for VHM models that are managed by the Huawei SingleCLOUD Manager. Virtual Host Manager upgrades the ICMP-only devices that meet the criteria for SNMP devices and places them within the Virtual Host Manager hierarchy.

Move a Huawei SingleCLOUD Host to a Different Huawei SingleCLOUD GalaX

Moving a Huawei SingleCLOUD Host from management by one Huawei SingleCLOUD GalaX to another can cause problems with CA Spectrum modeling when both Huawei SingleCLOUD Managers are modeled on the same SpectroSERVER.

Some possible symptoms of these modeling problems are as follows:

- CA Spectrum deletes the models associated with the host but does not recreate them after the move.
- False Proxy Lost alarms are created and remain, even though the new managing Huawei SingleCLOUD GalaX can contact the host and all hosted virtual machines.

To avoid these problems, perform the steps to move your host and reflect the changes in your modeled CA Spectrum environment in the correct order, as follows.

Follow these steps:

1. (Optional) Change the 'Allow Device Model Deletes During Huawei SingleCLOUD Discovery' option to No (see page 231).

   Note: Perform this step only if both the originating and destination Huawei SingleCLOUD Managers are modeled in the same SpectroSERVER. Setting this option to No keeps the existing Huawei SingleCLOUD Host, CNA FIP, and Virtual Machine models from being deleted when they become unmanaged by the first Huawei SingleCLOUD GalaX. Therefore, customizations or historical details for the models are preserved and available after the move.

2. Use Huawei SingleCLOUD GalaX to remove the host from management.

3. Wait for Virtual Host Manager to reflect the changes in the Navigation panel.

4. Use the destination Huawei SingleCLOUD GalaX to add management of the host.

   Note: Virtual Host Manager is not DSS (see definition on page 268) aware. Therefore, when moving the host to a Huawei SingleCLOUD GalaX managed on a different SpectroSERVER, a new set of models are created to represent the host, CNA FIP, and virtual machines.

5. (Optional) Change the 'Allow Device Model Deletes During Huawei SingleCLOUD Discovery' option back to Yes (see page 231).

   The host is successfully moved from management by one Huawei SingleCLOUD GalaX to another and accurately reflected in the CA Spectrum modeled environment.

Viewing Your Huawei SingleCLOUD Virtual Environment

This section describes concepts for viewing your Huawei SingleCLOUD virtual environment. The basic steps are no different from the standard CA Spectrum procedures. However, this section describes conceptual differences and details that only apply to the Huawei SingleCLOUD platform.

Viewing Your Huawei SingleCLOUD Virtual Network

On the Explorer tab under the Virtual Host Manager node, the expanded Huawei SingleCLOUD folder displays a hierarchical tree structure that helps you visualize the logical organization of your managed Huawei SingleCLOUD environment.

Using this information, you can see how resources are shared across your Huawei SingleCLOUD Managers, which can help you identify opportunities to reorganize and optimize your virtual environment. This hierarchy also provides a quick way to validate the appropriate status of allocated resources in your cloud architecture, monitor performance, and troubleshoot alarms.

Because Virtual Host Manager is not aware of a DSS environment (see definition on page 268), it is located within a landscape hierarchy. The following diagram shows where Virtual Host Manager appears on the Explorer tab in the Navigation panel and illustrates the Huawei SingleCLOUD hierarchy:

```
[-] SpectroSERVER host
    [+] Universe
    [-] Virtual Host Manager
        [-] Huawei SingleCLOUD
            [+] Huawei SingleCLOUD CAMM Presenter 1
            [-] Huawei SingleCLOUD CAMM Presenter 2
                [-] Huawei SingleCLOUD Manager 1
                     [+] Huawei SingleCLOUD Cloud 1
                     [-] Huawei SingleCLOUD Cloud 2
                         [+] Huawei SingleCLOUD Host 1
                         [-] Huawei SingleCLOUD Host 2
                             . Huawei SingleCLOUD CNA FIP
                             . Huawei SingleCLOUD Virtual Machine 1
                             . Huawei SingleCLOUD Virtual Machine 2
                [+] Huawei SingleCLOUD Manager 2
                [+] Huawei SingleCLOUD Manager 3
```

Virtual Host Manager is the root node for the entire virtual environment managed by this SpectroSERVER. Selecting this node in the Navigation panel displays Virtual Host Manager details in the Contents panel. You can view details such as events and alarms related to your virtual environment as a whole.

Directly under Virtual Host Manager, virtual environments are organized within folders that represent the technology with which they are created. In the example hierarchy above, the Huawei SingleCLOUD folder contains the portion of the virtual environment that was created and managed by Huawei SingleCLOUD. In this folder, Virtual Host Manager lists all CAMM Presenters, Huawei SingleCLOUD Managers, and clouds managed by this SpectroSERVER. Each Huawei SingleCLOUD Manager contains only the portion of the virtual environment that it manages.

The hierarchy represents the logical relationships between the following virtual entities:

- **Huawei SingleCLOUD CAMM Presenter**

  A Huawei SingleCLOUD CAMM Presenter node groups together all of the Huawei SingleCLOUD Managers that it manages. Selecting a CAMM Presenter provides access to the Huawei SingleCLOUD Managers subview, where you define the Huawei SingleCLOUD Managers managed by the Presenter by specifying the virtual IP addresses used to communicate with Huawei SingleCLOUD GalaX. Selecting the CAMM Presenter node also displays events and alarms related to the entities in its managed environment. A Physical Host Down alarm generated on the Huawei SingleCLOUD CAMM Presenter model indicates that all the Huawei SingleCLOUD Managers (virtual IP addresses) it manages have gone down.

- **Huawei SingleCLOUD Manager**

  A Huawei SingleCLOUD Manager represents the virtual IP address used by CAMM to communicate with the Huawei SingleCLOUD GalaX. CA Spectrum uses the virtual IP address to obtain information from the Huawei SingleCLOUD GalaX about the Huawei SingleCLOUD environment it manages. Selecting a Huawei SingleCLOUD Manager displays information about its managed environment, such as details about the GalaX OMMs, managed clouds, hosts, and virtual machines, including when data in the MIB was updated last. Traps received from the Huawei SingleCLOUD trap service are generated on the Huawei SingleCLOUD Manager model.

- **Huawei SingleCLOUD Cloud**

  A Huawei SingleCLOUD Cloud is the name of the managed cloud as defined in the Huawei SingleCLOUD platform. Selecting a Huawei SingleCLOUD Cloud displays details about the cloud, including:

  - Cloud type (public or private).
  - MIB-related status information, including when data for the cloud was updated last and how much time is expected between updates.

  In the hierarchy, beneath each cloud are the Huawei SingleCLOUD Hosts associated with the cloud.

- **Huawei SingleCLOUD Host**

  A Huawei SingleCLOUD Host is a CNA that hosts virtual machines. In the hierarchy, beneath each host are the CNA FIP and the virtual machines it manages. A Huawei SingleCLOUD Host can be part of a public or private cloud.

  Selecting the Huawei SingleCLOUD Host displays detailed host information including:

  - Cloud type (public or private) that the host is a part of.
  - Resources consumed by the CNA process, such as storage, CPU, and memory utilization.
  - Geographical information of the host for quick physical location during fault resolution.
  - MIB-related status information, including when data for the host was updated last and how much time is expected between updates.

  Note: Available host information differs depending on if the host is part of a public or private cloud. The cloud type is identified in the Host Information, CNA, Properties subview.

- **Huawei SingleCLOUD CNA FIP**

  The Huawei SingleCLOUD CNA FIP is the management interface to the hosted virtual machines. The model appears as a child to its corresponding Huawei SingleCLOUD Host model and is always a leaf node on the Virtual Host Manager hierarchy tree.

  Note: The Huawei SingleCLOUD CNA FIP model is the only Huawei SingleCLOUD model type that does not provide a Virtual Host Manager-specific subview on the Information tab.

- **Huawei SingleCLOUD Virtual Machine**

  A virtual machine is always a leaf node on the Virtual Host Manager hierarchy tree. Selecting a virtual machine displays details including:

  - Identifying information, such as IP address and MAC address.
  - Resource information, including storage, CPU, and memory utilization.
  - MIB-related status information, including when data for the virtual machine was updated last and how much time is expected between updates.

More information:

Models Created for Huawei SingleCLOUD (see page 226)
CAMM MIB Updates (see page 247)

Understanding the Huawei SingleCLOUD Virtual Topology

The Huawei SingleCLOUD Host, CNA FIP, and Virtual Machine models created for your virtual environment are integrated into the topology view. Huawei SingleCLOUD Host models automatically group their associated CNA FIP and Virtual Machine models. The topology shows how these elements are connected to your physical network entities.

The following example shows how these models can appear on the Explorer tab in the Navigation panel under the Universe group:

```
[-] Universe
    [-] Huawei SingleCLOUD Host
          .  Huawei SingleCLOUD CNA FIP
          .  Huawei SingleCLOUD Virtual Machine 1
          .  Huawei SingleCLOUD Virtual Machine 2
          .  Huawei SingleCLOUD Virtual Machine 3
```

Selecting one of these models displays these relationships graphically on the Topology tab in the Contents panel.

How the Huawei SingleCLOUD Data is Updated in Virtual Host Manager

During your initial Huawei SingleCLOUD Discovery, CA Spectrum populates the Virtual Host Manager hierarchy in the Navigation panel with your virtual device models. After CA Spectrum builds this initial hierarchy, your virtual network configuration can change, and Virtual Host Manager must continually work to keep this information accurate in CA Spectrum. For example, the following events can change your virtual network configuration:

- Creating or deleting clouds, hosts, or virtual machines
- Moving a virtual machine from one Huawei SingleCLOUD host to another

To keep your information accurate, Virtual Host Manager detects these changes by polling the CAMM Presenter to retrieve information about the virtual environment from the CAMM MIB. Accordingly, your virtual network configuration is updated in CA Spectrum at each polling cycle. Because of the communication with Huawei SingleCLOUD GalaX, CA Spectrum is aware of spontaneous network configuration changes (such as migrations and host outages), which are quickly reflected in OneClick and factored into the root cause analysis.

When CA Spectrum detects a change in your virtual network configuration, CA Spectrum performs the following tasks:

- Updates the placement of your virtual device models in the Virtual Host Manager hierarchy of the Navigation panel
- *Automatically* rediscovers connections to the affected models and associates them with the correct Huawei SingleCLOUD Host in the Universe topology

  Important! To reestablish connections to your virtual models correctly, all interconnecting routers and switches in your physical network must be modeled. If these models do not exist before connections to your virtual devices are rediscovered, CA Spectrum cannot resolve those connections and display the information correctly in the Universe topology view.

In addition to polling-based events, CA Spectrum also supports traps from the Huawei SingleCLOUD trap service and generates corresponding events. By reviewing the event log, you can find out when configuration changes occur, such as when a virtual machine is created or migrated.

More information:

CAMM MIB Updates (see page 247)

CAMM MIB Updates

CA Spectrum retrieves information about the Huawei SingleCLOUD environment from the CAMM MIB. To keep the modeling in CA Spectrum accurate, the data in the MIB must be up-to-date.

CAMM obtains data from Huawei SingleCLOUD GalaX and updates the MIB according to a configured poll rate in the CAMM Engine. CA Spectrum uses SNMP to retrieve data from the MIB according to the poll interval specified on the Huawei SingleCLOUD Manager model.

You can determine when CAMM last updated the MIB and when it is expected to be updated again by using the custom subviews for various Huawei SingleCLOUD entity models, where the following MIB-related status information fields are provided:

Last Updated

Displays when the MIB was last updated. This timestamp value is updated by CAMM when information about the respective entity is obtained from Huawei SingleCLOUD GalaX. You can use this value to determine how current the MIB information for the entity is.

Expected Update Delta (s)

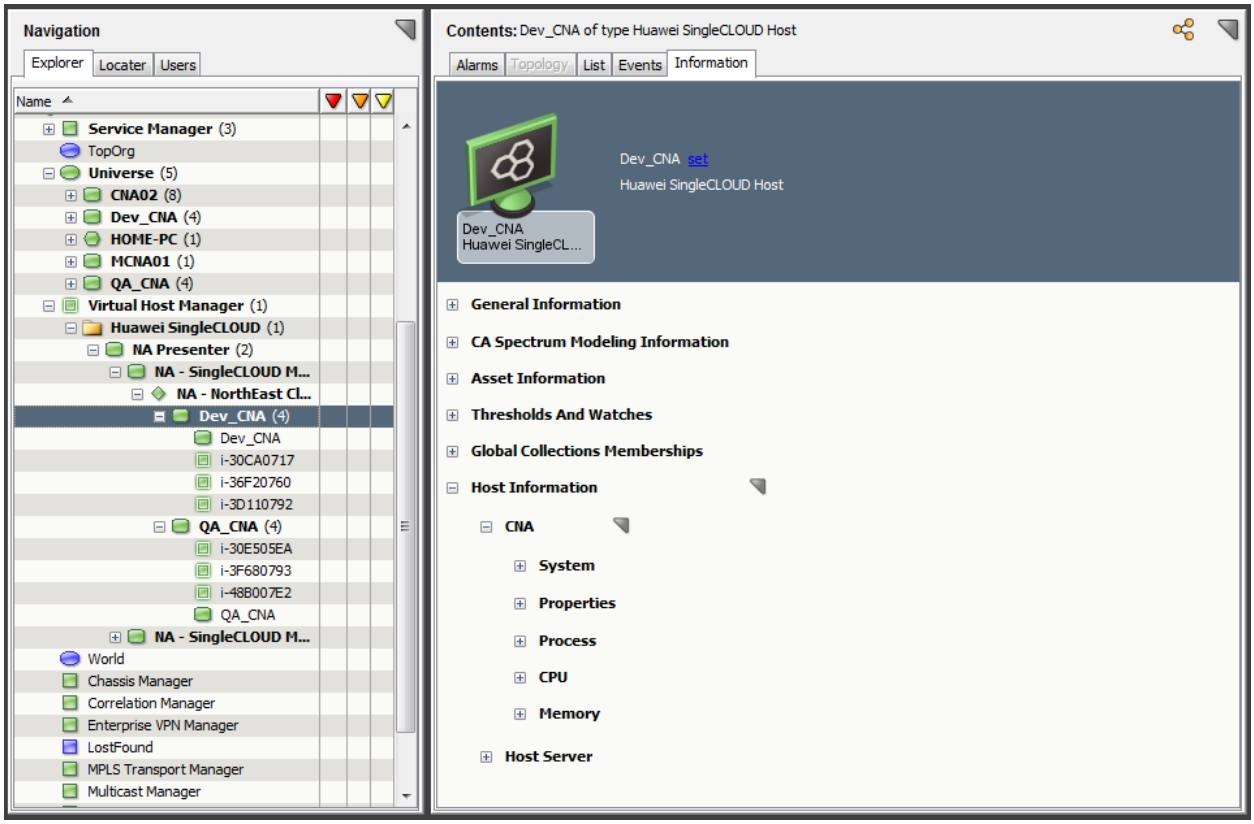
Displays the expected amount of time between MIB updates, in seconds. If a host or virtual machine has not been updated within the expected amount of time, a Proxy Lost alarm is generated to indicate that updated information cannot be obtained for the entity.

More information:

How Virtual Host Manager Works with Huawei SingleCLOUD (see page 225)
Viewing Your Huawei SingleCLOUD Virtual Environment (see page 242)
How Fault Isolation Works when Proxy Management is Lost (see page 257)

Custom Subviews

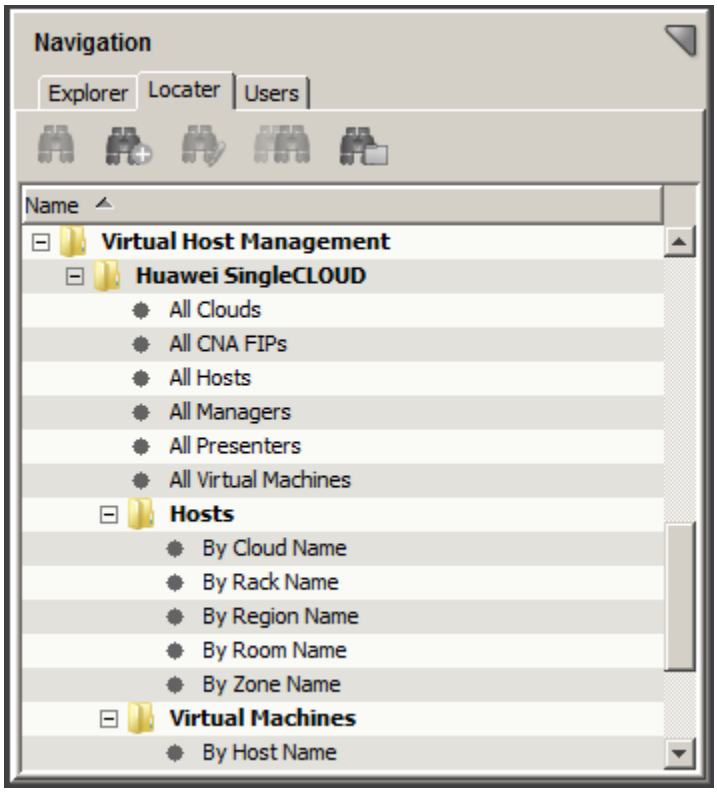
Your Virtual Host Manager models collectively provide information about your virtual environment. Individually, each model provides unique information or configuration settings, depending on the virtual entity type it represents. Custom subviews appear on the Information tab in the Contents panel. These subviews can contain real-time data, such as CPU status or memory utilization. For example, the custom subview for a Huawei SingleCLOUD Host model is the Host Information subview, which provides details specific to a host, as shown:



Note: The Huawei SingleCLOUD Manager model provides combined information for all virtual devices managed by the Huawei SingleCLOUD Manager. Selecting the Huawei SingleCLOUD Manager model in the Navigation panel displays unique information, such as about the Huawei SingleCLOUD GalaX OMMs, as well as combined information about all Huawei SingleCLOUD clouds, hosts, and virtual machines it manages. This information contains some of the same data that is displayed on the Information tab for each individual entity model. The combined view in the Huawei SingleCLOUD Manager model can provide a good overview about all of the virtual entities it manages.

Locater Tab for Huawei SingleCLOUD Searches

In addition to viewing details about your virtual environment on the Explorer tab, you can also use the Locater tab to run preconfigured searches. The search options are grouped under the Virtual Host Management, Huawei SingleCLOUD folder on the Locater tab, as shown:



These detailed searches can help you investigate information related to Huawei SingleCLOUD entities that have been modeled in the CA Spectrum database.

Note: Although Virtual Host Manager is not DSS (see definition on page 268) aware, these preconfigured searches let you select multiple landscapes to search in the search parameters.

The following types of searches are provided for Huawei SingleCLOUD:

Huawei SingleCLOUD

Locates Huawei SingleCLOUD entities that have been modeled in the CA Spectrum database by model type. These include:

- All Clouds
- All CNA FIPs
- All Hosts
- All Managers
- All Presenters
- All Virtual Machines

Hosts

Locates Huawei SingleCLOUD Hosts by cloud name or geographic location (rack, region, room, and zone).

Virtual Machines

Locates all virtual machines that reside on a particular Huawei SingleCLOUD Host.

Deleting Virtual Host Manager Models

Models can be deleted from OneClick at any time for various reasons. However, Virtual Host Manager restricts your ability to delete models from the Virtual Host Manager hierarchy in the Navigation panel. To delete models manually, you have the following options:

- Delete the Huawei SingleCLOUD folder, a Huawei SingleCLOUD Presenter model, or a Huawei SingleCLOUD Manager model in Virtual Host Manager
- Remove a virtual entity using Huawei SingleCLOUD GalaX

In Virtual Host Manager, models are sometimes deleted automatically. The following circumstances cause CA Spectrum to automatically delete Virtual Host Manager models:

- **The Huawei SingleCLOUD folder, a Huawei SingleCLOUD CAMM Presenter model, or a Huawei SingleCLOUD Manager model is deleted**

  If you delete the Huawei SingleCLOUD folder, a Huawei SingleCLOUD CAMM Presenter model, or a Huawei SingleCLOUD Manager model from the Navigation panel, CA Spectrum deletes all related child models. For the CAMM Presenter model, this includes all virtual IP addresses.

- **An entity is removed from a Huawei SingleCLOUD virtual environment**

  As you delete Huawei SingleCLOUD hosts and virtual machines using Huawei SingleCLOUD GalaX, CA Spectrum also deletes those models and their child models from Virtual Host Manager.

- **Upgraded models exist.**

  In some cases, a virtual machine is first modeled for Virtual Host Manager without SNMP capabilities. If SNMP capabilities are later added to a VHM model (see definition on page 270), the previous model is deleted and replaced with the new SNMP-capable model.

Note: Although the default setting is to delete the models, you can configure Virtual Host Manager to place the Huawei SingleCLOUD Host and Huawei SingleCLOUD Virtual Machine models in the LostFound container when they are removed from Virtual Host Manager. This configuration setting applies only when you remove an entity using Huawei SingleCLOUD GalaX. However, this setting does not apply when you delete the Huawei SingleCLOUD folder, delete a Huawei SingleCLOUD Manager model, or upgrade a VHM model.

Alarms and Fault Isolation for Huawei SingleCLOUD

To alert you to problems within your virtual network, CA Spectrum generates alarms. Quickly identifying any device faults helps you to maximize system up-time and the reliability of your cloud architecture. Alarms are created by:

- Traps sent from Huawei SingleCLOUD (see page 251).
- Polling. Alarms are generated for the following conditions:
  - A Huawei SingleCLOUD Manager (proxy) is down or communication is lost.
  - A Huawei SingleCLOUD virtual machine is not running.
  - CAMM has not been updated within the defined poll rate.
  - A virtual machine has moved to a new Huawei SingleCLOUD Host.
  - An unsupported Virtual Host Manager configuration has been encountered.

  Alarms that are generated from polling are described in Fault Management for Huawei SingleCLOUD (see page 253).

Traps for Huawei SingleCLOUD

Traps are generated by the Huawei SingleCLOUD trap service and identify events related to configuration changes, process status, disk or memory usage, and power supply or fan status, as well as others. Traps are generated on the Huawei SingleCLOUD Manager model and can generate alarms in CA Spectrum.

This section includes the following topics:

- Traps and Alarm Severity for Huawei SingleCLOUD (see page 252)
- Supported Traps for Huawei SingleCLOUD (see page 252)

Traps and Alarm Severity for Huawei SingleCLOUD

If a trap is received and generates an alarm, CA Spectrum uses the value of the “state” varbind passed with the trap to determine the alarm severity. CA Spectrum maps these Huawei SingleCLOUD states to a CA Spectrum alarm severity, as shown:

Huawei SingleCLOUD State	CA Spectrum Alarm Severity
0: Warning	Minor (Yellow)
1: Minor	Minor (Yellow)
2: Major	Major (Orange)
3: Critical	Critical (Red)

Supported Traps for Huawei SingleCLOUD

The following tables provide the supported Huawei SingleCLOUD traps and their respective trap types. The value of the OID suffix (the lowest node in the trap OID) indicates the trap type.

Huawei SingleCLOUD Trap Types

OID Suffix	Trap Type
.1	Set
.2	Update
.3	Clear

Huawei SingleCLOUD Traps

Trap Name	Trap OID
Config Management Agent Process Abnormal	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
Occupied Space in the Directory Too High	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 Node Disk Usage Above the Threshold	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

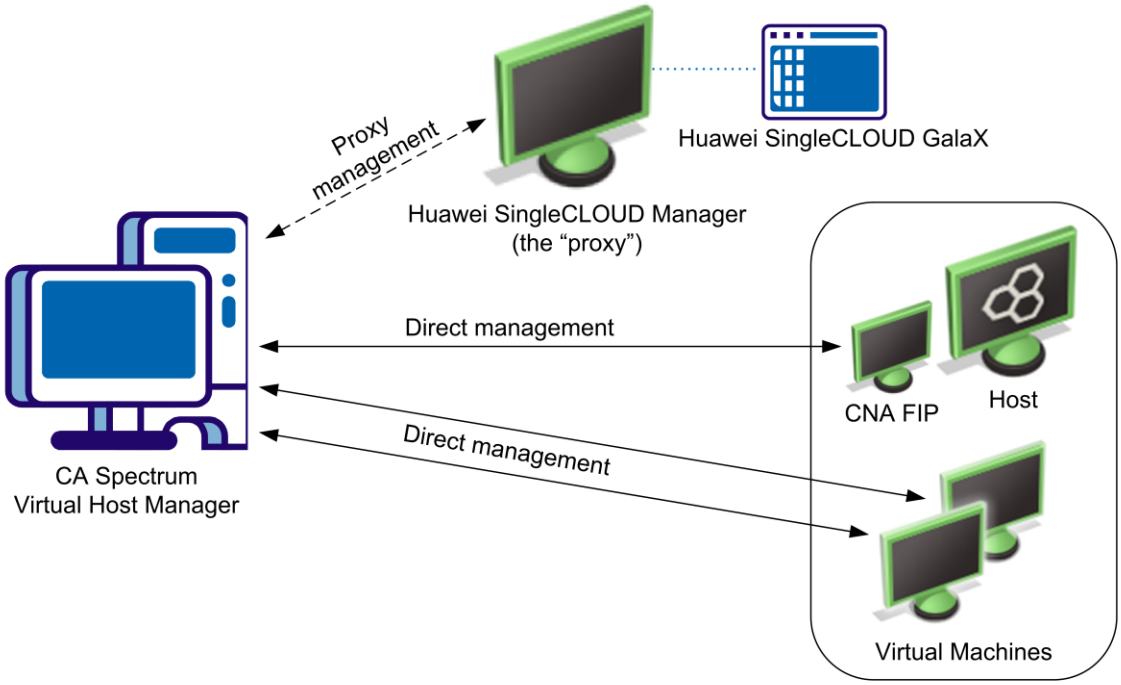
Trap Name	Trap OID
Hard Disk Lost	1.3.6.1.4.1.60001.10.1.15.1000202.6.1 1.3.6.1.4.1.60001.10.1.15.1000202.6.2 1.3.6.1.4.1.60001.10.1.15.1000202.6.3
VM MEM Usage Over the Threshold	1.3.6.1.4.1.60001.10.1.15.1000102.6.1 1.3.6.1.4.1.60001.10.1.15.1000102.6.2 1.3.6.1.4.1.60001.10.1.15.1000102.6.3
Fan Status Abnormal	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
Controller Node Hard Disk Usage Above the Threshold	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
Power Supply Status Abnormal	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

Fault Management for Huawei SingleCLOUD

The goal of fault isolation is to narrow down the root cause of a networking problem. Finding the root cause can help you to troubleshoot and quickly correct the problem or to correct the problem programmatically with automated scripts. Deciding which device is the root cause of an alarm can be difficult, because problems with a single device can cause several devices in your network to generate events.

For example, losing contact with a Huawei SingleCLOUD Host often means that you have also lost contact with the virtual machines it manages. Therefore, the Huawei SingleCLOUD Host model and all affected virtual machines generate alarms. Using fault isolation techniques, Virtual Host Manager correlates these alarms in an attempt to identify a single root cause.

Virtual networks provide a unique management opportunity because they provide CA Spectrum an alternate management perspective. That is, CA Spectrum can gather information through direct contact with your virtual devices or through CAMM, which communicates with Huawei SingleCLOUD GalaX.



This alternate management perspective enhances standard CA Spectrum fault management in two ways:

- **Enhanced Contact Lost alarms**—Two sources of information about a device means Virtual Host Manager can pinpoint the cause and more easily correlate events to a single root cause.
- **Proxy Failure alarms**—Proxy management is the act of managing network devices using an alternate management source in place of or in addition to the primary manager. For example, CA Spectrum can manage Huawei SingleCLOUD virtual machines by contacting them directly or through CAMM, which obtains data from Huawei SingleCLOUD GalaX. When the Huawei SingleCLOUD Manager loses contact with Huawei SingleCLOUD GalaX or when Huawei SingleCLOUD GalaX loses contact with a virtual device, Virtual Host Manager generates one of the proxy management alarms for each device. These alarms alert you to the fact that *management* of the device through the *proxy* is affected, not the state of the device or direct (SNMP) management.

The following sections provide additional information about what to expect when contact with a device or proxy is lost.

More information:

How Fault Isolation Works when Device Contact is Lost (see page 255)
How Fault Isolation Works when Proxy Management is Lost (see page 257)

How Fault Isolation Works when Device Contact is Lost

To help you troubleshoot networking problems with your devices, CA Spectrum uses fault isolation to narrow down the root cause of an alarm. For virtual networks, Virtual Host Manager uses information from direct contact with the device plus information provided by Huawei SingleCLOUD GalaX through CAMM. In many cases, standard CA Spectrum fault management can pinpoint the root cause. But in special circumstances, the approach for isolating problems in a virtual network goes beyond the standard methods.

The type of fault isolation Virtual Host Manager uses to discover the root cause depends on which devices are alarming and the type of events the devices generate. The following scenarios describe fault management situations and how CA Spectrum isolates the networking error in your virtual network.

Scenario 1: Huawei SingleCLOUD Virtual Machine is not running

In a virtual environment, the virtual management application can provide more details than CA Spectrum can discover through standard device monitoring. For example, Huawei SingleCLOUD GalaX is aware when a virtual machine changes from the running state to another state.

If a virtual machine is no longer running and CA Spectrum loses contact with it, but proxy management (see definition on page 269) of the virtual machine is uninterrupted, CA Spectrum determines the root cause as follows:

1. When CA Spectrum loses contact with a virtual machine, it generates a Contact Lost alarm.
2. During its next polling cycle, the Huawei SingleCLOUD Manager model polls CAMM, which communicates with Huawei SingleCLOUD GalaX, to gather information about the virtual machine. Because Huawei SingleCLOUD GalaX manages the virtual machines, it can provide a unique view into the possible cause of alarms generated by the virtual machine.
3. If Huawei SingleCLOUD GalaX indicates that the virtual machine is in the not-running mode, it generates a Huawei SingleCLOUD Not Running alarm.

   Note: This alarm is cleared during the poll cycle after which CAMM determines the virtual machine is running again.
4. Virtual Host Manager correlates the Contact Lost alarm to the corresponding Huawei SingleCLOUD Not Running alarm created by CA Spectrum. Virtual Host Manager makes the Contact Lost alarm appear as a symptom of the Huawei SingleCLOUD Not Running alarm.

Scenario 2: Huawei SingleCLOUD Host is down

If CA Spectrum loses contact with all virtual machines running on a Huawei SingleCLOUD Host, CA Spectrum checks the status of the upstream routers and switches. Depending on their status, CA Spectrum determines the root cause as follows:

- **When all upstream devices for one or more Huawei SingleCLOUD Virtual Machines are unavailable**

  Standard CA Spectrum fault isolation techniques are used to determine the root cause:

  - A Gateway Unreachable alarm is generated on the Huawei SingleCLOUD Host when *all* upstream connected devices are down.

- **When at least one upstream device is available for every virtual machine connected to the Huawei SingleCLOUD Host**

  CA Spectrum infers that the Huawei SingleCLOUD Host is the root cause and responds as follows:

  a. All Huawei SingleCLOUD virtual machines, ports, and fanouts that are directly connected to the Huawei SingleCLOUD Host models generate the standard fault isolation alarms.

  b. Virtual Host Manager creates a Physical Host Down alarm for the Huawei SingleCLOUD Host model.

  c. All fault isolation-related alarms that are created for the impacted devices (such as virtual machines, ports, and fanouts) are correlated to the Physical Host Down alarm, making them symptoms of the Physical Host Down alarm. These symptom alarms appear in the Symptoms table on the Impact tab for the Physical Host Down alarm.

     Note: For each Huawei SingleCLOUD Host model, Virtual Host Manager creates a "virtual fault domain." This domain includes the Huawei SingleCLOUD Host, CNA FIP, and Virtual Machines, plus all ports and fanouts directly connected to the Huawei SingleCLOUD Hosts. When the Huawei SingleCLOUD Host generates the Physical Host Down alarm, all standard fault isolation alarms within the domain are correlated to it. Correlating these alarms as symptoms indicates that the Physical Host Down alarm on the Huawei SingleCLOUD Host is the root cause.

d. All impacted devices are listed in the Management Lost Impact table on the Impact tab for the Physical Host Down alarm.

   Note: Devices that are suppressed do not have a corresponding alarm in the Symptoms table.

   For more information about using the Impact tab for alarm information, see Determining Virtual Machines Affected by Host Outages (see page 259).

e. If all upstream devices for one or more virtual machines go down, CA Spectrum can no longer reliably state that the fault lies with the Huawei SingleCLOUD Host. CA Spectrum clears the Physical Host Down alarm and applies the standard CA Spectrum fault isolation techniques.

How Fault Isolation Works when Proxy Management is Lost

Huawei SingleCLOUD GalaX, which is used to create your virtual network, provides CA Spectrum a unique management opportunity. CA Spectrum can use the standard methods to contact your virtual devices directly, plus CA Spectrum can simultaneously gather virtual device information from CAMM with the Huawei SingleCLOUD Device Pack, which communicates with Huawei SingleCLOUD GalaX. In this sense, CAMM is a "proxy" from which CA Spectrum gathers virtual device information. If CA Spectrum loses direct contact with a device, it generates alarms. Likewise, if CAMM loses contact with a virtual device (by way of Huawei SingleCLOUD GalaX) or if Virtual Host Manager loses contact with CAMM, Virtual Host Manager generates alarms—proxy management alarms (see definition on page 269).

In response, CA Spectrum attempts to isolate the cause of the proxy management failure. Proxy fault isolation is similar to the standard CA Spectrum fault isolation, except that these alarms alert you to the fact that *proxy* management of a virtual device is affected. Proxy management fault isolation cannot tell you whether a virtual device is up or down. However, it is important to know when contact through the proxy is lost, because you could be missing important virtual information about a device.

The type of proxy fault isolation Virtual Host Manager uses to discover the root cause depends on which devices are alarming and the type of events the devices generate. The following scenarios describe proxy fault management situations and how Virtual Host Manager isolates the networking error in your virtual network.

Scenario 1: Contact between CA Spectrum and CAMM (Huawei SingleCLOUD Manager) is lost

If CA Spectrum loses contact with or stops polling the Huawei SingleCLOUD Manager model, CA Spectrum cannot obtain updated Huawei SingleCLOUD GalaX data about all virtual models managed by that Huawei SingleCLOUD Manager. To isolate the problem, Virtual Host Manager determines the root cause as follows:

1. CA Spectrum generates Proxy Lost alarms for all virtual models managed by that Huawei SingleCLOUD Manager, including Huawei SingleCLOUD Clouds, Hosts, CNA FIPs, and Virtual Machines. CA Spectrum also generates a separate Manager Unavailable alarm on the Huawei SingleCLOUD Manager model.
2. The Huawei SingleCLOUD alarms are correlated to their corresponding Huawei SingleCLOUD Host model alarm.
3. The Huawei SingleCLOUD Cloud and Host model alarms are correlated to a Proxy Unavailable alarm for the Huawei SingleCLOUD Manager model.
4. This Proxy Unavailable alarm is then correlated to the root cause of the Huawei SingleCLOUD Manager being down. The root cause is typically an alarm generated by standard CA Spectrum fault management, such as the alarms created for the following situations:
   - Lost management of Huawei SingleCLOUD Manager (that is, a problem occurred with CAMM)
   - Machine contact is lost
   - Huawei SingleCLOUD Manager model is in maintenance mode

Scenario 2: Contact between CAMM and Huawei SingleCLOUD GalaX is lost

If CAMM is not updated within a certain amount of time, the Huawei SingleCLOUD platform data reported by CAMM may not be current. Using a heartbeat indicator and the configured poll rate, CA Spectrum can identify when a managed Huawei SingleCLOUD entity was last updated.

When a Huawei SingleCLOUD Host or Virtual Machine has not been updated within the configured amount of time, Virtual Host Manager determines that the CAMM is unable to contact Huawei SingleCLOUD GalaX. Proxy Lost alarms are generated on the Huawei SingleCLOUD Host, CNA FIP and Virtual Machine models managed by this Huawei SingleCLOUD Manager. When multiple elements have not been updated, CA Spectrum correlates these alarms to the appropriate root cause (for example, multiple virtual machine alarms correlated to a host). In addition, when none of the virtual IPs associated with the CAMM Presenter can be contacted, a Physical Host Down alarm is generated on the Huawei SingleCLOUD CAMM Presenter model. Identifying information for the faulting CAMM Engines and the time since the last successful communication is provided in the alarm text.

Scenario 3: Contact between Huawei SingleCLOUD GalaX and Huawei SingleCLOUD Host is lost

If Huawei SingleCLOUD GalaX loses contact with one of the Huawei SingleCLOUD Hosts it is managing, the proxy data about the host and all hosted virtual devices is lost. To isolate the problem, Virtual Host Manager determines the root cause as follows:

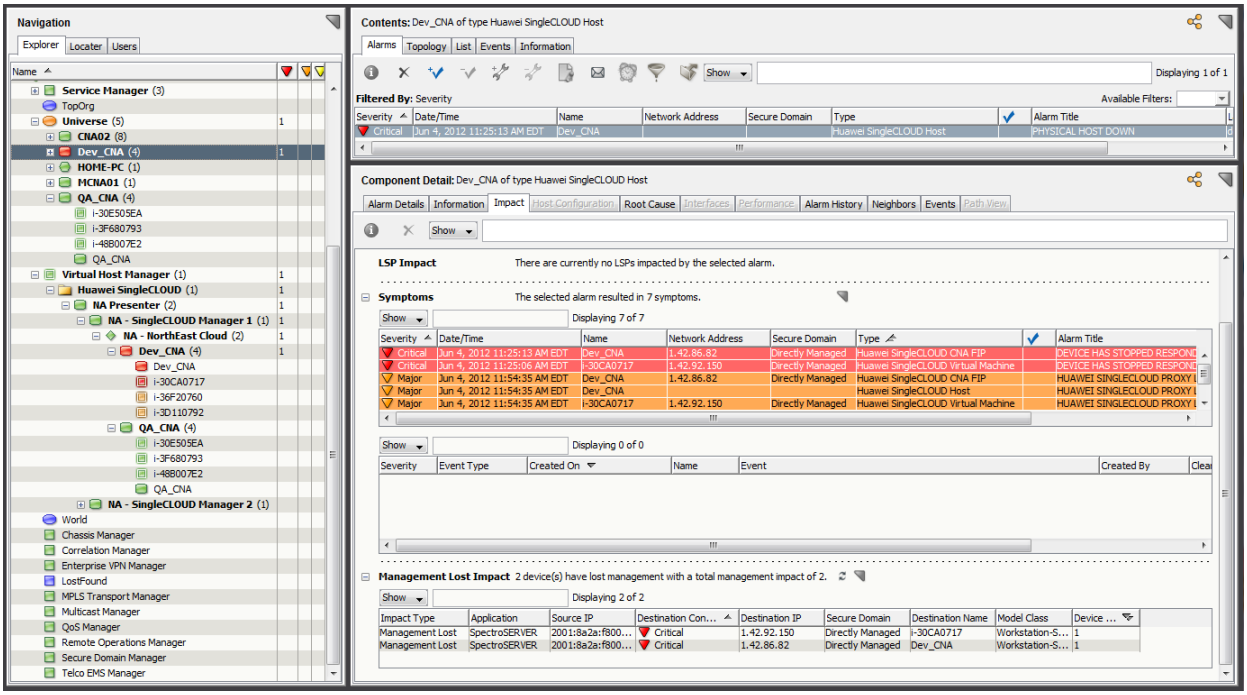
1. A Proxy Lost alarm is generated on the Huawei SingleCLOUD Host, CNA FIP, and all hosted virtual machines.
2. The CNA FIP and virtual machine alarms are correlated to the Proxy Lost alarm for the Huawei SingleCLOUD Host, making these alarms symptoms of the Huawei SingleCLOUD Host alarm. Correlating these alarms as symptoms indicates that the Huawei SingleCLOUD Host alarm is the root cause.
3. If CA Spectrum also loses contact with the Huawei SingleCLOUD Host and generates a Physical Host Down alarm, the Proxy Lost alarm generated for the Huawei SingleCLOUD Host is correlated to the Physical Host Down alarm. In this case, the Proxy Lost alarm becomes a symptom of the Physical Host Down alarm. Correlating this alarm as a symptom indicates that the Physical Host Down alarm on the Huawei SingleCLOUD Host is the root cause.

Determining Virtual Machines Affected by Host Outages

When contact with a Huawei SingleCLOUD Host is interrupted or the Huawei SingleCLOUD Host goes down, all virtual machines hosted by the Huawei SingleCLOUD Host are affected. Because the Huawei SingleCLOUD Manager cannot communicate with the Huawei SingleCLOUD Host to get usage information, you might not receive alarms for a critical virtual machine hosted on that Huawei SingleCLOUD Host.

To find out if a critical virtual machine is impacted, you can view a list of affected virtual machines on the Impact tab of the alarm, as follows:

- Symptoms subview—displays all symptom alarms generated by the affected virtual machines
- Management Lost Impact subview—lists the virtual machines impacted by the alarm



Appendix A: Troubleshooting

This section describes common symptoms or issues that can occur when using Virtual Host Manager and our recommended solution.

Duplicate Models Created After SNMP and vCenter Discovery

Symptom:

After I run the standard CA Spectrum Discovery on my virtual network and then let Virtual Host Manager run a vCenter Discovery, I get a Duplicate Models alarm for some of my virtual machines. Which model should I delete, and how do I prevent it from happening again?

Solution:

When modeling a virtual environment, a duplicate model can be created when a virtual machine does not have either VMware tools or an SNMP agent installed. The duplicate model is created as follows:

1. CA Spectrum Discovery models the virtual machine using a pingable model type, because the virtual machine does not have an SNMP agent installed. This model contains an IP address, but it does not contain a MAC address. The upstream router that usually looks up the MAC address for a device is not yet modeled, so the MAC address for the virtual machine cannot be resolved.
2. Virtual Host Manager runs a vCenter Discovery and finds the same virtual machine. Because the virtual machine does not have VMware tools installed, Discovery can identify a MAC address but cannot determine the IP address. Therefore, vCenter Discovery does not recognize it as the existing model created in step 1, so it creates a second model for the virtual machine. This model contains a MAC address but no IP address.
3. When CA Spectrum finds a model with no IP address, it performs an OS call using the model name to get the IP address. If the virtual machine name in vCenter matches the name returned from the OS, the OS passes the IP address of the virtual machine device to CA Spectrum. CA Spectrum sets the IP address in the model created by the vCenter Discovery—this model now contains both the MAC address and IP address.
4. The Duplicate Model alarm is triggered for each model, because they both have the same IP address.

To correct the problem, delete the virtual machine device model created by the CA Spectrum Discovery (that is, the model that contains the IP address only)—*keep the model that has both an IP and MAC address*. Otherwise, the same problem repeats the next vCenter poll cycle. If the delete affects the Virtual Host Manager hierarchy, wait one polling cycle of the vCenter server host, and the modeling is restored.

To avoid this problem when modeling your virtual environment using CA Spectrum Discovery, verify that the upstream routers for all virtual machines without VMware tools meet one of the following criteria:

- Routers have already been modeled with an SNMP-capable model type
- Routers are included in your Discovery range along with the proper SNMP credentials

By including the upstream routers, CA Spectrum attempts to resolve the physical address belonging to each host that does not have an SNMP agent.

If you model your virtual environment by modeling your VMware vCenter server by IP address and Discovery creates models without IP addresses, you must manually specify the IP for those devices before running CA Spectrum Discovery.

Duplicate Models Created After Solaris Zones Discovery

Symptom:

After I run the standard CA Spectrum Discovery on my virtual network and then let Virtual Host Manager run a Solaris Zones Discovery, I get a Duplicate Models alarm for some of my device models. Which model should I delete, and how do I prevent it from happening again?

Solution:

When modeling a Solaris Zones virtual environment, a duplicate model can be created when more than one instance of a virtual technology manager is managing a device model. For example, if both a vCenter server and a Solaris Zones Manager are managing a device, CA Spectrum creates a duplicate.

To correct this problem, verify that only one virtual technology manager within your SpectroSERVER environment is managing the device.

More information:

Deleting Virtual Host Manager Models (see page 114)

Duplicate MAC, Different IP Address Alarm Generated on Solaris Zones Models

Symptom:

CA Spectrum is generating a Duplicate MAC, Different IP Address alarm for some of my Solaris Zones Hosts and Solaris zone instances. Many of the virtual and physical NICs in my Solaris Zones technology environment share the same MAC address. Why am I getting alarms for only some of these devices, and how do I disable these alarms?

Solution:

In a Solaris Zones virtual environment, sharing a MAC address can be a common occurrence. Therefore, CA Spectrum intelligence suppresses these alarms for devices managed by Virtual Host Manager, although the event is still logged. CA Spectrum generates a Duplicate MAC, Different IP Address alarm on your Solaris Zones Host and Solaris zone devices in the following circumstances:

- **Solaris Zones Discovery has not modeled the devices, and Virtual Host Manager is not yet managing them.**
  In this case, verify that Solaris Zones Discovery is configured to model the devices. You can also adjust the polling cycle to cause modeling to occur sooner.
- **The device models were deleted from Virtual Host Manager management, but the models remain in the Universe topology.**
  To stop the alarms in this situation, place the devices back in Virtual Host Manager or delete the device models from CA Spectrum.

Duplicate Model Alarm on Huawei SingleCLOUD Models

Symptom:

CA Spectrum has generated a Duplicate Model Detected alarm for some of my Huawei SingleCLOUD models. Why are these alarms being generated and how do I correct this?

Solution:

When modeling a Huawei SingleCLOUD environment, a duplicate model can be created for different reasons. The following provides situations that can cause duplicate model alarms and explains how to correct them:

- **More than one instance of a virtual technology manager is managing a device model.**

  To correct this problem, verify that only one virtual technology manager within your SpectroSERVER environment is managing the device.

- **The virtual IP address used to define a Huawei SingleCLOUD Manager is the same as the primary IP address of the device where the CAMM Presenter is installed.**

  To correct this problem, verify that the virtual IP address used to communicate with Huawei SingleCLOUD Galax is not the same as the primary IP address of the device where the CAMM Presenter is installed.

More information:

Define Huawei SingleCLOUD Managers (see page 237)

Connections Do Not Appear in Huawei SingleCLOUD Topology

Symptom:

After I discover and model my Huawei SingleCLOUD environment, I do not see all of the connections between my Huawei SingleCLOUD components in the Topology. I have followed the correct procedures to install and set up my Huawei SingleCLOUD Device Pack for CAMM, as well as the recommended process for Huawei SingleCLOUD Discovery. Why do I not see the connections for my Huawei SingleCLOUD components in the Topology?

Solution:

To produce the connections between your Huawei SingleCLOUD components in the Topology view, CA Spectrum requires certain models and information to be available when determining Layer 2 connectivity during the modeling process, as follows:

- **Models of connecting devices**

  For CA Spectrum to make connections between your Huawei SingleCLOUD components in your modeled environment, any connecting devices must be modeled before the virtual entities are modeled. When discovering and modeling your Huawei SingleCLOUD environment, a standard CA Spectrum Discovery should be run first to model upstream routers and switches. Then, Huawei SingleCLOUD Discovery can run, creating models and connections for the virtual entities. If the connecting devices are not modeled first, connections are not made between the virtual elements.

- **Information about managed network elements**

  CA Spectrum requires specific information about managed network elements to be able to determine the Layer 2 connectivity within the network. If this information is not available, the connections in the Topology cannot be produced. There are two known issues that contribute to limitations in determining the Layer 2 connectivity of the Huawei SingleCLOUD components:

  - The Huawei switch used in the Huawei SingleCLOUD platform does not support the dot1d bridge tables correctly. Without the correct bridge table information, CA Spectrum cannot determine the Layer 2 connectivity of the Huawei SingleCLOUD components.
  - The Huawei SingleCLOUD API currently does not provide MAC addresses for the Huawei SingleCLOUD Virtual Machines. The MAC address is necessary for CA Spectrum to determine connectivity to the upstream networking devices. With the necessary information not available directly from the Huawei SingleCLOUD API, CA Spectrum attempts to resolve the MAC address from the upstream devices. If CA Spectrum cannot resolve the MAC address, the connectivity cannot be determined.

Follow these steps:

1. Verify that your upstream routers and switches were modeled correctly before Huawei SingleCLOUD Discovery ran.
2. If the connecting devices were not modeled correctly, do the following:
   a. Run Discover Connections on the affected virtual machines.

      Note: For more information on Discover Connections, see the *Modeling and Managing Your IT Infrastructure Administrator Guide*.

   b. If Discover Connections does not create the connections, delete the respective Huawei SingleCLOUD models and repeat the discovery and modeling process (see page 235).
3. If connecting devices have been modeled correctly, check for an SNMP Get_Next Loop Detected alarm on your upstream routers and switches.
   - If the alarm exists, the lack of Layer 2 connectivity in the Topology is due to how the Huawei device is populating the bridge table, for which there is no workaround.
   - If the alarm does not exist, verify that the Huawei SingleCLOUD Virtual Machines have valid MAC addresses, as follows:
     a. Run a Locater search for Huawei SingleCLOUD, All Virtual Machines.
     b. In the Results tab, review the values in the MAC Address column.

     Although CA Spectrum attempts to resolve the MAC address when it is not provided, the necessary information is not always available.

Glossary

application insight module (AIM)

The CA SystemEDGE agent provides a plug-in architecture through which it can load optional *application insight modules (AIMs)* when it initializes. AIMs are functional extensions to the SystemEDGE agent. For example, the vCenter AIM enables CA SystemEDGE to manage vSphere environments through VMware vCenter Servers.

CAMM Presenter (Huawei SingleCLOUD)

The *Huawei SingleCLOUD CAMM Presenter* model represents a CA Mediation Manager (CAMM) Presenter. The CAMM Presenter model allows configuration of the virtual IP addresses used by the CAMM Engines to communicate with Huawei SingleCLOUD GalaX. Each CAMM Presenter model can support multiple Huawei SingleCLOUD Managers.

cluster

A *cluster* is a group of ESX hosts and their associated virtual machines. When a host is added to a cluster, the host resources become part of the cluster resources. The cluster manages the resources of all hosts within it.

CNA FIP (Huawei SingleCLOUD)

The *Huawei SingleCLOUD CNA FIP* represents the management interface of the CNA that is hosting the virtual machines. This model is assigned the IP address of the CNA FIP and lives within the host container.

Computing Node Agent (CNA) (Huawei SingleCLOUD)

The *Computing Node Agent (CNA)* is an administrative process used in the Huawei SingleCLOUD platform that resides on a server that hosts virtual machines. A CNA is represented by a Huawei SingleCLOUD Host model in CA Spectrum. The Huawei SingleCLOUD CNA FIP model is assigned the IP address of the CNA.

data center (VMware)

A *data center* serves as a container for your hosts, virtual machines, resource pools, or clusters. Depending on their virtual configuration, data centers can represent organizational structures, such as geographical regions or separate business functions. You can also use data centers to create isolated virtual environments for testing or to organize your infrastructure.

datacenter (VMware)

A *datacenter* serves as a container for your hosts, virtual machines, resource pools, or clusters. Depending on their virtual configuration, datacenters can represent organizational structures, such as geographical regions or separate business functions. You can also use datacenters to create isolated virtual environments for testing or to organize your infrastructure.

distributed SpectroSERVER (DSS)

Distributed SpectroSERVER (DSS) is a powerful modeling feature that enables the distribution of management for portions of a large-scale network, either geographically, or across multiple servers in a single physical location.

ESX host (VMware)

An *ESX host* is a physical computer that uses ESX Server virtualization software to run virtual machines. Hosts provide the CPU and memory resources that virtual machines use and give virtual machines access to storage and network connectivity.

ESX service console (VMware)

The *ESX service console* is a Linux kernel running on the ESX host that provides a management interface to the hosted virtual machines.

global zone (Solaris)

A *global zone* is a zone that is contained on every Solaris system. If non-global zones exist on the system, the global zone is the default zone for the system and for systemwide administration.

Hardware Management Console (HMC)

The *Hardware Management Console (HMC)* is the IBM LPAR virtualization technology application used to configure IBM LPARs. This console provides centralized management of the IBM LPAR environment.

Huawei SingleCLOUD

The *Huawei SingleCLOUD* platform is an enterprise-grade turn-key offering that consists of a complete system of network, storage, servers and software for creating private or public clouds.

Huawei SingleCLOUD GalaX

Huawei SingleCLOUD GalaX is the software suite that collectively manages the Huawei SingleCLOUD. It includes the Operation and Management Module (OMM), which is responsible for managing the Universal Virtualization Platform (UVP).

Huawei SingleCLOUD Manager

The *Huawei SingleCLOUD Manager* represents a virtual IP address on the CAMM Presenter. CAMM monitors the Huawei SingleCLOUD GalaX, which is responsible for managing the Huawei SingleCLOUD virtual platform. Information for each Huawei SingleCLOUD GalaX being monitored by CAMM is provided through a virtual IP address on the CAMM Presenter and is represented by a Huawei SingleCLOUD Manager model.

Hyper-V Host

A *Hyper-V Host* is a physical computer that uses Microsoft Hyper-V virtualization software to run virtual machines. Hosts provide the CPUs and memory resources that Hyper-V virtual machines use. They also give these virtual machines access to storage and network connectivity.

Hyper-V management operating system

The *Hyper-V management operating system* is the original operating system running on the Hyper-V Host. Microsoft Hyper-V uses this operating system to configure the hosted Hyper-V virtual machines.

IBM LPAR

An *IBM LPAR* is a logical partition instance configured on the IBM LPAR Host that, like a physical computer, runs an operating system and applications. An IBM LPAR dynamically consumes resources on its physical host, depending on its workload and configuration.

IBM LPAR Host

An *IBM LPAR Host* is a physical computer that uses IBM LPAR virtualization software to host IBM LPAR instances. IBM LPAR Hosts provide the CPU and memory resources that IBM LPARs use. They also give these IBM LPARs access to storage and network connectivity.

IBM LPAR Manager

The *IBM LPAR Manager* in Virtual Host Manager is the CA SystemEDGE agent with the IBM LPAR AIM enabled. The IBM LPAR Managers are responsible for reporting on all of the configured IBM LPARs. Virtual Host Manager communicates with the IBM LPAR Managers to gather details about your IBM LPAR virtual environment.

non-global zone (Solaris)

A *non-global zone* provides a virtualized operating system environment in a single instance of the Solaris operating system. The Solaris Zones software partitioning technology virtualizes operating system services.

Operation and Management Module (OMM)

The *Operation and Management Module (OMM)* is part of the Huawei SingleCLOUD GalaX software application that is responsible for managing the Huawei SingleCLOUD Hypervisor Universal Virtualization Platform (UVP).

pingable model

A *pingable model* is a generic type of network model created in CA Spectrum based on a non-SNMP model type. CA Spectrum can poll these devices to provide basic model management, but SNMP-capable monitoring is not available.

proxy management

Proxy management is the act of managing network devices using an alternate management source in place of or in addition to the primary manager. For example, CA Spectrum can manage virtual network devices by contacting them directly or through the virtual technology application's contact with the devices.

resource pool (Solaris)

A *resource pool* defines a configuration mechanism for partitioning system resources. A resource pool is an association between resource groups which can be partitioned.

resource pool (VMware)

A *resource pool* defines partitions of physical computing and memory resources of a single host or a cluster. You can partition any resource pool into smaller resource pools to divide and assign resources to specific groups or for specific purposes. You can also hierarchically organize and nest resource pools.

Solaris Global Zone

The *Solaris Global Zone* is the management operating system running on the Solaris Zones Host that Solaris Zones uses to configure the hosted Solaris zone instances.

Solaris zone

A *Solaris zone* is a non-global zone instance managed by Virtual Host Manager that runs on a Solaris Zones Host.

Solaris Zones Host

Solaris Zones Hosts represent the physical hardware of the Solaris Host managed by Virtual Host Manager.

Solaris Zones Manager

The *Solaris Zones Manager* in Virtual Host Manager is the CA SystemEDGE agent with the Solaris Zones AIM enabled. The Solaris Zones Managers are responsible for reporting on all of the configured Solaris zones. Virtual Host Manager communicates with the Solaris Zones Managers to gather details about your Solaris Zones virtual environment.

Universal Virtualization Platform (UVP)

The *Universal Virtualization Platform (UVP)* is the Huawei HyperVisor, a part of the Huawei SingleCLOUD solution that consists of the hosts and virtual machines that make up its cloud architecture.

vCenter

vCenter is a VMware application that provides centralized management, operational automation, and resource optimization for ESX environments.

vCenter Server (VMware)

VMware *vCenter Server* provides the central point of control for configuring, provisioning, and managing a virtual vSphere environment. vCenter Server runs as a service on Microsoft Windows Servers and Linux Servers.

VHM model

A *VHM model* in CA Spectrum represents a virtual entity managed by Virtual Host Manager. Instead of retrieving status and management information from SNMP like some traditional CA Spectrum models, a VHM model communicates with the proxy manager for its fault and virtual management capabilities. A VHM model can additionally communicate via SNMP if an SNMP agent is installed and configured on the modeled device.

virtual machine

A *virtual machine (VM)* is a software computer that, like a physical computer, runs an operating system and applications. A virtual machine dynamically consumes resources on its physical host, depending on its workload. Because virtual machines are flexible computing units, their deployment comprises a wide range of environments. Examples include environments such as data centers, cloud computing, test environments, or desktops and laptops. In data center implementations, they are used for server consolidation, workload optimization, or higher energy efficiency.

virtual NIC (VMware)

A *virtual NIC* is a virtual Ethernet adapter on a virtual machine. The guest operating system communicates with the virtual Ethernet adapter through a device driver as if the virtual Ethernet adapter was a physical Ethernet adapter. The virtual Ethernet adapter has its own MAC address, one or more IP addresses, and responds to the standard Ethernet protocol like a physical NIC.

VMware Manager

The *VMware Manager* in Virtual Host Manager is the CA SystemEDGE agent with the vCenter Server AIM loaded. The VMware Manager is responsible for reporting on all of the configured virtual machines it manages. Virtual Host Manager communicates with the VMware Managers to gather details about your VMware virtual environment.

Index

I

L

M

N

O

P

R

S

T

U

V