CA Spectrum®

Cluster Manager Solution Guide

Release 9.4

ca technologies

This Documentation, which includes embedded help systems and electronically distributed materials, (hereinafter referred to as the “Documentation”) is for your informational purposes only and is subject to change or withdrawal by CA at any time.

This Documentation may not be copied, transferred, reproduced, disclosed, modified or duplicated, in whole or in part, without the prior written consent of CA. This Documentation is confidential and proprietary information of CA and may not be disclosed by you or used for any purpose other than as may be permitted in (i) a separate agreement between you and CA governing your use of the CA software to which the Documentation relates; or (ii) a separate confidentiality agreement between you and CA.

Notwithstanding the foregoing, if you are a licensed user of the software product(s) addressed in the Documentation, you may print or otherwise make available a reasonable number of copies of the Documentation for internal use by you and your employees in connection with that software, provided that all CA copyright notices and legends are affixed to each reproduced copy.

The right to print or otherwise make available copies of the Documentation is limited to the period during which the applicable license for such software remains in full force and effect. Should the license terminate for any reason, it is your responsibility to certify in writing to CA that all copies and partial copies of the Documentation have been returned to CA or destroyed.

TO THE EXTENT PERMITTED BY APPLICABLE LAW, CA PROVIDES THIS DOCUMENTATION “AS IS” WITHOUT WARRANTY OF ANY KIND, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. IN NO EVENT WILL CA BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY LOSS OR DAMAGE, DIRECT OR INDIRECT, FROM THE USE OF THIS DOCUMENTATION, INCLUDING WITHOUT LIMITATION, LOST PROFITS, LOST INVESTMENT, BUSINESS INTERRUPTION, GOODWILL, OR LOST DATA, EVEN IF CA IS EXPRESSLY ADVISED IN ADVANCE OF THE POSSIBILITY OF SUCH LOSS OR DAMAGE.

The use of any software product referenced in the Documentation is governed by the applicable license agreement and such license agreement is not modified in any way by the terms of this notice.

The manufacturer of this Documentation is CA.

Provided with “Restricted Rights.” Use, duplication or disclosure by the United States Government is subject to the restrictions set forth in FAR Sections 12.212, 52.227-14, and 52.227-19(c)(1) - (2) and DFARS Section 252.227-7014(b)(3), as applicable, or their successors.

CA Technologies Product References

This document references the following products:

- CA Spectrum®
- CA Spectrum® Active Directory and Exchange Server Manager (Active Directory and Exchange Server Manager)
- CA Spectrum® Virtual Host Manager (Virtual Host Manager)
- CA SystemEDGE (SystemEDGE)
- CA Virtual Assurance for Infrastructure Managers (CA Virtual Assurance)

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: Cluster Manager

This section contains the following topics:

About Cluster Manager

Cluster Manager is a CA Spectrum feature that models and monitors your cluster environment and is intended for administrators. Cluster Manager provides an enterprise-wide view of your cluster environments, showing both topology and the logical relationships among your cluster components. Cluster Manager also provides visibility into useful metrics and helps you pinpoint and effectively troubleshoot problems by applying unique fault isolation techniques.

A key challenge when monitoring your cluster environment is tracking where work is occurring, or identifying the active nodes. Clustering technology is designed to sustain high availability for your server-based applications by providing a fail-safe environment. Resource groups move from one cluster node to another when needed, resulting in the distribution of work and node status changing periodically. Cluster Manager keeps up with these activities by continuously monitoring your cluster components, and quickly notifies you of any changes to your environment.

Features

Cluster Manager includes the following features:

- Automated device discovery and modeling. Cluster Manager automatically creates models and connections for all managed cluster components, as appropriate.
- A distributed solution that can handle scaling. Cluster management can be distributed across multiple SpectroSERVERs.
- Identification of cluster components in the topology.
- Hierarchical representation of cluster environments.
- Icons that distinguish devices in your cluster environment, including distinct identification of active and inactive nodes.
- Dedicated Cluster Manager views that provide visibility into data specific to cluster environments and respective technologies.

- Events and alarming on cluster entities and activities, provided out-of-box.
- Enhanced fault management. Cluster Manager recognizes and correlates symptomatic alarms and aids fault isolation with proxy management.
- Locater searches specific to cluster components.
- Consistent representation across all supported cluster technologies.

Supported Technologies

Cluster Manager supports the following cluster technologies when all required components are installed and configured properly per solution, as follows:

IBM PowerHA

- CA Spectrum 9.2.3 or later
- A dedicated host machine with:
  - SystemEDGE 5.x or later
  - High Availability Cluster Multiprocessing (HACMP) AIM r12.7 or later

  Important! The HACMP AIM must be the only AIM installed on the SystemEDGE host. The SystemEDGE host itself cannot be a node in your managed cluster environment.

Microsoft Cluster Service (MSCS)

- CA Spectrum 9.2.3 or later
- A dedicated host machine with:
  - SystemEDGE 5.x or later
  - MSCS AIM r12.7 or later

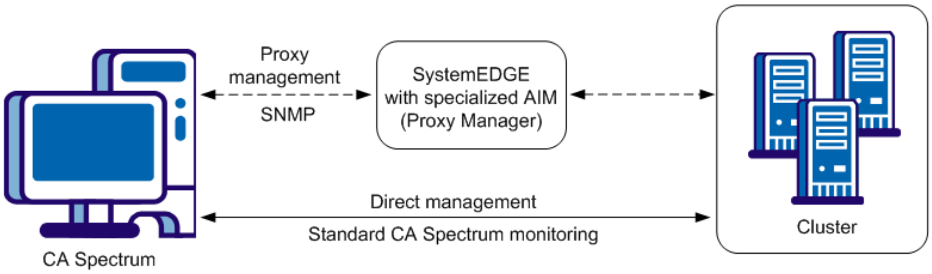
  Important! The MSCS AIM must be the only AIM installed on the SystemEDGE host. The SystemEDGE host itself cannot be a node in your managed cluster environment.

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

Solution Architecture

Cluster Manager monitors your cluster components seamlessly within your network, while providing data that is specific to cluster technologies. CA Spectrum gathers information about your cluster components using two different methods. As with other CA Spectrum-managed devices, Cluster Manager uses standard CA Spectrum monitoring. In addition, Cluster Manager also retrieves specialized information from an alternate (proxy) manager, the SystemEDGE Application Insight Module (AIM).

An AIM is a specialized extension of the SystemEDGE agent and resides on its own host. The proxy manager communicates directly with entities in your cluster environment. CA Spectrum then uses SNMP to retrieve this information from the proxy manager and uses it to model and monitor your cluster components in OneClick.


Proxy management
SNMP
SystemEDGE with specialized AIM (Proxy Manager)
Cluster
Direct management
Standard CA Spectrum monitoring
CA Spectrum

The AIMs that work with Cluster Manager include:

- **High Availability Cluster Multiprocessing (HACMP) AIM**

  Provides capabilities to monitor your IBM PowerHA cluster environment.

- **Microsoft Cluster Service (MSCS) AIM**

  Provides capabilities to monitor your Microsoft Cluster Service environment.

Note: For more information about the SystemEDGE agent and AIMs, see the *CA Virtual Assurance for Infrastructure Managers Administration Guide*.

More information:

Solution Architecture for MSCS (see page 57)
Solution Architecture for IBM PowerHA (see page 41)

Cluster Concepts

Administrators organize resources into functional units that are called resource groups, and assign these groups to individual nodes. If a node fails, the resource groups that were being hosted on a particular node move to other nodes in the cluster.

The following terms describe these components of a cluster environment and appear in the Cluster Manager solution:

Cluster

A group of locally attached machines that provide distributed processing power and high availability. A cluster appears to clients as a single system image and IP address.

Node

An independent computer system that participates in a cluster.

Active node

A system in a cluster environment where application processes (as part of a resource group) are currently running. Within Cluster Manager, an active node has resource groups as children.

Inactive node

A system that is allocated to a cluster but not currently processing any resources. Within Cluster Manager, an inactive node does not have any resource groups as children.

Resource group

A collection of resources that forms a functional unit existing on a single node.

Resource

A logical component or entity that runs on only one node at a time. Resources encompass all elements needed for an application, such as network interfaces, disks, file systems, and application software.

Migration

Movement of a resource group from one node to another. Different terms are used regarding migration depending on the cluster technology; for example, failover, fall over, failback, and fallback.

Chapter 2: Getting Started

Note: Unless otherwise noted, the information in this section applies to all supported cluster technologies.

This section contains the following topics:

Planning Your Implementation

The purpose of Cluster Manager is to monitor your cluster components and notify you of various activities in your environment. Cluster Manager is highly scalable and can manage cluster nodes under different technologies using multiple AIMs across distributed SpectroSERVERs. Understanding how CA Spectrum manages the models for the components in your cluster environment provides for a more efficient Cluster Manager implementation.

Before you set up Cluster Manager, review the following topics:

- Environment Management Considerations (see page 13)
- Modeling (see page 14)

Environment Management Considerations

During setup of Cluster Manager, you specify how to organize the management of your environments. With a small environment, you can have a single AIM managing all of your cluster nodes (by vendor) in a single location on one SpectroSERVER. In a complex environment, you can have multiple AIMs across multiple SpectroSERVERs managing various cluster environments in different locations using different vendors.

Although organizational specifications can be changed at any time, knowing the available configuration options allows for a better initial setup.

Consider the following points when setting up your Cluster Manager environment:

- AIMs for Cluster Manager are vendor-specific. If you use cluster technologies from more than one vendor, you need multiple AIMs and dedicated SystemEDGE hosts.
- Each AIM can manage more than one cluster.
- Management of your cluster environment can be distributed across multiple AIMs, which can be supported in a single landscape or across multiple SpectroSERVERs.
- Management of each cluster can be by one cluster technology AIM only.

When deciding how to distribute management of your cluster environment, consider the number and location of nodes in your environment. The number of cluster nodes an AIM manages and the geographic proximity of the AIM to the monitored environment can affect performance. For best performance, size and balance management of the environment appropriately.

Note: The clusters that a particular AIM manages are controlled on the AIM and not in CA Spectrum. For information about defining nodes to manage by an AIM, see the *CA Virtual Assurance for Infrastructure Managers Administration Guide*.

Modeling

As with other network elements supported in CA Spectrum, you discover and model the components of your cluster environment to monitor them. Cluster Manager obtains information about the clusters and nodes to manage from the AIM. CA Spectrum then uses this information to model each component using AutoDiscovery.

Note: Information that is used for the Cluster Manager feature is gathered primarily from the proxy manager (AIM). Additional information is also gathered directly from the nodes.

The following topics provide more details about the modeling process:

- What Is Modeled (see page 14)
- Modeling Methods (see page 15)
- Node Management and Multiple Cluster AIMs (see page 16)
- Node Management and Multiple CA Spectrum AIM Solutions (see page 16)

What Is Modeled

Using information provided in the AIM MIB, CA Spectrum extracts and models any clusters, nodes, resource groups, and resources that the AIM manages.

Modeling Methods

Cluster nodes are modeled as SNMP-managed elements when possible. SNMP modeling supports enriched device monitoring that can provide added value to your Cluster Manager solution. If an SNMP agent is not installed on the host, it is modeled as an ICMP (Pingable) device.

The following sections provide details about how cluster nodes are modeled:

- Model Naming (see page 15)
- IP Address and MAC Address Determination (see page 16)

More information:

How to Convert an ICMP (Pingable) Model to SNMP-Managed (see page 39)

Model Naming

When modeling cluster nodes, the model name assigned in CA Spectrum depends on the type of modeling used, as follows:

- For SNMP modeling, CA Spectrum automatically attempts to supply a name for the model using standard CA Spectrum naming conventions. Automatic naming is controlled at the SpectroSERVER level by the Model Naming Order value. This field is on the SpectroSERVER Control view for the VNM model.
- For ICMP (Pingable) modeling (when not a virtual device), CA Spectrum uses the host name provided in the AIM.

  Important! For ICMP (Pingable) modeling, model names that CA Spectrum Virtual Host Manager sets take precedence over Cluster Manager.

The administrator can modify the name of a cluster node model at any time. As with other managed network elements, CA Spectrum automatically updates the model name using established naming rules, which can replace the user-defined value. To retain a user-defined value, lock the model name.

Note: You can modify and lock the cluster node model name using the following model attributes: Model_Name (0x1006e) and Lock_Model_Name (0x12a52).

More information:

Node Management and Multiple CA Spectrum AIM Solutions (see page 16)

IP Address and MAC Address Determination

When modeling cluster nodes, the IP address and MAC address assigned in CA Spectrum depend on the type of modeling used, as follows:

- For SNMP modeling, CA Spectrum automatically attempts to determine the addresses by querying the resident SNMP agent.
- For ICMP (Pingable) modeling (when not a virtual device), CA Spectrum uses the addresses that the AIM provides.

  Important! For ICMP (Pingable) modeling, addresses that CA Spectrum Virtual Host Manager sets take precedence over Cluster Manager.

If the SNMP modeling or Virtual Host Manager cannot supply a valid IP address or MAC address, the AIM value is used.

More information:

Node Management and Multiple CA Spectrum AIM Solutions (see page 16)

Node Management and Multiple Cluster AIMs

Manage a cluster node by a single cluster technology AIM only. If you inadvertently manage a cluster node by multiple cluster technology AIMs, Cluster Manager issues the following alarm on the cluster model:

```
UNSUPPORTED CLUSTER AIM CONFIGURATION
```

Children are not created for the cluster model.

Node Management and Multiple CA Spectrum AIM Solutions

When managing a cluster node model 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 node with a SystemEDGE agent is already modeled in CA Spectrum, Cluster Manager recognizes the model and a duplicate model is not created. Instead, Cluster Manager pulls the existing model into its own management, abiding by and applying the rules of each solution in the ranked order.

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

If a node is removed from management by a solution, the rules of the remaining solutions are reapplied in the ranked order. Typically, any changes are made at the next polling cycle.

This defined order of management also affects how models appear in the Universe topology.

More information:

Topology View (see page 25)
How to Model Your Environment When Using Multiple AIM Solutions (see page 18)
Deleting Models When Using Multiple AIM Solutions (see page 40)

How to Install Cluster Manager

When you install CA Spectrum, the Cluster Manager components are automatically installed and available for use. However, Cluster Manager is operable only after you also install and configure the appropriate proxy manager for your solution.

Refer to the respective section for your solution.

More information:

How to Set Up Cluster Manager for MSCS (see page 58)
How to Set Up Cluster Manager for IBM PowerHA (see page 42)

Discovery and Modeling

After the necessary components have been installed, discover and model any entities that Cluster Manager is going to manage.

Cluster Manager uses the following types of discovery:

- Standard CA Spectrum Discovery to model the cluster technology AIM and connecting devices
- Cluster Manager discovery to model cluster components

After the cluster technology AIM is modeled successfully, Cluster Manager obtains information about the cluster components in your environment from the AIM. Using a list of machines that is obtained from the AIM, Cluster Manager uses AutoDiscovery to model each cluster node. All supporting cluster components (clusters, resource groups, and resources) are also modeled.

Cluster Manager models cluster nodes as SNMP-managed when possible and when AutoDiscovery parameters are set up correctly.

Note: For information about AutoDiscovery control settings, see the *Modeling and Managing Your IT Infrastructure Administrator Guide*.

The information provided in this topic applies to all cluster technologies. For more details, refer to the respective section for your solution.

More information:

Discover and Model Your MSCS Environment (see page 59)
Discover and Model Your IBM PowerHA Environment (see page 43)
How to Convert an ICMP (Pingable) Model to SNMP-Managed (see page 39)

How to Model Your Environment When Using Multiple AIM Solutions

Depending on your environment, you can use Cluster Manager in combination with other CA Spectrum AIM solutions simultaneously to manage your network entities. Any of the following configurations require the use of multiple solutions for complete management of your environment:

- A cluster node runs on a virtual machine.
- A cluster technology AIM runs on a virtual machine.
- A cluster node is an Active Directory or Exchange Server host.

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

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

The combination of these features provides a complete monitoring solution. To set up your implementation of multiple AIM solutions effectively, the following approach is recommended.

Important! When using multiple AIMs, only a single AIM can be installed on a given 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 *Virtual Host Manager Solution Guide* and the *Active Directory and Exchange Server Manager Solution Guide*.

More information:

Node Management and Multiple CA Spectrum AIM Solutions (see page 16)
Deleting Models When Using Multiple AIM Solutions (see page 40)

Viewing Your Cluster Environments

The purpose of Cluster Manager is to provide visibility into your cluster environments. This visibility lets you identify the organization of your environment, where resource groups are allocated, and the status of each node. Most importantly, when a problem occurs in your environment, you can pinpoint its cause.

Cluster Manager provides several methods for viewing your cluster environments, as follows:

- The Cluster Manager hierarchy in the Navigation panel indicates the logical relationships between components. Examples of hierarchy nodes include clusters, cluster nodes, resource groups, and resources.
- A graphical topology view helps you to group cluster nodes and visualize the connections between them.
- Custom Information views in the Component Detail panel provide details that are specific to cluster technologies and specific vendors.
- Custom searches provide a quick way to find cluster elements.
- Custom icons for individual models provide status and model type information at a glance and are integrated throughout the Cluster Manager feature.

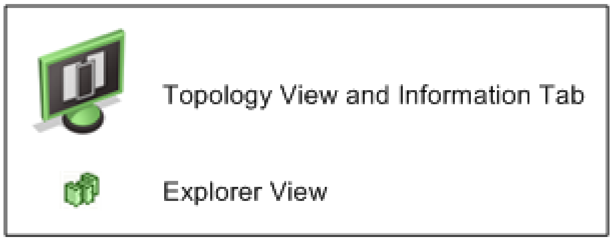
Understanding each of these methods can help you monitor your cluster environments more efficiently, letting you troubleshoot issues more effectively.

Icons for Cluster Manager

Cluster Manager provides icons that are designed specifically to distinguish devices in your cluster environment. The same icons are used across all cluster vendor technologies.

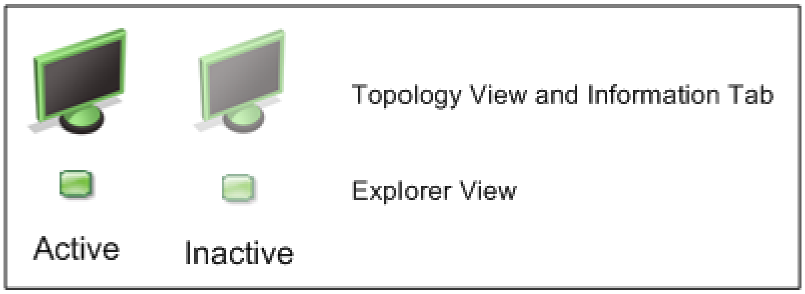
Cluster

Cluster icons have a distinctive cluster pattern, representing three workstations that are clustered together, as follows:



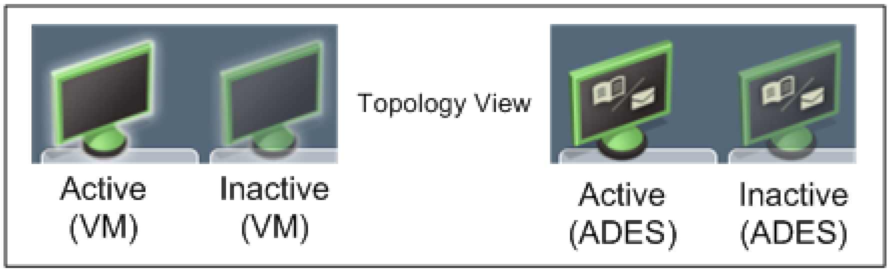
Cluster Node

Cluster nodes use standard workstation icons. An active node has a solid (nontransparent) representation whereas an inactive node is faded (transparent), as follows:



The icon also reflects when Cluster Manager is used in combination with other CA Spectrum AIM-based solutions. The following example shows:

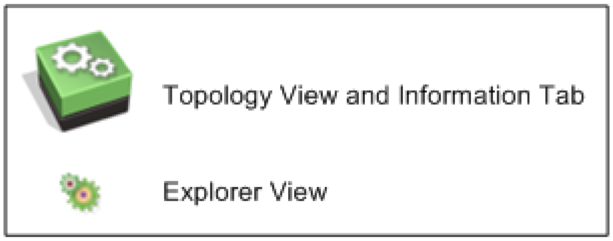
- An active node and an inactive node in the topology where both nodes are virtual machines that Virtual Host Manager manages. Notice that the virtual halo is brighter for the active node.
- An active node and an inactive node in the topology where both nodes are Active Directory or Exchange Server hosts.



Note: When an inactive node is used with the spotlighting feature, the icon becomes even more transparent.

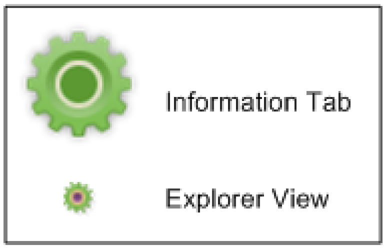
Resource Group

Resource groups have an icon that has multiple gears, as follows:



Resource

Resources have an icon that has a single gear, as follows:



Note: Resources are not displayed in the topology view.

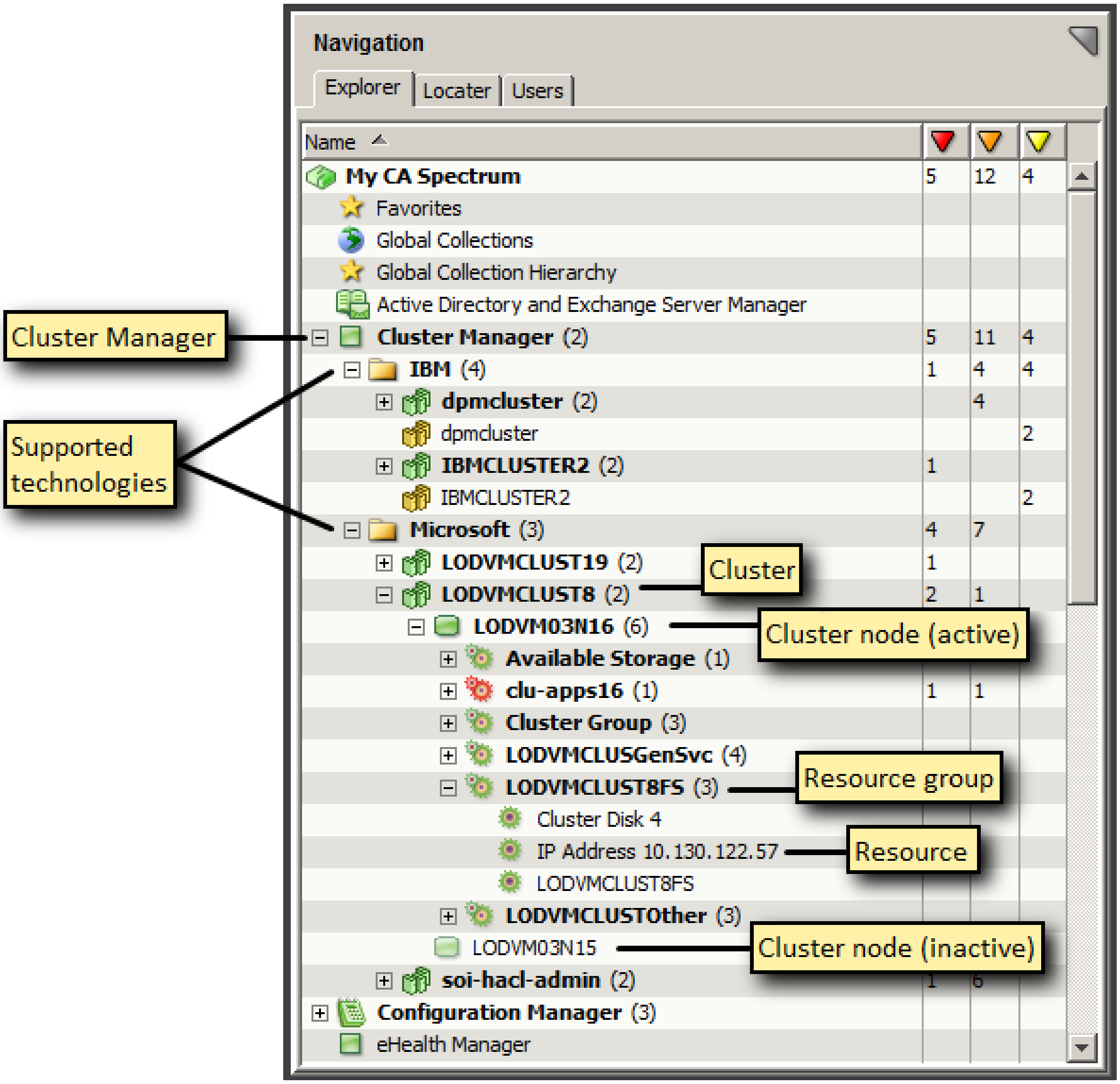
Explorer View

On the Explorer tab of the Navigation panel, Cluster Manager provides a hierarchical tree structure that illustrates the logical organization of your managed cluster environments. Custom icons provide status and model type information for your cluster components at a glance.

Using this information, you can see how the clusters and respective resources are arranged logically in your environment and where they are active.

Note: Only users with the appropriate privileges and model security access can view the Cluster Manager hierarchy and components. For more information, see the *Administrator Guide*.

The following image is an example of the Cluster Manager hierarchy:



Name ▲	▼	▼	▼
My CA Spectrum	5	12	4
Favorites			
Global Collections			
Global Collection Hierarchy			
Active Directory and Exchange Server Manager			
⊟ Cluster Manager (2)	5	11	4
⊟ IBM (4)	1	4	4
⊞ dpmcluster (2)		4	
dpmcluster			2
⊞ IBMCLUSTER2 (2)	1		
IBMCLUSTER2			2
⊟ Microsoft (3)	4	7	
⊞ LODVMCLUST19 (2)	1		
⊟ LODVMCLUST8 (2)	2	1	
⊟ LODVM03N16 (6)			
⊞ Available Storage (1)			
⊞ clu-apps16 (1)	1	1	
⊞ Cluster Group (3)			
⊞ LODVMCLUSGenSvc (4)			
⊟ LODVMCLUST8FS (3)			
Cluster Disk 4			
IP Address 10.130.122.57			
LODVMCLUST8FS			
⊞ LODVMCLUSTOther (3)			
LODVM03N15			
⊞ soi-hacl-admin (2)	1	6	
⊞ Configuration Manager (3)			
eHealth Manager			

The following elements form the hierarchy. When an element in the hierarchy has children, the label is in bold.

Cluster Manager

Denotes the root for the cluster environments that are currently managed. Cluster Manager is a distributed solution that handles multiple landscapes and so appears above the landscape level. Expanding the Cluster Manager element displays the technologies that are supported. The clusters and participating cluster components for each technology are also presented, as depicted in the following diagram:

```
[-] Cluster_technology_1
    [-] Cluster_1
        [-] Cluster_node_1 (active)
            [-] Resource_group_1
                . Resource 1
                . Resource 2
                . Resource 3
            Cluster_node_2 (inactive)
            Cluster_node_3 (inactive)
    [+] Cluster 2
[+] Cluster_technology_2
```

Note: Only those solutions for which a respective AIM has been installed appear in your implementation. The AIM itself does not appear in the Cluster Manager hierarchy. The Cluster Manager (AIM) model appears in the Universe topology and the Universe hierarchy.

Cluster technology

Represents a vendor cluster technology. The cluster technology folder displays all managed clusters across all landscapes for the respective technology, such as IBM or Microsoft.

The hierarchy within the vendor folder shows the logical relationships between the participating components. When all cluster components for a cluster technology are deleted, the empty cluster technology folder remains.

Cluster

Represents a cluster. The cluster name that is used is obtained from the AIM and differs based on technology.

Cluster node

Represents a cluster node. The transparency of the icon reflects whether a cluster node is active or inactive. A solid (nontransparent) icon represents an active node; a faded (transparent) icon represents an inactive node. An active node has resource groups as children; an inactive group does not have any resource groups.

Resource group

Represents a resource group.

Resource

Represents a resource.

Note: Resources are displayed in the hierarchy view only; resources are not displayed in the topology view.

Management by Multiple AIM Solutions

When Cluster Manager and another CA Spectrum AIM solution simultaneously and successfully manage a cluster node, the following details apply when viewing your environment:

- The Cluster Manager hierarchy provides a complete and accurate view of your cluster environment. The Universe hierarchy presents all models by defined order of solution management. For example, when a cluster node is a virtual machine, it does not appear within its cluster container in the Universe hierarchy. Instead, it appears in its physical host container in the Virtual Host Manager hierarchy.

  Note: When multiple solutions are managing a node, you can quickly locate it in the correct hierarchy from the Contents panel. Locate the model in the List view or Topology view, then right-click the model and select Location.

- In the Explorer view, the icon for the highest ranking solution applies.
- If Virtual Host Manager manages the node, the node name that appears in the Cluster Manager hierarchy and List view is as follows:
  - For ICMP (Pingable) models, the model name that Virtual Host Manager sets is used.
  - For SNMP models, default Cluster Manager model naming is used.

  Note: Typically, most CA Spectrum AIM solutions use the Domain Naming System (DNS) name. Regardless, the highest ranking solution applies.

More information:

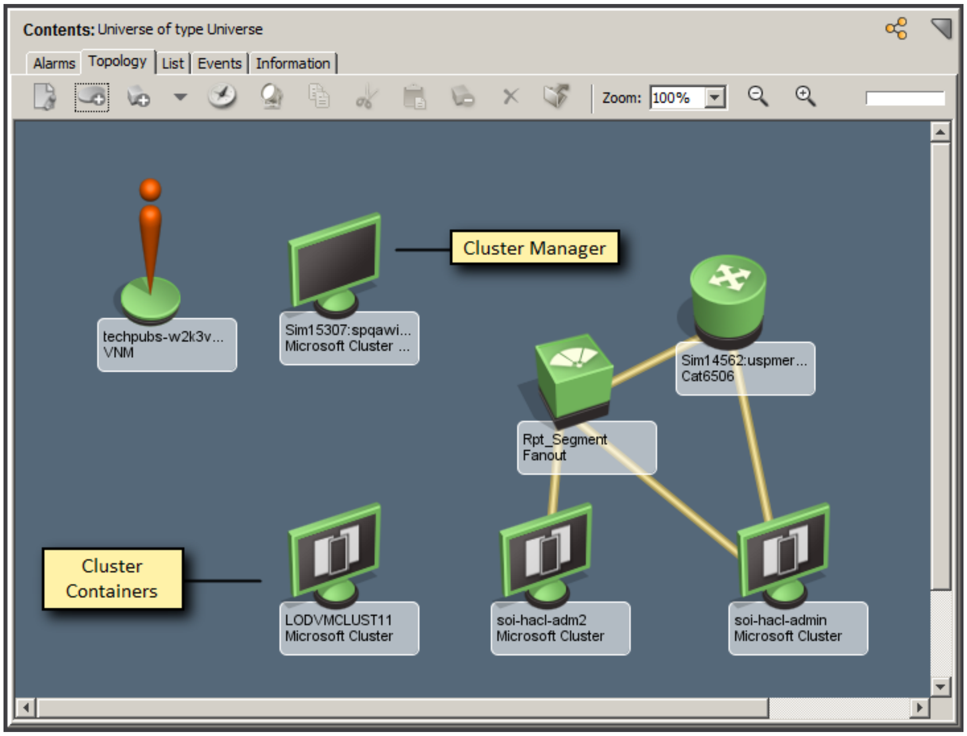
Model Naming (see page 15)
Node Management and Multiple CA Spectrum AIM Solutions (see page 16)

Topology View

The models for your managed cluster environment are organized and integrated into the Universe topology view. These models include the Cluster Manager (SystemEDGE host), cluster, cluster node, and resource group models. This graphical representation helps you visualize the structure of your managed environment, including connections between cluster nodes and other elements of your network.

Cluster node and resource group models are organized in the topology in cluster containers. When possible, the cluster container model is created alongside the Cluster Manager model, as shown in the following Universe topology top view example.

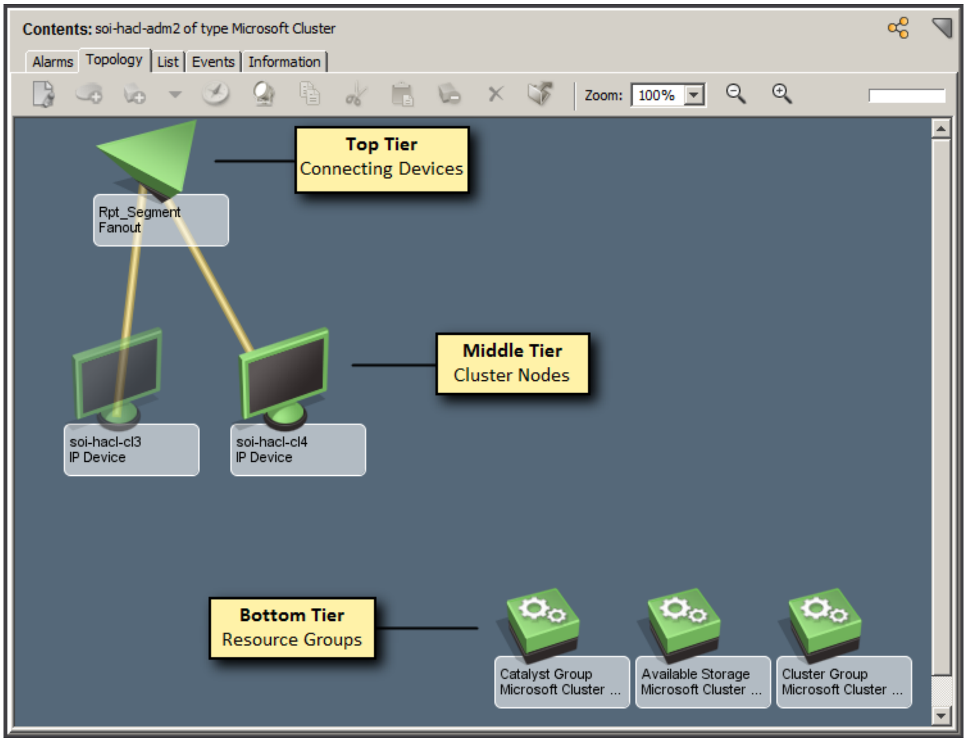
Note: If the Cluster Manager is a virtual machine, the cluster container is created in the same topology as the Virtual Host Manager physical host container.



Drilling down into a cluster container reveals its contents. These contents include off-page references to connected network devices, cluster nodes, and active resource groups participating in the cluster.

Note: Resources are displayed in the Cluster Manager hierarchy view only; resources are not displayed in the topology view.

The following illustration shows a drill-down view of a cluster container. Cluster components are arranged in three tiers, as shown:



Contents: soi-hacl-adm2 of type Microsoft Cluster

Important! Although you can edit the cluster container topology view, CA Spectrum enforces the placement of the models within the appropriate tiers. If you rearrange the models in this view, their placement is not preserved. Other changes, such as text annotations and background changes, are retained.

Top tier

Displays any off-page references to connecting devices modeled in other views, such as upstream routers, repeaters, and switches. These elements connect your cluster nodes to your network.

Middle tier

Displays the cluster nodes that participate in the cluster. If a cluster node has already been modeled in Virtual Host Manager before Cluster Manager discovery, it is not modeled again. However, it is included in the cluster container topology to provide a complete view of your cluster environment.

Bottom tier

Displays the resource groups that participate in the cluster.

Note: Associations between the resource groups and their respective nodes are not displayed in this view; this information is provided in the Cluster Manager hierarchy view.

The following rules apply to cluster containers:

- You cannot add or remove models from a cluster container. Changes in cluster container contents can occur when components are added or removed from management by an AIM or changes occur in the cluster environment. However, CA Spectrum controls the placement of models within a cluster container exclusively.
- You cannot destroy a cluster container directly. The cluster container is destroyed only when the respective Cluster Manager model is deleted or when the cluster is removed from management by the AIM. When the cluster container is destroyed, all cluster node models in the container are moved to the Lost and Found (LostFound). An exception is when a cluster node is in a global collection; in this case, the model remains in the global collection.

More information:

Node Management and Multiple CA Spectrum AIM Solutions (see page 16)
Models Created for MSCS (see page 62)
Models Created for IBM PowerHA (see page 46)
Maintaining Your Cluster Manager Implementation (see page 37)
Placement of Models (see page 28)

Placement of Models

The placement of cluster node and resource group models in the topology during Cluster Manager discovery occurs as follows:

- If Cluster Manager discovery creates the model, the model is placed in a cluster container.
- If the model exists and is for a virtual machine that Virtual Host Manager manages, the model remains in the physical host container. And, the model is also included in the cluster container. Within the cluster container, the cluster node icon retains the characteristics of a virtual machine.
- If the model exists and is for a physical machine that another AIM solution manages, the model is moved to the cluster container. An example of another AIM solution is ADES Manager.

  Note: When you remove a model from management by Cluster Manager, it is removed from the cluster container. If ADES Manager continues to manage the host, the model does not appear in the ADES Managed Hosts container automatically. To move the model, cut and paste the model from Lost and Found (LostFound) into the ADES Managed Hosts container.
- If the model exists and no other AIM solution manages the model, the model is moved to the cluster container.

More information:

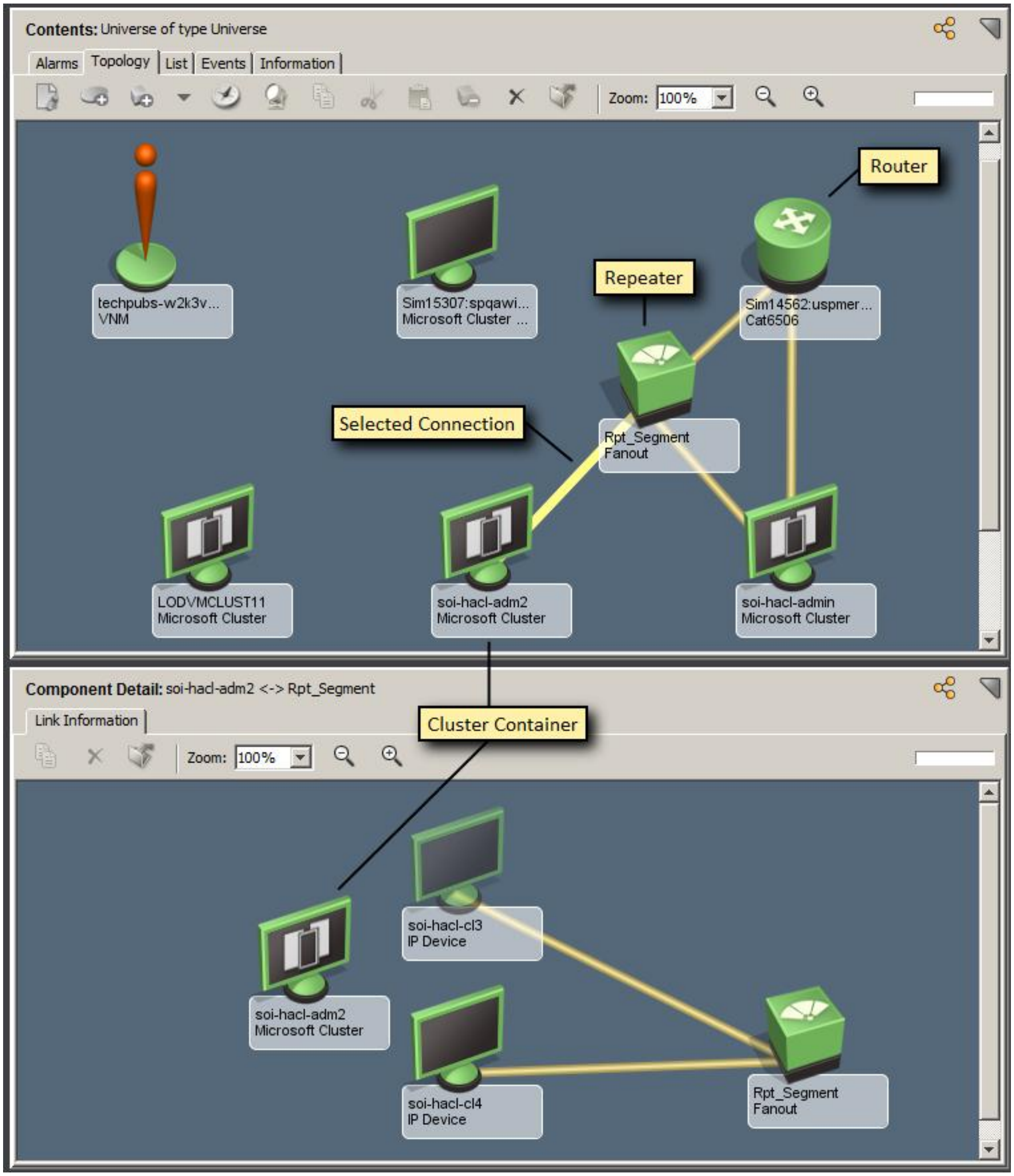
Deleting Cluster Manager Models (see page 39)
Icons for Cluster Manager (see page 20)

Connectivity

The Topology view displays the connectivity for your cluster environment within your network. Cluster Manager provides the links between your cluster nodes and any connecting devices that have been modeled in your network.

Important! Cluster Manager provides the connection to the physical IP address of the cluster node and not to the virtual IP address of the cluster.

In the Universe view, the connections (pipes) represent connections from the connecting devices to the cluster nodes within the cluster containers. By selecting a connection to examine the link more closely, the connections to the specific nodes are displayed, as illustrated in the following example:



Discover Connections runs automatically when the following actions occur:

- A cluster node is initially discovered and modeled.
- The IP address or MAC address of the cluster node has changed.

Discover Connections runs when necessary on the poll cycle. If the Discover Connections process does not complete within a single polling interval, the next Cluster Manager discovery is postponed.

Information Subviews

CA Spectrum includes several tabs in the Contents and Component Detail panels to provide quick access to information you need for monitoring your cluster environment. The Information tab provides details about a single entity in your environment. These details are displayed in the expandable subviews and vary by solution.

Custom subviews provide detailed information that is specific to the cluster component type. Custom subviews are provided for the following cluster components:

- Cluster Manager
- Cluster
- Cluster Node
- Resource Group
- Resource

More information:

Custom Subviews for IBM PowerHA (see page 47)
Custom Subviews for MSCS (see page 63)

Locater Searches

CA Spectrum provides a collection of preconfigured searches on the Locater tab that are designed specifically for your cluster environment. You can use these searches to locate entities in the CA Spectrum database that are related to the supported cluster technologies. These searches identify specific models or groups of models and can help you obtain details that you can use when monitoring your cluster environment. The searches are grouped under the Cluster Manager folder in the Locater tab of the Navigation panel.

Note: Only users with the appropriate privileges can access Cluster Manager searches. For more information, see the *Administrator Guide*.

More information:

Locater Searches for IBM PowerHA (see page 50)
Locater Searches for MSCS (see page 66)

Event and Availability Reports

To monitor the cluster environment, you can create event and availability reports. Event reports gather information that helps you make informed decisions about the components in the cluster environment. Using the event filters, you can base the event reports on any of the management events that are generated for the cluster environment in CA Spectrum.

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

Cluster.xml

Contains all cluster events, including IBM and Microsoft.

IBM-Cluster-all.xml

Contains all of the IBM cluster events.

IBM-run-status.xml

Contains all of the IBM cluster events that are related to Status (such as up, down, offline).

MS-Cluster-all.xml

Contains all of the Microsoft cluster events.

MS-run-status.xml

Contains the Microsoft cluster events that are related to Status (such as up, down, offline).

ClusterTrap.xml

Contains only the trap events from IBM and Microsoft clusters.

Cluster-spectrum-managing.xml

Contains the CA Spectrum management events, such as cluster proxy events, management events, and polling events.

Availability reports provide historical information about uptime and downtime for assets in the IT infrastructure. The calculation of uptime and downtime depends on the UP and DOWN events that correspond to the cluster model type.

Note: You can use the event codes of the .xml files to generate event reports in Report Manager. For more information, see the *Report Manager User Guide*. You can also generate reports using the predefined event filter files. For more information, see the *Report Manager Installation and Administration Guide*.

Alarms and Fault Management

Knowing about certain activities, such as a resource group migration or a cluster node failure, can minimize potential problems in your cluster environment. To alert you, CA Spectrum generates alarms and uses advanced fault management techniques to isolate the root cause.

Problems with a single device can cause several other devices in your network to generate events. Deciding which devices are the root cause of an alarm can be challenging. For example, when you lose contact with the Cluster Manager (the proxy manager), you also lose proxy communication with the cluster nodes that it manages. As a result, alarms are generated for the Cluster Manager and each of its managed components. Sifting through potentially hundreds of simultaneously produced alarms manually to pinpoint the problem could be a tedious and error-prone process. Using fault isolation techniques, Cluster Manager significantly simplifies the troubleshooting process by automatically correlating these alarms to identify a single root cause. As a result, you can identify and correct the problem more quickly.

Alarms and fault isolation vary by cluster technology. Cluster Manager evaluates which devices are issuing alarms and the type of events the devices generate. CA Spectrum uses all available information to correlate the alarms to the appropriate root cause, only alarming on the isolated faulty device. Cluster Manager relies on the combination of standard CA Spectrum monitoring, proxy management, state-polling, and traps to create meaningful events and alarms.

Note: In addition to what is provided out-of-box, you can also create your own custom watches to generate events and alarms on other specific metrics. For information about creating watches, see the *Watches User Guide*.

More information:

Alarms for IBM PowerHA (see page 51)
Alarms for MSCS (see page 67)
Cluster Manager Alarms (see page 33)
Proxy Management (see page 33)
Alarm Correlation (see page 35)

Cluster Manager Alarms

Alarms are created from information that is obtained from technology-specific traps and polling. To alert you to important activities within your cluster environment, Cluster Manager generates (or clears) alarms for the following conditions:

- A Cluster Manager (proxy) is down or communication lost
- Multiple cluster technology AIMs manage the same cluster
- A cluster is up, down, not configured, or in an unknown state
- A cluster node is up, down, joining, leaving, paused, or in an unknown state
- A resource group is online, offline, pending, unmanaged, in an unknown state, in various other states, or has produced an error
- A resource group migrates from one node to another
- A resource is online, online-pending, offline, offline-pending, initializing, pending, inherited, failed, or in an unknown state

Note: Alarms and conditions vary by cluster technology.

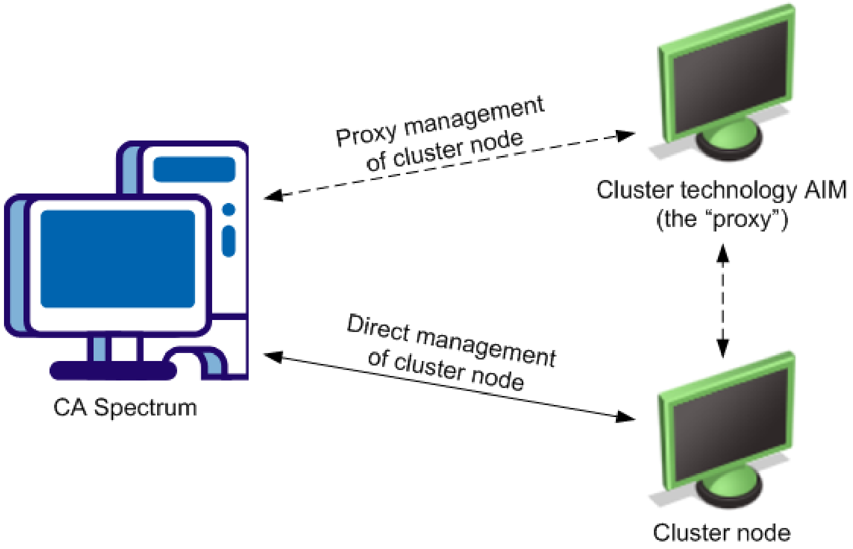
More information:

State Monitoring for IBM PowerHA (see page 52)
State Monitoring for MSCS (see page 68)

Proxy Management

Managing cluster components by a cluster technology AIM provides CA Spectrum a unique management opportunity. Using this approach, CA Spectrum has an alternate management perspective in addition to standard device monitoring methods.

Along with gathering information directly from a device, CA Spectrum also simultaneously gathers information specific to cluster components from the cluster technology AIM. The AIM serves as a "proxy" from which CA Spectrum gathers information specific to the cluster technologies. Management of a device using an alternate source (such as the AIM) rather than the device directly is called *proxy management*.


Proxy management of cluster node
Cluster technology AIM (the “proxy”)
Direct management of cluster node
CA Spectrum
Cluster node

CA Spectrum fault isolation handles this dual management by producing the following alarms:

Proxy management alarms

By using the cluster technology AIM for management, proxy-related alarms can be generated. These alarms are unique because they alert you when acquisition of cluster-specific information through the proxy is affected, not the state of the device or direct (SNMP) management. When contact through the proxy is lost, you could be missing important cluster-specific information about your environment. Proxy management alarms are of major severity and are not clearable by the user.

Proxy unavailable

When CA Spectrum cannot communicate with the cluster technology AIM, a proxy unavailable alarm is generated on the Cluster Manager model.

The following text is used for the proxy unavailable alarm:

```
CLUSTER MANAGER UNAVAILABLE
```

Proxy lost

When CA Spectrum cannot obtain information about the managed device by way of the proxy, a proxy lost alarm is generated. A proxy lost alarm is generated for the following conditions:

- When CA Spectrum cannot communicate with the vendor-specific Cluster Manager model. A proxy unavailable alarm on the Cluster Manager model is generated as well as a proxy lost alarm for each of its managed components.
- When the cluster technology AIM cannot successfully communicate with the cluster node.

The following text is used for the proxy lost alarm:

CLUSTER MANAGER PROXY LOST FOR *cluster_entity*

Cluster entity values include the cluster, cluster node, resource group, and resource.

A proxy lost alarm is generated only for entities that Cluster Manager manages. If the host is removed from management by the proxy, the respective proxy management alarms are cleared.

Enhanced contact lost alarms

Standard CA Spectrum alarms that indicate loss of contact with the proxy contain added correlation of Cluster Manager proxy management alarms. These proxy management alarms indicate loss of cluster-specific data acquisition.

The following text is used for the contact lost alarm:

```
DEVICE HAS STOPPED RESPONDING TO POLLS
```

Alarm Correlation

Using standard CA Spectrum fault management, state-monitoring data, and added information from the proxy, Cluster Manager automatically correlates the alarms to identify a single root cause. Various state-monitoring and proxy-related alarms are correlated to an alarm on the relevant model to pinpoint the true root cause, such as:

- Contact lost
- Management lost
- Entity down, offline, or in a problem state
- Maintenance
- Hibernation

Cluster Manager provides many default correlations. To view or modify correlations, use the Condition Correlation Editor in OneClick.

Note: After an alarm has been issued, use the Impact tab for the alarm to view any correlated or symptomatic alarms.

More information:

How to Change Cluster Node Down Alarm Correlation (see page 75)
How to View and Modify Cluster Manager Correlations (see page 74)

Chapter 3: Maintaining Your Cluster Manager Implementation

This section contains the following topics:

Updating Cluster Data

When the CA Spectrum administrator runs the initial Discovery process, Cluster Manager populates the Explorer tab in the Navigation panel with your cluster environment models. After Cluster Manager builds this initial hierarchy, your cluster environment can change. Cluster Manager continually works to keep this information updated. The information is useful for troubleshooting issues and optimizing performance only when it accurately reflects your environment.

Understanding how and when the information is updated can help you better evaluate the data and how your cluster environment is operating. For example, the following events can change your cluster environment configuration:

- Creating or deleting clusters, cluster nodes, resource groups, and resources
- Migration of cluster components from one entity to another

To keep your information accurate, Cluster Manager detects these changes by polling the AIM. Your modeled cluster environment is updated in CA Spectrum at each polling cycle. When a change in your cluster environment is detected, CA Spectrum performs the following tasks:

- Updates the placement of your cluster component models in the Cluster Manager hierarchy in the Explorer view
- Automatically rediscovers connections to the affected components in the Universe topology

CA Spectrum also receives traps from the AIM and generates the corresponding events. By reviewing the event log, you can find out when changes occur, such as when a resource group has migrated.

Important! To reestablish connections to your cluster component models correctly, all interconnecting routers and switches must be modeled. If these models do not exist before connections to your cluster components are rediscovered, CA Spectrum cannot resolve those connections. As a result, CA Spectrum cannot display the information correctly in the Universe topology view.

Controlling Polling Intervals

Polling intervals control how often information is obtained from managed devices. To keep data for your managed cluster environments current, Cluster Manager uses the polling intervals set on the following components:

- **Cluster technology AIM**

  The AIM polling interval indicates how often the AIM queries the cluster components for information. The AIM polling interval exists in the AIM, but you can modify this value from within CA Spectrum. The default value is 300 seconds with a minimum value of 30 seconds.

- **Cluster Manager model**

  The polling interval on the Cluster Manager model determines how often CA Spectrum polls the cluster technology AIM. The default value is 300 seconds with a minimum value of 30 seconds. This setting is available on the CA Spectrum Modeling Information view for the Cluster Manager (Host_systemEDGE) model.

More information:

Controlling the MSCS AIM Polling Interval (see page 71)
Controlling the HACMP AIM Polling Interval (see page 55)

Modifying Cluster Manager Management and Models

When changing your modeled environment, consider the following behaviors:

- When Cluster Manager no longer manages a cluster node, the model moves to the Lost and Found (LostFound), except in the following cases:
  - Virtual Host Manager is managing the host.
  - The host is in a global collection.

- When cluster component names change, Cluster Manager reflects the new values automatically.
- When the IP address or MAC address for a cluster node model is modified, connections to any connecting devices are automatically updated.

How to Convert an ICMP (Pingable) Model to SNMP-Managed

You can model a cluster node as an ICMP (Pingable) model and then later install an SNMP agent on the host. To take advantage of the SNMP capabilities, the cluster node must be remodeled.

Perform a discovery for the node manually to replace the model. A new model is created and then is pulled into Cluster Manager management during the next Cluster Manager discovery.

Deleting Cluster Manager Models

Consider the following behaviors and restrictions regarding the deletion of cluster component models in your CA Spectrum modeled environment:

- Models typically can be deleted from OneClick at any time for various reasons. However, Cluster Manager restricts your ability to delete models from the Cluster Manager hierarchy in the Navigation panel. To delete models manually, you have the following options:
  - Delete the Cluster Manager model.
  - Remove a cluster component using the vendor-specific cluster management tool.
- In Cluster Manager, models are sometimes deleted automatically. The following circumstances cause CA Spectrum to delete Cluster Manager models automatically:
  - A Cluster Manager model is deleted. If you delete a Cluster Manager model, CA Spectrum deletes all associated models.
  - An entity is removed from a supported cluster environment. As you update your cluster environment by modifying cluster, cluster node, resource group, and resource allocation, CA Spectrum also modifies those models accordingly. This update includes deleting respective models and their children where appropriate.
  - Upgraded models exist. In some cases, a cluster node is first modeled for Cluster Manager without SNMP capabilities. If SNMP capabilities are later added to a node, the previous model is deleted and replaced with the new, manually discovered SNMP-managed model.

- Hosts that both Virtual Host Manager and Cluster Manager manage adhere to all the standard modeling behaviors of virtual machines. These models cannot be deleted from the topology.
- When a Cluster Manager (Host_SystemEDGE) model is deleted, the corresponding cluster containers are destroyed. All cluster node models in the containers are moved to the Lost and Found (LostFound). An exception is when a cluster node is in a global collection, in which case, the model remains in the global collection.
- When all cluster components for a particular cluster technology are deleted, the cluster technology folder remains in the Cluster Manager hierarchy. An unbolded label indicates an empty folder.

Deleting Models When Using Multiple AIM Solutions

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

- If you plan to no longer manage models using Virtual Host Manager, configure Virtual Host Manager delete settings to retain models. Otherwise, Virtual Host Manager deletes the cluster node model initially, losing any history or customization on the models. Cluster Manager then recreates the cluster node model during the next Cluster Manager discovery, which occurs on the next poll cycle.
- When Virtual Host Manager unmanages a cluster node and the model is retained, it is pulled back into Cluster Manager management automatically.
- If a node is removed from management by a solution, the rules of the remaining solutions are reapplied in the ranked order. Typically, any changes are made at the next polling cycle.
- When you remove a cluster node model from management by Cluster Manager, it is removed from the cluster container. If ADES Manager continues to manage the host, the model does not appear in the ADES Managed Hosts container automatically. To move the model into the ADES Managed Hosts container, cut and paste the model from the Lost and Found (or global collection, if applicable).

  Note: Cluster node models that are removed from Cluster Manager management are moved to the Lost and Found (LostFound). An exception is when a cluster node is in a global collection, in which case, the model remains in the global collection.
- The Cluster Manager hierarchy synchronizes after the Lost and Found (LostFound) is emptied.

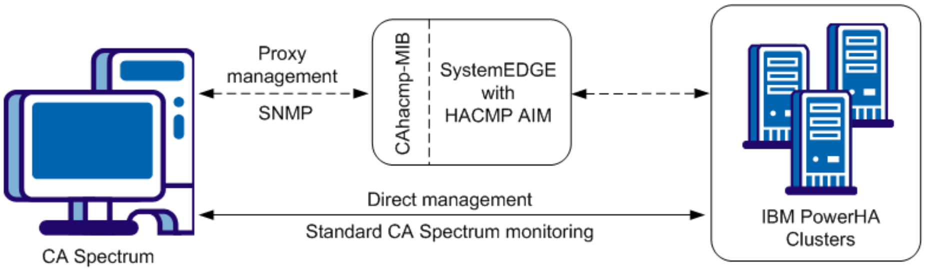
Chapter 4: IBM PowerHA

This section contains the following topics:

Solution Architecture for IBM PowerHA

CA Spectrum gathers information about your IBM PowerHA cluster environment using two different methods. As with other CA Spectrum-managed devices, Cluster Manager uses standard CA Spectrum monitoring. In addition, Cluster Manager also retrieves specialized information for your IBM PowerHA environment from a proxy manager, the HACMP AIM.

The following diagram shows how CA Spectrum gathers information about your IBM PowerHA cluster environment:



The SystemEDGE agent with the HACMP AIM resides on its own host. This host is referred to as the IBM PowerHA Cluster Manager. The HACMP AIM obtains information from the IBM PowerHA cluster environment and writes this data to a CA-developed MIB (CAhacmp-MIB). CA Spectrum then uses SNMP to retrieve this information from the MIB and uses it to model and monitor your IBM PowerHA cluster components in OneClick.

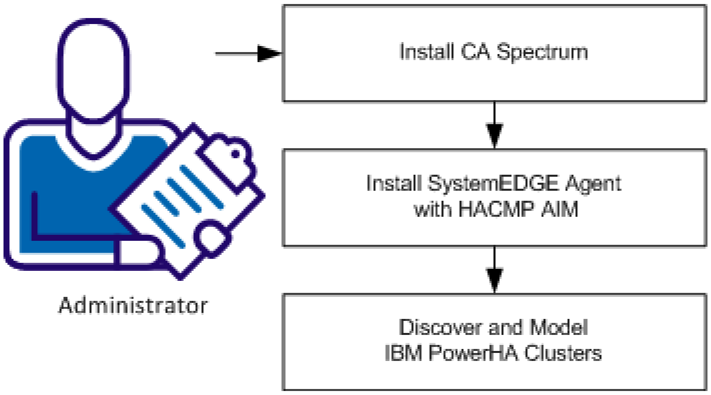
Cluster Manager can support multiple HACMP AIMs either within a single SpectroSERVER or distributed across multiple landscapes.

Note: For more information about the HACMP MIB, see the *CA Virtual Assurance for Infrastructure Managers Administration Guide*.

How to Set Up Cluster Manager for IBM PowerHA

The following diagram shows the steps that are required for a CA Spectrum administrator to set up Cluster Manager to monitor IBM clusters:

Set Up CA Spectrum Cluster Manager for IBM PowerHA


Install CA Spectrum
Install SystemEDGE Agent with HACMP AIM
Discover and Model IBM PowerHA Clusters
Administrator

Follow these steps:

1. Install CA Spectrum (see page 42).
2. Install SystemEDGE agent with HACMP AIM (see page 43).
3. Discover and Model Your IBM PowerHA Environment (see page 43).

More information:

Node Management and Multiple CA Spectrum AIM Solutions (see page 16)
How to Model Your Environment When Using Multiple AIM Solutions (see page 18)

Install CA Spectrum

Cluster Manager is included in all CA Spectrum extraction keys. When you install CA Spectrum, the Cluster Manager components are automatically installed.

Follow this step:

- Install CA Spectrum r9.2.3 or later.

  Important! Do not install the SpectroSERVER on a host that Cluster Manager is going to manage.

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

Install the SystemEDGE Agent and HACMP AIM

After CA Spectrum has been installed, install and configure the proxy manager; for IBM clusters, the proxy manager is the HACMP AIM.

The HACMP AIM is a specialized SystemEDGE AIM and resides on its own host. This host is referred to as the IBM PowerHA Cluster Manager.

When configuring the HACMP AIM, you manually specify the IBM PowerHA clusters to manage. Although your implementation can consist of multiple HACMP AIMs, manage each cluster with a single HACMP AIM only.

Follow this step:

- Install the SystemEDGE agent and load and configure the HACMP AIM on a host other than where CA Spectrum is installed. Note the following requirements:
  - Install only a single AIM on a particular SystemEDGE host.
  - Do not install the SystemEDGE agent and HACMP AIM on a node that Cluster Manager is going to manage.
  - Register each cluster and cluster node with a single HACMP AIM only.

  Note: For more information, see the *CA Virtual Assurance for Infrastructure Managers Installation Guide* and *CA Virtual Assurance for Infrastructure Managers Administration Guide.*

  After the HACMP AIM has been successfully installed and configured, it begins gathering data for its managed components. This information is made available in the MIB.

  You can now discover and model your IBM cluster environment in CA Spectrum.

Discover and Model Your IBM PowerHA Environment

After you have installed the necessary components, discover and model any entities in your IBM PowerHA cluster environment that Cluster Manager is going to manage.

Follow these steps:

1. Run a CA Spectrum Discovery for modeling the IBM PowerHA Cluster Manager and connecting devices (see page 44).
2. (Optional) Upgrade the SystemEDGE model, if necessary (see page 45).

   Note: This step is required only if the SystemEDGE host has been modeled in CA Spectrum before installing the HACMP AIM on the agent.
3. Let Cluster Manager discovery run (see page 45).

Run CA Spectrum Discovery to Model the IBM PowerHA Cluster Manager and Connecting Devices

After the SystemEDGE agent and HACMP AIM are set up, model the IBM PowerHA Cluster Manager and any connecting devices in CA Spectrum. You can use standard CA Spectrum Discovery to do the following actions:

- Model the IBM PowerHA Cluster Manager, which must be modeled with a read/write community string.
- Model the necessary upstream routers and switches of your IBM PowerHA cluster environment so that connections from the cluster models can later be established.

Important! Do not include cluster nodes. Clusters, cluster nodes, resource groups, and resources are discovered and modeled automatically using information from the AIM.

Note: For details about how to perform a Discovery, see the *Modeling and Managing Your IT Infrastructure Administrator Guide*.

Gather the correct community strings, IP addresses, and port numbers for any SNMP agents that run on a nonstandard port. Note the following guidelines when configuring your Discovery parameters:

- Include IP addresses for all IBM PowerHA Cluster Managers and interconnecting switches and routers.
- Model the IBM PowerHA Cluster Manager with a read/write community string. If you are modeling the IBM PowerHA Cluster Manager in this Discovery, place its community string appropriately in the SNMP Information ordered list. Alternatively, you can change the community string for the IBM PowerHA Cluster Manager to its read/write value after the discovery.
- Determine pingable MAC addresses during connectivity mapping by using the "ARP Tables for Pingables" option.

  Note: Using this option can increase the time Discover Connections takes to run.
- Add any nonstandard SNMP ports using Advanced Options.

Discovery creates models for the following entities and adds them to your network topology in CA Spectrum:

- IBM PowerHA Cluster Manager.

  Note: If the Discovery process did not assign the read/write community string to this model, update this setting manually. Use the CA Spectrum Modeling Information subview for the model.
- The upstream switches and routers that connect the IBM PowerHA cluster nodes to your network.

When Discovery has completed and these models exist in CA Spectrum, Cluster Manager discovery begins.

Note: Instead of using standard CA Spectrum Discovery, you can manually model your IBM PowerHA Cluster Manager by IP address or host name. If you do, model the upstream devices first (since modeling the IBM PowerHA Cluster Manager automatically triggers a Cluster Manager discovery). Modeling in the proper order allows the correct creation of connections in the topology between your cluster nodes and the remainder of your network. For more information, see *Modeling and Managing Your IT Infrastructure Administrator Guide*.

More information:

Cluster Manager Discovery (see page 45)

Upgrade the SystemEDGE Host Model (If Necessary)

If the SystemEDGE host model was created before loading the HACMP AIM on the agent, the existing model is not compatible with Cluster Manager. Upgrade the SystemEDGE host (Host_systemEDGE) model so that Cluster Manager can access the HACMP AIM capabilities in SystemEDGE.

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

The SystemEDGE host model is upgraded to support the HACMP AIM.

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

Cluster Manager Discovery

Cluster Manager discovery is the automatic discovery and modeling process within CA Spectrum of cluster components. The IBM PowerHA Cluster Manager initiates this process.

With communication between CA Spectrum and the HACMP AIM established, Cluster Manager gathers information about your IBM PowerHA environment from the HACMP AIM. A list of cluster nodes is passed to AutoDiscovery for modeling. For cluster node models, an SNMP-managed model is created if an SNMP agent exists on the host; otherwise, an ICMP (Pingable) model is created.

New cluster-related models appear in the Cluster Manager hierarchy in the Explorer view and are placed into new cluster containers in the topology view. Connections to any upstream devices are made.

Note: If a cluster node is already modeled in your CA Spectrum-managed network before Cluster Manager discovery, it is not modeled again. However, the model is included in the cluster container topology.

After the initial modeling, Cluster Manager discovery runs automatically at a frequency that is based on the IBM PowerHA Cluster Manager model poll cycle. During subsequent Cluster Manager discoveries, the modeling within CA Spectrum is updated with any changes in your cluster environment.

More information:

Topology View (see page 25)

Models Created for IBM PowerHA

Cluster Manager provides several models to represent the components of your IBM PowerHA cluster environment, as follows:

IBM PowerHA Cluster Manager

Model Type: Host_systemEDGE

Represents the host that contains the HACMP AIM. The HACMP AIM monitors the IBM PowerHA cluster elements (clusters, nodes, resource groups, and resources) in your environment.

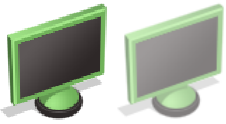
IBM PowerHA Cluster

Model Type: ClusterIBMCluster

Contains cluster node and resource group models that belong to the cluster. You cannot add or remove models from a cluster container, and you cannot destroy the container itself. When possible, this container model is created alongside the IBM PowerHA Cluster Manager model.

Note: If the IBM PowerHA Cluster Manager is a virtual machine, the cluster container is placed in the same topology as the physical host container.

IBM PowerHA Cluster Node



Represents a cluster node in an IBM PowerHA cluster environment. Cluster nodes are modeled as SNMP-managed elements when possible. A cluster node can be active or inactive.

An active node has resource groups currently running on it and is represented with a solid (nontransparent) icon. An inactive node does not have any resource groups and is represented with a faded (transparent) icon. When resource groups fall over from one node to another, changing the state of the node, the icon transitions automatically.

Note: Unlike a model in maintenance mode or hibernation mode, the inactive node model is fully functional. Data is gathered for the node, and any alarm activity or events for the node are generated on the model.

IBM PowerHA Cluster Resource Group

Model Type: ClusterIBMResourceGroup

Represents a resource group.

IBM PowerHA Cluster Resource

Model Type: ClusterIBMResource

Represents a resource.

More information:

Topology View (see page 25)

Custom Subviews for IBM PowerHA

Custom subviews in the Component Detail panel provide detailed information about the components in your cluster environment. You can view information specific to IBM PowerHA clusters by:

- IBM PowerHA Cluster Manager (see page 48)
- IBM PowerHA Cluster Component (see page 49) (Cluster, Cluster Node, Resource Group, Resource)

IBM PowerHA Cluster Manager

Using subviews that are provided for the IBM PowerHA Cluster Manager (HACMP AIM), you can view the following information:

- Information specific to the IBM PowerHA Cluster Manager host. Data includes the agent version, agent polling interval, and when the HACMP AIM MIB (CAhacmp-MIB) was last updated.
- List of clusters that have been registered to the AIM.
- Consolidated information about all cluster components that this HACMP AIM manages.

The following procedure describes how to view information for an IBM PowerHA Cluster Manager.

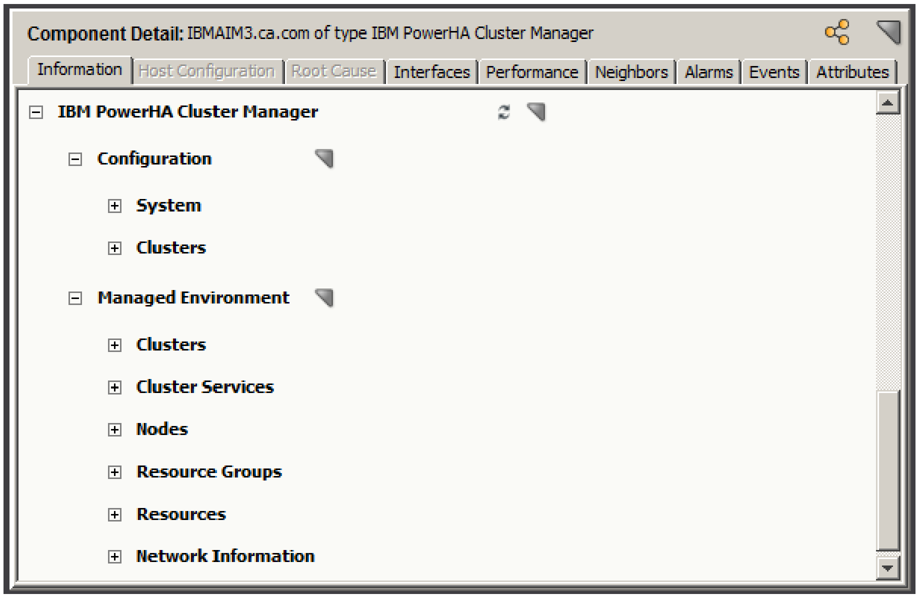
Follow these steps:

1. Select the IBM PowerHA Cluster Manager model in the Universe hierarchy or topology.

   The Component Detail panel displays information for the selected IBM PowerHA Cluster Manager.

2. In the Information tab in the Component Detail panel, expand the IBM PowerHA Cluster Manager subview.

   The expanded subview appears, as follows:



Component Detail: IBMAIM3.ca.com of type IBM PowerHA Cluster Manager

⊟ IBM PowerHA Cluster Manager

⊟ Configuration

⊞ System

⊞ Clusters

⊟ Managed Environment

⊞ Clusters

⊞ Cluster Services

⊞ Nodes

⊞ Resource Groups

⊞ Resources

⊞ Network Information

The following subviews are available for an IBM PowerHA Cluster Manager:

Configuration

Provides information specific to the IBM PowerHA Cluster Manager, including:

- Information about the SystemEDGE agent including version, when the MIB was last updated, and polling interval. You can also modify the polling interval, as described in Controlling the HACMP AIM Polling Interval (see page 55).
- List of clusters that have been registered to this AIM and their respective readiness

Managed Environment

Provides consolidated information about all the entities that this AIM manages, including cluster components, services, resource groups, resources, and network information.

IBM PowerHA Cluster Component

You can view information for any of your clusters or cluster components (cluster node, resource group, resource) in your managed IBM PowerHA cluster environment. Views are tailored to the entity type, providing information that is specific to the component.

The following procedure describes how to view information for an IBM PowerHA cluster or cluster component.

Follow these steps:

1. Select an IBM PowerHA Cluster, Cluster Node, Resource Group, or Resource model.

   The Component Detail panel displays information for the selected model.

2. In the Information tab in the Component Detail panel, expand the respective cluster-related subview for the model.

   The expanded subview appears, as follows, depending on the model type:

   Cluster Information

   Provides general cluster information for the selected cluster model. Data includes cluster states, number of nodes, and instance name as registered in the AIM.

   Node Information

   Provides general node information such as the node state and the number of network interfaces it has. CPU usage and memory statistics are also provided.

Resource Group Information

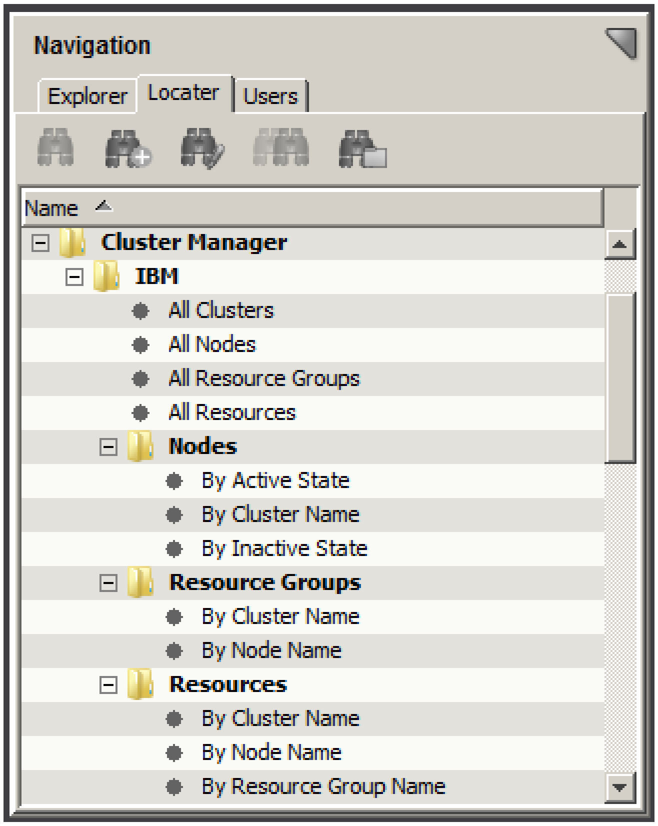
Provides statistics such as the number of resources in the group, the node currently owning the group as well as the previous node. The number of startup, fallover, and fallback policies for the group are also provided.

Resource Information

Provides the resource type and index information.

Locater Searches for IBM PowerHA

You can use the Locater tab to run preconfigured searches. The search options are grouped under the Cluster Manager, IBM folder on the Locater tab, as shown:



These detailed searches can help you investigate information that is related to IBM PowerHA cluster entities that have been modeled in the CA Spectrum database.

Note: Only users with the appropriate privileges can access Cluster Manager searches. For more information, see the *Administrator Guide*.

Alarms for IBM PowerHA

To alert you to problems within your IBM PowerHA cluster environment, CA Spectrum generates alarms. Quickly identifying any device faults helps you to maximize your system up-time and the reliability of your cluster environment and high availability applications. Alarms are created from information that is obtained from technology-specific traps and polling. The following sections describe the Cluster Manager events and alarms for your IBM PowerHA cluster environment.

Note: To view specific event definitions that are related to Cluster Manager, use the Event Configuration application.

More information:

Alarms and Fault Management (see page 32)
Traps for IBM PowerHA (see page 51)
State Monitoring for IBM PowerHA (see page 52)
Viewing and Configuring Events and Alarms (see page 73)

Traps for IBM PowerHA

CA Spectrum supports all traps that the HACMP AIM generates. An event is created for any trap activity and is reported initially on the IBM PowerHA Cluster Manager model. Some events are then forwarded to a corresponding cluster entity type (that is, the "destination" entity), depending on the type of trap.

The following table provides the traps and destination entity type and indicates whether the trap generates an alarm by default.

Trap Name	Trap OID	Alarm?	Destination Entity
hacmpAimInstanceAddedTrap	1.3.6.1.4.1.546.1.1.0.165800	No	Cluster Manager
hacmpAimInstanceRemovedTrap	1.3.6.1.4.1.546.1.1.0.165801	No	Cluster Manager
hacmpAimInstanceDataStatusChanged	1.3.6.1.4.1.546.1.1.0.165802	No	Cluster Manager
hacmpAimNodeAddedTrap	1.3.6.1.4.1.546.1.1.0.165803	No	Cluster Manager
hacmpAimNodeRemovedTrap	1.3.6.1.4.1.546.1.1.0.165804	No	Cluster Manager
hacmpAimResourceGroupAddedTrap	1.3.6.1.4.1.546.1.1.0.165805	No	Cluster Manager
hacmpAimResourceGroupRemovedTrap	1.3.6.1.4.1.546.1.1.0.165806	No	Cluster Manager
hacmpAimResourceGroupMigration	1.3.6.1.4.1.546.1.1.0.165807	No	Resource Group
hacmpAimResourceAddedTrap	1.3.6.1.4.1.546.1.1.0.165808	No	Cluster Manager

Trap Name	Trap OID	Alarm?	Destination Entity
hacmpAimResourceRemovedTrap	1.3.6.1.4.1.546.1.1.0.165809	No	Cluster Manager
aggregateStateTrap*	1.3.6.1.4.1.546.1.1.0.20	Yes*	various*

* The aggregateStateTrap is a SystemEDGE trap. Alarms are generated for certain aggregateStateTrap conditions. For more information, see Self Monitors for IBM PowerHA (see page 54).

Note: For more information about traps that the HACMP AIM generates, see the *CA Virtual Assurance for Infrastructure Managers Administration Guide*. You can also use MIB Tools to view the traps in the "CAhacmp-MIB" MIB. For more information, see the *Modeling and Managing Your IT Infrastructure Administrator Guide*.

More information:

How to View and Modify Cluster Manager Event Definitions (see page 73)

State Monitoring for IBM PowerHA

Cluster Manager monitors the state of various cluster components in your environment and obtains this information from the following sources:

- Polling the "CAhacmp-MIB" MIB. More than 100 objects are monitored regularly about the elements in your cluster environment. This information is updated in CA Spectrum according to the polling cycle. Cluster Manager derives pertinent information from these objects to create various events and alarms that provide insight into the health and status of your environment.
- Self-monitor traps (see page 54). When installed, the HACMP AIM configures self monitors on the SystemEDGE agent which track various resources and activities of the managed cluster components. The monitors are threshold-based, and an aggregateState trap is sent when a threshold is violated. CA Spectrum then generates an event and, depending on the current severity state of the monitor, an applicable alarm. Data that is gathered from self monitors includes CPU or memory usage for a node.

Cluster Manager uses information from both sources to monitor the state of your cluster components. Alarms are generated and, when the condition has been corrected, cleared automatically. All state-based alarms are also user-clearable. When both trap and polling sources reveal the same activity, Cluster Manager identifies the overlap. A single alarm is created, with the alarm that polling generates taking precedence.

When a resource group moves from a primary node to a secondary node, an alarm occurs. When the resource group moves from the secondary node back to the primary, a new alarm is generated for the latest migration. The original alarm does not clear automatically, but it is user-clearable.

The following table lists the state-based alarm information by cluster component:

Entity	State	CA Spectrum Alarm Severity
Cluster	Up	Clear
Cluster	Down	Critical (Red)
Cluster	Unknown	Major (Orange)
Cluster	Not Configured	Critical (Red)
Cluster	Network state down*	Major (Orange)
Node	Up	Clear
Node	Down	Critical (Red)
Node	Joining	Event only
Node	Leaving	Event only
Node	Unknown	Major (Orange)
Node	High CPU Utilization*	Major (Orange)
Node	High Memory Utilization*	Major (Orange)
Node	Network interface state down*	Major (Orange)
Resource Group	Unknown	Major (Orange)
Resource Group	Online	Clear
Resource Group	Offline	Critical (Red)
Resource Group	Acquiring	Event only
Resource Group	Releasing	Event only
Resource Group	Error	Critical (Red)
Resource Group	Onlinesec	Clear
Resource Group	Acquiringsec	Event only
Resource Group	Releasingsec	Event only
Resource Group	Errorsec	Critical (Red)
Resource Group	Offline_due_to_failover	Minor (Yellow)

Entity	State	CA Spectrum Alarm Severity
Resource Group	Off_line_due_to_parent_off	Critical (Red)
Resource Group	Unmanagedsec	Minor (Yellow)
Resource Group	Offline_due_to_lack_of_node	Critical (Red)
Resource Group	Unmanaged	Minor (Yellow)
Resource Group	Parent changes	Major (Orange)

* Alarms generated from self-monitor aggregateStateTrap.

More information:

How to View and Modify Cluster Manager Event Definitions (see page 73)

Self Monitors for IBM PowerHA

Self monitors are threshold-based watches that are configured on the SystemEDGE agent. When installed, the HACMP AIM configures self monitors that are specific to the cluster environment. The HACMP AIM sets the initial severities and threshold values, but you can access and modify the values from within OneClick.

When a configured threshold is violated, the SystemEDGE agent sends the pertinent information to CA Spectrum using the aggregateStateTrap. CA Spectrum then generates an event and forwards the event to the respective entity.

For the following monitors only, CA Spectrum generates alarms by default:

- Node CPU Utilization
- Node Memory Utilization
- Network State
- Network Interface State

The state value as configured for the self monitor determines the severity of the CA Spectrum alarm, as shown in the following table:

HACMP AIM State	CA Spectrum Alarm Severity
1: None/Unknown	Event only
2: OK	Clear
3: Warning	Clear
4: Minor	Minor (Yellow)
5: Major	Major (Orange)

HACMP AIM State	CA Spectrum Alarm Severity
6: Critical	Major (Orange)
7: Fatal	Major (Orange)

More information:

How to View and Modify Threshold Values (see page 78)
How to View and Modify Cluster Manager Event Definitions (see page 73)

Controlling the HACMP AIM Polling Interval

Cluster Manager uses the HACMP AIM for discovery, modeling, and monitoring of your IBM PowerHA environment. The HACMP AIM has its own polling interval, which can be set from within CA Spectrum.

Note: For information about other HACMP AIM settings, see the *CA Virtual Assurance for Infrastructure Managers Administration Guide*.

Follow these steps:

1. Select the IBM PowerHA Cluster Manager model that represents the HACMP AIM.

   The Component Detail panel displays information for the selected IBM PowerHA Cluster Manager.

2. In the Information tab in the Component Detail panel, expand the IBM PowerHA Cluster Manager, Configuration, System subview.

   The expanded System subview appears.

3. For the Agent Polling Interval, click set, modify the value, and press Enter.

   The polling interval for the HACMP AIM is updated.

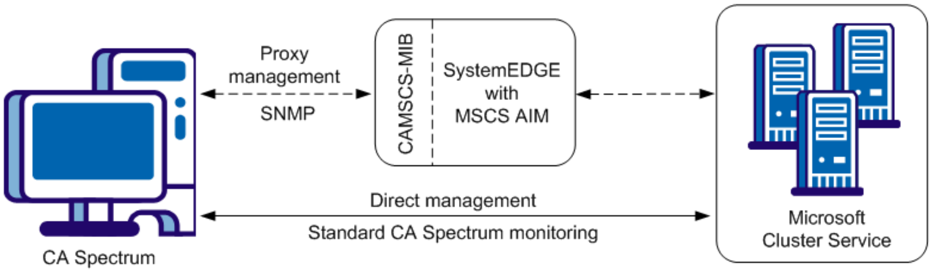
Chapter 5: Microsoft Cluster Service (MSCS)

This section contains the following topics:

Solution Architecture for MSCS

CA Spectrum gathers information about your Microsoft Cluster Service (MSCS) environment using two different methods. As with other CA Spectrum-managed devices, Cluster Manager uses standard CA Spectrum monitoring. In addition, Cluster Manager also retrieves specialized information for your MSCS environment from a proxy manager, the MSCS AIM.

The following diagram shows how CA Spectrum gathers information about your MSCS environment:



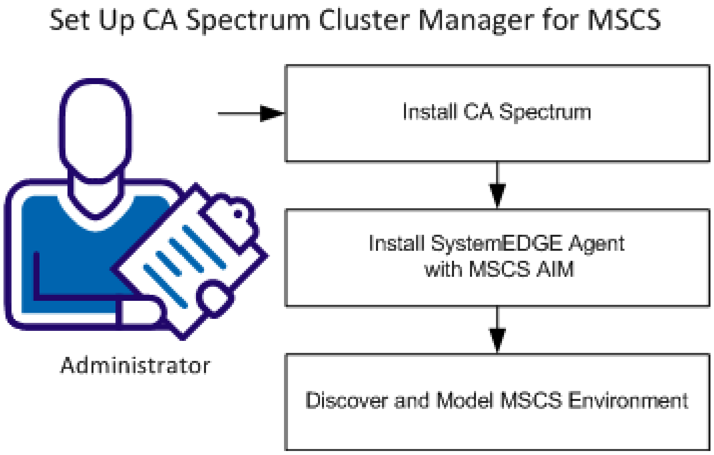
The SystemEDGE agent with the MSCS AIM resides on its own host. This host is referred to as the Microsoft Cluster Manager. The MSCS AIM obtains information from the MSCS environment and writes this data to a CA-developed MIB (CAMSCS-MIB). CA Spectrum then uses SNMP to retrieve this information from the MIB and uses it to model and monitor your MSCS cluster components in OneClick.

Cluster Manager can support multiple MSCS AIMs either within a single SpectroSERVER or distributed across multiple landscapes.

Note: For more information about the MSCS MIB, see the *CA Virtual Assurance for Infrastructure Managers Administration Guide*.

How to Set Up Cluster Manager for MSCS

The following diagram shows the steps that are required for a CA Spectrum administrator to set up Cluster Manager to monitor MSCS clusters:


Set Up CA Spectrum Cluster Manager for MSCS
Administrator
Install CA Spectrum
Install SystemEDGE Agent with MSCS AIM
Discover and Model MSCS Environment

Follow these steps:

1. Install CA Spectrum (see page 58).
2. Install SystemEDGE agent with MSCS AIM (see page 59).
3. Discover and Model Your MSCS Environment (see page 59).

More information:

Node Management and Multiple CA Spectrum AIM Solutions (see page 16)
How to Model Your Environment When Using Multiple AIM Solutions (see page 18)

Install CA Spectrum

Cluster Manager is included in all CA Spectrum extraction keys. When you install CA Spectrum, the Cluster Manager components are automatically installed.

Follow this step:

- Install CA Spectrum r9.2.3 or later.

  Important! Do not install the SpectroSERVER on a host that Cluster Manager is going to manage.

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

Install the SystemEDGE Agent and MSCS AIM

After CA Spectrum has been installed, install and configure the proxy manager; for MSCS, the proxy manager is the MSCS AIM.

The MSCS AIM is a specialized SystemEDGE AIM and resides on its own host. This host is referred to as the Microsoft Cluster Manager.

When configuring the MSCS AIM, you manually specify the MSCS clusters to manage. Although your implementation can consist of multiple MSCS AIMs, manage each cluster with a single MSCS AIM only.

Follow this step:

- Install the SystemEDGE agent and load and configure the MSCS AIM on a host other than where CA Spectrum is installed. Note the following requirements:
  - Install only a single AIM on a particular SystemEDGE host.
  - Do not install the SystemEDGE agent and MSCS AIM on a node that Cluster Manager is going to manage.
  - Register each cluster and cluster node with a single MSCS AIM only.

  Note: For more information, see the *CA Virtual Assurance for Infrastructure Managers Installation Guide* and *CA Virtual Assurance for Infrastructure Managers Administration Guide.*

  After the MSCS AIM has been successfully installed and configured, it begins gathering data for its managed components. This information is made available in the MIB.

  You can now discover and model your MSCS environment in CA Spectrum.

Discover and Model Your MSCS Environment

After you have installed the necessary components, discover and model any entities in your MSCS environment that Cluster Manager is going to manage.

Follow these steps:

1. Run a CA Spectrum Discovery for modeling the Microsoft Cluster Manager and connecting devices (see page 60).
2. (Optional) Upgrade the SystemEDGE model, if necessary (see page 61).

   Note: This step is required only if the SystemEDGE host has been modeled in CA Spectrum before installing the MSCS AIM on the agent.
3. Let Cluster Manager discovery run (see page 61).

Run CA Spectrum Discovery to Model the Microsoft Cluster Manager and Connecting Devices

After the SystemEDGE agent and MSCS AIM are set up, model the Microsoft Cluster Manager and any connecting devices in CA Spectrum. You can use standard CA Spectrum Discovery to do the following actions:

- Model the Microsoft Cluster Manager, which must be modeled with a read/write community string.
- Model the necessary upstream routers and switches of your MSCS environment so that connections from the cluster models can later be established.

Important! Do not include cluster nodes. Clusters, cluster nodes, resource groups, and resources are discovered and modeled automatically using information from the AIM.

Note: For details about how to perform a Discovery, see the *Modeling and Managing Your IT Infrastructure Administrator Guide*.

Gather the correct community strings, IP addresses, and port numbers for any SNMP agents that run on a nonstandard port. Note the following guidelines when configuring your Discovery parameters:

- Include IP addresses for all Microsoft Cluster Managers and interconnecting switches and routers.
- Model the Microsoft Cluster Manager with a read/write community string. If you are modeling the Microsoft Cluster Manager in this Discovery, place its community string appropriately in the SNMP Information ordered list. Alternatively, you can change the community string for the Microsoft Cluster Manager to its read/write value after the discovery.
- Determine pingable MAC addresses during connectivity mapping by using the "ARP Tables for Pingables" option.

  Note: Using this option can increase the time Discover Connections takes to run.
- Add any nonstandard SNMP ports using Advanced Options.

Discovery creates models for the following entities and adds them to your network topology in CA Spectrum:

- Microsoft Cluster Manager.

  Note: If the Discovery process did not assign the read/write community string to this model, update this setting manually. Use the CA Spectrum Modeling Information subview for the model.
- The upstream switches and routers that connect the MSCS cluster nodes to your network.

When Discovery has completed and these models exist in CA Spectrum, Cluster Manager discovery begins.

Note: Instead of using standard CA Spectrum Discovery, you can manually model your Microsoft Cluster Manager by IP address or host name. If you do, model the upstream devices first (since modeling the Microsoft Cluster Manager automatically triggers a Cluster Manager discovery). Modeling in the proper order allows the correct creation of connections in the topology between your cluster nodes and the remainder of your network. For more information, see *Modeling and Managing Your IT Infrastructure Administrator Guide*.

Upgrade the SystemEDGE Host Model (If Necessary)

If the SystemEDGE host model was created before loading the MSCS AIM on the agent, the existing model is not compatible with Cluster Manager. Upgrade the SystemEDGE host (Host_systemEDGE) model so that Cluster Manager can access the MSCS AIM capabilities in SystemEDGE.

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

The SystemEDGE host model is upgraded to support the MSCS AIM.

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

Cluster Manager Discovery

Cluster Manager discovery is the automatic discovery and modeling process within CA Spectrum of cluster components. The Microsoft Cluster Manager initiates this process.

With communication between CA Spectrum and the MSCS AIM established, Cluster Manager gathers information about your MSCS environment from the MSCS AIM. A list of cluster nodes is passed to AutoDiscovery for modeling. For cluster node models, an SNMP-managed model is created if an SNMP agent exists on the host; otherwise, an ICMP (Pingable) model is created.

New cluster-related models appear in the Cluster Manager hierarchy in the Explorer view and are placed into new cluster containers in the topology view. Connections to any upstream devices are made.

Note: If a cluster node is already modeled in your CA Spectrum-managed network before Cluster Manager discovery, it is not modeled again. However, the model is included in the cluster container topology.

After the initial modeling, Cluster Manager discovery runs automatically at a frequency that is based on the Microsoft Cluster Manager model poll cycle. During subsequent Cluster Manager discoveries, the modeling within CA Spectrum is updated with any changes in your cluster environment.

More information:

Topology View (see page 25)

Models Created for MSCS

Cluster Manager provides several models to represent the components of your MSCS environment, as follows:

Microsoft Cluster Manager

Model Type: Host_systemEDGE

Represents the host that contains the MSCS AIM. The MSCS AIM monitors the MSCS elements (clusters, nodes, resource groups, and resources) in your environment.

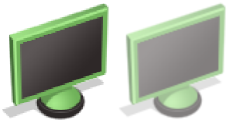
Microsoft Cluster

Model Type: ClusterMSCSCluster

Contains cluster node and resource group models that belong to the cluster. You cannot add or remove models from a cluster container, and you cannot destroy the container itself. When possible, this container model is created alongside the Microsoft Cluster Manager model.

Note: If the Microsoft Cluster Manager is a virtual machine, the cluster container is placed in the same topology as the physical host container.

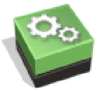
Microsoft Cluster Node



Represents a cluster node in an MSCS environment. Cluster nodes are modeled as SNMP-managed elements when possible. A cluster node can be active or inactive.

An active node has resource groups currently running on it and is represented with a solid (nontransparent) icon. An inactive node does not have any resource groups and is represented with a faded (transparent) icon. When resource groups fail over from one node to another, changing the state of the node, the icon transitions automatically.

Note: Unlike a model in maintenance mode or hibernation mode, the inactive node model is fully functional. Data is gathered for the node, and any alarm activity or events for the node are generated on the model.

Microsoft Cluster Resource Group 

Model Type: ClusterMSCSResourceGroup

Represents a resource group.

Microsoft Cluster Resource

Model Type: ClusterMSCSResource

Represents a resource.

More information:

Topology View (see page 25)

Custom Subviews for MSCS

Custom subviews in the Component Detail panel provide detailed information about the components in your cluster environment. You can view information specific to MSCS clusters by:

- Microsoft Cluster Manager (see page 63)
- MSCS Component (see page 65) (Cluster, Cluster Node, Resource Group, Resource)

Microsoft Cluster Manager

Using subviews that are provided for the Microsoft Cluster Manager (MSCS AIM), you can view the following information:

- Information specific to the Microsoft Cluster Manager host. Data includes the agent version, agent polling interval, and when the MSCS AIM MIB (CAMSCS-MIB) was last updated. You can also control the MSCS AIM polling interval from these views.
- List of clusters that have been registered to the AIM.
- Consolidated information about all cluster components that this MSCS AIM manages.

The following procedure describes how to view information for a Microsoft Cluster Manager.

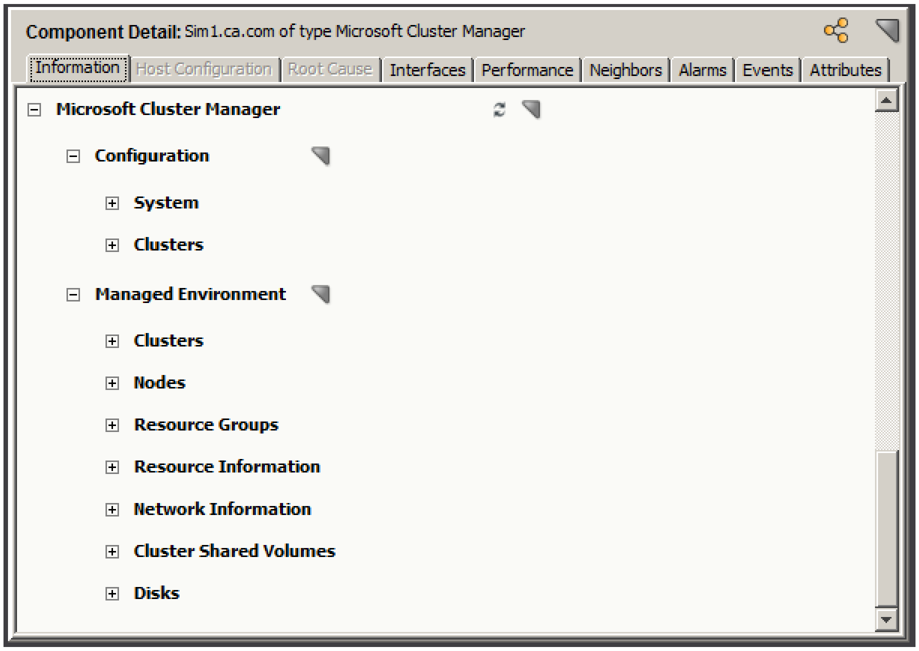
Follow these steps:

1. Select the Microsoft Cluster Manager model in the Universe hierarchy or topology.

   The Component Detail panel displays information for the selected Microsoft Cluster Manager.

2. In the Information tab in the Component Detail panel, expand the Microsoft Cluster Manager subview.

   The expanded subview appears, as follows:



Component Detail: Sim1.ca.com of type Microsoft Cluster Manager

The following subviews are available for a Microsoft Cluster Manager:

Configuration

Provides information specific to the Microsoft Cluster Manager, including:

- Information about the SystemEDGE agent including version, when the MIB was last updated, and polling interval. You can also modify the polling interval, as described in Controlling the MSCS AIM Polling Interval (see page 71).
- List of clusters that have been registered to this AIM and their respective readiness

Managed Environment

Provides consolidated information about all the entities that this AIM manages, including cluster components, resource groups, resources, network information, and storage devices.

MSCS Component

You can view information for any of your clusters or cluster components (cluster node, resource group, resource) in your managed MSCS environment. Views are tailored to the entity type, providing information that is specific to the component.

The following procedure describes how to view information for an MSCS cluster or cluster component.

Follow these steps:

1. Select a Microsoft Cluster, Cluster Node, Resource Group, or Resource model.

   The Component Detail panel displays information for the selected model.

2. In the Information tab in the Component Detail panel, expand the respective cluster-related subview for the model.

   The expanded subview appears, as follows, depending on the model type:

   Cluster Information

   Provides cluster data including:

   - The virtual IP address of the cluster
   - The number of online and failed node resources
   - Log level and the log file size
   - Various timeout values
   - Statistics on resources, crypto checkpoints, registry checkpoints, messages

   Node Information

   Provides cluster node data including:

   - General node information including node state, installed Windows details, and the parent cluster
   - Host CPU usage and memory statistics
   - Data and message information

   Resource Group Information

   Provides resource group data including:

   - The state of the resource group
   - The list of its preferred nodes
   - Failback and failover threshold values

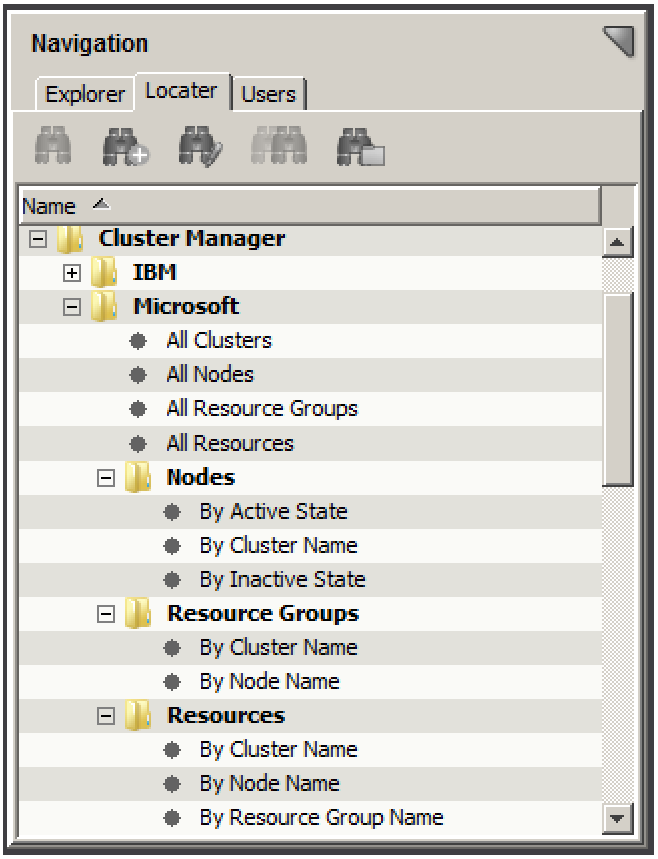
Resource Information

Provides resource data including:

- The state of the resource
- Possible owners of the resource
- Various timeout, polling, and restart values

Locater Searches for MSCS

You can use the Locater tab to run preconfigured searches. The search options are grouped under the Cluster Manager, Microsoft folder on the Locater tab, as shown:



- Cluster Manager
  - IBM
  - Microsoft
    - All Clusters
    - All Nodes
    - All Resource Groups
    - All Resources
    - Nodes
      - By Active State
      - By Cluster Name
      - By Inactive State
    - Resource Groups
      - By Cluster Name
      - By Node Name
    - Resources
      - By Cluster Name
      - By Node Name
      - By Resource Group Name

These detailed searches can help you investigate information that is related to MSCS cluster entities that have been modeled in the CA Spectrum database.

Note: Only users with the appropriate privileges can access Cluster Manager searches. For more information, see the *Administrator Guide*.

Alarms for MSCS

To alert you to problems within your MSCS environment, CA Spectrum generates alarms. Quickly identifying any device faults helps you to maximize your system up-time and the reliability of your cluster environment and high availability applications. Alarms are created from information that is obtained from technology-specific traps and polling. The following sections describe the Cluster Manager events and alarms for your MSCS environment:

Note: To view specific event definitions that are related to Cluster Manager, use the Event Configuration application.

More information:

Alarms and Fault Management (see page 32)
Traps for MSCS (see page 67)
Viewing and Configuring Events and Alarms (see page 73)
State Monitoring for MSCS (see page 68)

Traps for MSCS

CA Spectrum supports all traps that the MSCS AIM generates. An event is created for any trap activity and is reported initially on the Microsoft Cluster Manager model. Some events are then forwarded to a corresponding cluster entity type (that is, the "destination" entity), depending on the type of trap.

The following table provides the traps and destination entity type and indicates whether the trap generates an alarm by default.

Trap Name	Trap OID	Alarm?	Destination Entity
mscsAimInstanceAddedTrap	1.3.6.1.4.1.546.1.1.0.165100	No	Cluster Manager
mscsAimInstanceRemovedTrap	1.3.6.1.4.1.546.1.1.0.165101	No	Cluster Manager
mscsAimInstanceDataStatusChanged	1.3.6.1.4.1.546.1.1.0.165102	No	Cluster Manager
mscsAimResourceGroupMigration	1.3.6.1.4.1.546.1.1.0.165103	No	Resource Group
aggregateStateTrap*	1.3.6.1.4.1.546.1.1.0.20	Yes*	various*

* The aggregateStateTrap is a SystemEDGE trap. Alarms are generated for certain aggregateStateTrap conditions. For more information, see Self Monitors for MSCS (see page 70).

Note: For more information on MSCS traps, use MIB Tools to view the "CAMSCS-MIB" MIB. For more information, see the *Modeling and Managing Your IT Infrastructure Administrator Guide*.

More information:

How to View and Modify Cluster Manager Event Definitions (see page 73)

State Monitoring for MSCS

Cluster Manager monitors the state of various cluster components in your environment and obtains this information from the following sources:

- Polling the CAMSCS-MIB. Hundreds of objects are monitored regularly about the elements in your cluster environment. This information is updated in CA Spectrum according to the polling cycle. Cluster Manager derives pertinent information from these objects to create various events and alarms that provide insight into the health and status of your environment.
- Self-monitor traps (see page 70). When installed, the MSCS AIM configures self monitors on the SystemEDGE agent which track various resources and activities of the managed cluster components. The monitors are threshold-based, and an aggregateState trap is sent when a threshold is violated. CA Spectrum then generates an event and, depending on the current severity state of the monitor, an applicable alarm. Data that is gathered from self monitors includes CPU or memory usage for a node.

Cluster Manager uses information from both sources to monitor the state of your cluster components. Alarms are generated and, when the condition has been corrected, cleared automatically. All state-based alarms are also user-clearable. When both trap and polling sources reveal the same activity, Cluster Manager identifies the overlap. A single alarm is created, with the alarm that polling generates taking precedence.

The following details apply:

- The MSCS AIM does not provide a state for a cluster. The state is determined by pinging the virtual IP address of the cluster.
- When a resource group moves from a primary node to a secondary node, an alarm occurs. When the resource group moves from the secondary node back to the primary, a new alarm is generated for the latest migration. The original alarm does not clear automatically, but it is user-clearable.

The following table lists the state-based alarm information by cluster component:

Entity	State	CA Spectrum Alarm Severity
Cluster	Up	Clear
Cluster	Down	Critical (Red)
Node	Up	Clear
Node	Down	Critical (Red)
Node	Joining	Event only
Node	Paused	Event only
Node	Unknown	Major (Orange)
Node	High CPU Utilization*	Major (Orange)
Node	High Memory Utilization*	Major (Orange)
Resource Group	Unknown	Major (Orange)
Resource Group	Online	Clear
Resource Group	Offline	Critical (Red)
Resource Group	Failed	Critical (Red)
Resource Group	Partial_online	Minor (Yellow)
Resource Group	Pending	Event only
Resource Group	Parent changes	Major (Orange)
Resource	Unknown	Major (Orange)
Resource	Inherited	Event only
Resource	Initializing	Event only
Resource	Online	Clear
Resource	Offline	Major (Orange)
Resource	Failed	Critical (Major)
Resource	Pending	Event only
Resource	Online_Pending	Event only
Resource	Offline_Pending	Event only

* Alarms generated from self-monitor aggregateStateTrap.

More information:

How to View and Modify Cluster Manager Event Definitions (see page 73)

Self Monitors for MSCS

Self monitors are threshold-based watches that are configured on the SystemEDGE agent. When installed, the MSCS AIM configures self monitors that are specific to the cluster environment. The MSCS AIM sets the initial severities and threshold values, but you can access and modify the values from within OneClick.

When a configured threshold is violated, the SystemEDGE agent sends the pertinent information to CA Spectrum using the aggregateStateTrap. CA Spectrum generates an event and forwards the event to the respective entity.

For the following monitors only, CA Spectrum generates alarms by default:

- Node CPU Utilization
- Node Memory Utilization

The state value as configured for the self monitor determines the severity of the CA Spectrum alarm, as shown in the following table:

MSCS AIM State	CA Spectrum Alarm Severity
1: None/Unknown	Event only
2: OK	Clear
3: Warning	Clear
4: Minor	Minor (Yellow)
5: Major	Major (Orange)
6: Critical	Major (Orange)
7: Fatal	Major (Orange)

More information:

How to View and Modify Threshold Values (see page 78)
How to View and Modify Cluster Manager Event Definitions (see page 73)

Controlling the MSCS AIM Polling Interval

Cluster Manager uses the MSCS AIM for discovery, modeling, and monitoring of your MSCS environment. The MSCS AIM has its own polling interval, which can be set from within CA Spectrum.

Note: For information about other MSCS AIM settings, see the *CA Virtual Assurance for Infrastructure Managers Administration Guide*.

Follow these steps:

1. Select the Microsoft Cluster Manager model that represents the MSCS AIM.

   The Component Detail panel displays information for the selected Microsoft Cluster Manager.

2. In the Information tab in the Component Detail panel, expand the Microsoft Cluster Manager, Configuration, System subview.

   The expanded System subview appears.

3. For the Agent Polling Interval, click set, modify the value, and press Enter.

   The polling interval for the MSCS AIM is updated.

Appendix A: Viewing and Configuring Events and Alarms

This section contains the following topics:

How to View and Modify Cluster Manager Event Definitions

To identify the events that Cluster Manager uses, you can use the Event Configuration application in OneClick. Using this application, you can also modify the generated alarm severity that is associated with the event.

Note: Using default settings, Cluster Manager identifies any overlap when multiple monitoring methods reveal the same activity, raising only a single alarm. If you use Event Configuration to add custom alarming, duplicate alarms for the same activity can occur.

Follow these steps:

1. Select Tools, Utilities, Event Configuration.

   The Event Configuration window opens. The Navigation panel displays all events that are defined in your CA Spectrum installation.

2. Filter for events that apply to Cluster Manager. Using the Show field, enter any of the following event codes one at a time:

   - **0x01169b32 - 0x01169b39, 0x01169c** – Related SystemEDGE events
   - **0x0621** – Cluster Manager events

3. Select an event.

   Event details appear in the Contents panel.

4. (Optional) Use the Details panel to modify any parameter for the event, including alarm severity, and click Save.

Note: For more information, see the *Event Configuration User Guide*.

How to View and Modify Cluster Manager Correlations

To view the correlations that Cluster Manager uses, use the Condition Correlation Editor application in OneClick.

Follow these steps:

1. Select Tools, Utilities, Condition Correlation Editor.

   The Condition Correlation Editor opens to the Conditions tab by default. The Conditions tab displays all conditions that are defined in your CA Spectrum installation.

2. On the Conditions tab, enter **0x0621** in the Show field to display conditions that apply to Cluster Manager.

   Only the conditions that apply to Cluster Manager are displayed. The Condition Name identifies the cluster component and its state. A condition is the basic building block of a correlation. Set Event and Clear Event codes for each condition are also displayed.

   Note: For alarm information associated with a displayed event code, use the Event Configuration application.

3. (Optional) Edit a condition to modify any default settings.

4. Select the Rules tab.

   A list of all correlation rules that are defined for your installation are displayed. The rule defines the relationship between two or more conditions when specific criteria are met.

5. Enter **cluster** in the Show field to filter for rules that apply to Cluster Manager.

6. (Optional) Sort the results by Symptom Condition(s) or Root Cause Condition by selecting the respective column heading.

7. Select a rule.

   The conditions that define the rule are displayed in the Rule Criteria tab.

8. (Optional) Edit a rule to modify any default settings.

Note: For more information, see the *Condition Correlation User Guide*.

More information:

How to Change Cluster Node Down Alarm Correlation (see page 75)

How to Change Cluster Node Down Alarm Correlation

When a cluster node fails, Cluster Manager correlates the Cluster Node Down alarm to the Contact Lost alarm with Contact Lost as the root cause. You can modify the correlation behavior using the Condition Correlation Editor so that the Cluster Node Down alarm is the root cause. You can also have no correlation and get both alarms.

More information:

Modify the Correlation Rule (see page 75)
Remove the Correlation Rule (see page 77)

Modify the Correlation Rule

This procedure describes how to change the reported root cause when a cluster node fails by modifying the default correlation behavior.

Follow these steps:

1. Select Tools, Utilities, Condition Correlation Editor.

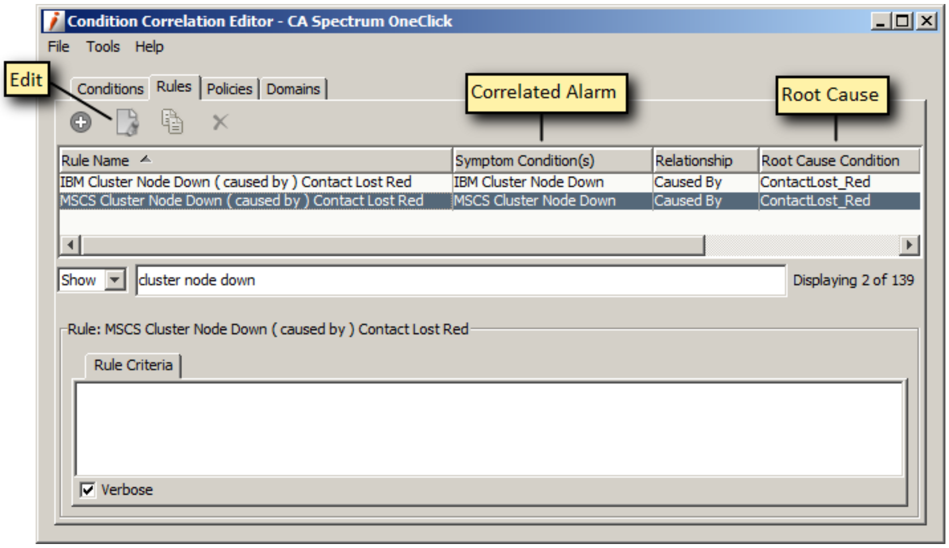
   The Condition Correlation Editor opens.

2. Select the Rules Tab.

   A list of all correlation rules that are defined for your installation are displayed. The following rules apply to Cluster Manager and the Cluster Node Down alarm:

   - IBM Cluster Node Down (caused by) Contact Lost Red
   - MSCS Cluster Node Down (caused by) Contact Lost Red

As shown in the following example, the Symptom Condition of "Cluster Node Down" for each cluster solution correlates to the Root Cause Condition of ContactLost_Red.



Rule Name	Symptom Condition(s)	Relationship	Root Cause Condition
IBM Cluster Node Down (caused by) Contact Lost Red	IBM Cluster Node Down	Caused By	ContactLost_Red
MSCS Cluster Node Down (caused by) Contact Lost Red	MSCS Cluster Node Down	Caused By	ContactLost_Red

Show: cluster node down — Displaying 2 of 139

Rule: MSCS Cluster Node Down (caused by) Contact Lost Red

Rule Criteria

☑ Verbose

3. Select the rule that you want to modify, and click the Edit button.

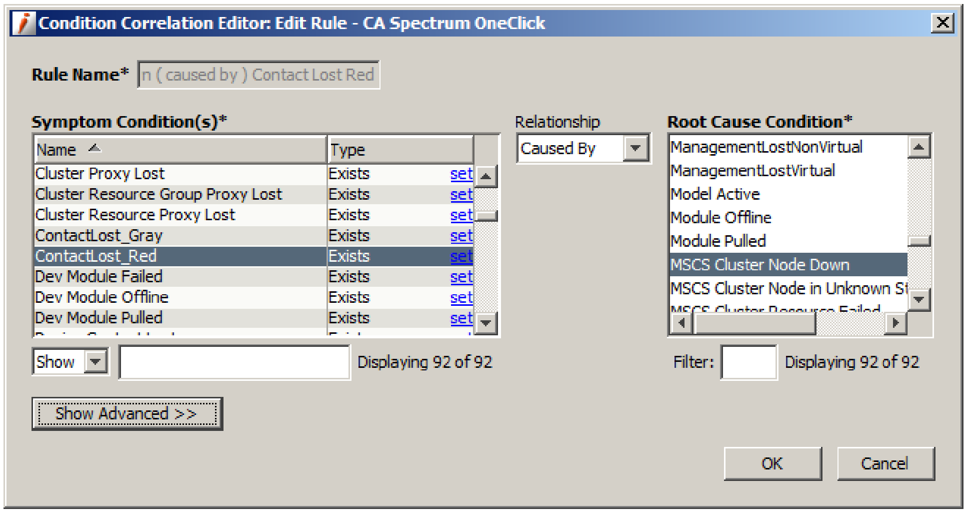
   The Edit Rule window opens.

4. Modify the values as follows:

   a. Select ContactLost_Red as the new Symptom Condition.

   b. Select the appropriate "Cluster Node Down" value as the Root Cause Condition. As defined in the original out-of-box rules, these values are:

      - IBM Cluster Node Down
      - MSCS Cluster Node Down


Condition Correlation Editor: Edit Rule - CA Spectrum OneClick
Show Advanced >>
OK
Cancel

Rule Name* n (caused by) Contact Lost Red

Symptom Condition(s)*

Name	Type	
Cluster Proxy Lost	Exists	set
Cluster Resource Group Proxy Lost	Exists	set
Cluster Resource Proxy Lost	Exists	set
ContactLost_Gray	Exists	set
ContactLost_Red	Exists	set
Dev Module Failed	Exists	set
Dev Module Offline	Exists	set
Dev Module Pulled	Exists	set

Show — Displaying 92 of 92

Relationship: Caused By

Root Cause Condition*

ManagementLostNonVirtual
ManagementLostVirtual
Model Active
Module Offline
Module Pulled
MSCS Cluster Node Down
MSCS Cluster Node in Unknown St

Filter: — Displaying 92 of 92

5. Click OK.

   Any new alarms for a cluster node failure use Cluster Node Down as the root cause. Existing alarms and symptoms do not change.

Note: For more information, see the *Condition Correlation User Guide*.

Remove the Correlation Rule

This procedure explains how to remove the correlation rule when a cluster node fails. As a result, both the Cluster Node Down and the Contact Lost alarms are reported.

Follow these steps:

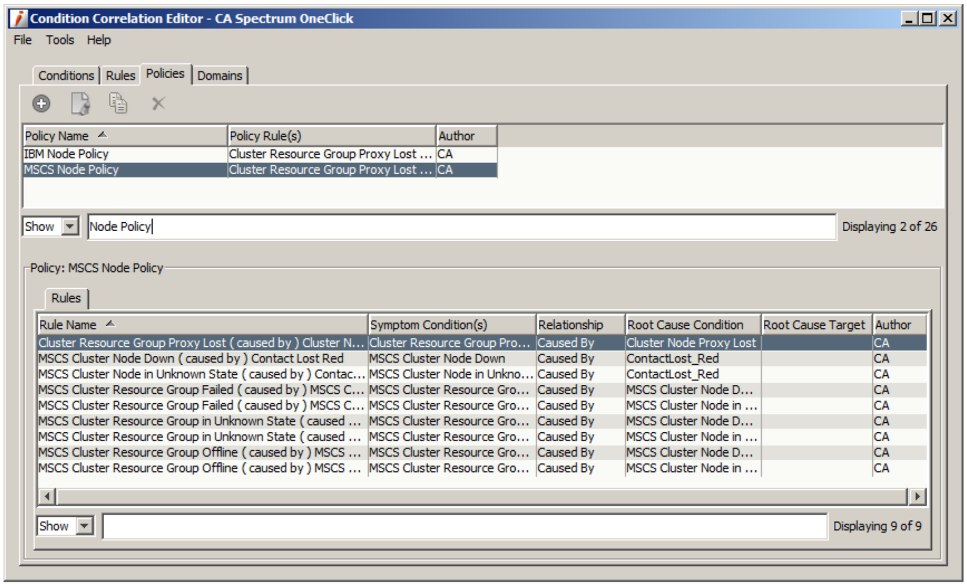
1. Select Tools, Utilities, Condition Correlation Editor.

   The Condition Correlation Editor opens.

2. Select the Policies Tab.

   A list of all correlation policies that are defined for your installation are displayed. The following policies apply to Cluster Manager and the Cluster Node Down alarm:

   - IBM Node Policy
   - MSCS Node Policy



Policy Name	Policy Rule(s)	Author
IBM Node Policy	Cluster Resource Group Proxy Lost ...	CA
MSCS Node Policy	Cluster Resource Group Proxy Lost ...	CA

Show: Node Policy — Displaying 2 of 26

Policy: MSCS Node Policy

Rule Name	Symptom Condition(s)	Relationship	Root Cause Condition	Root Cause Target	Author
Cluster Resource Group Proxy Lost (caused by) Cluster N...	Cluster Resource Group Pro...	Caused By	Cluster Node Proxy Lost		CA
MSCS Cluster Node Down (caused by) Contact Lost Red	MSCS Cluster Node Down	Caused By	ContactLost_Red		CA
MSCS Cluster Node in Unknown State (caused by) Contac...	MSCS Cluster Node in Unkno...	Caused By	ContactLost_Red		CA
MSCS Cluster Resource Group Failed (caused by) MSCS C...	MSCS Cluster Resource Gro...	Caused By	MSCS Cluster Node D...		CA
MSCS Cluster Resource Group Failed (caused by) MSCS C...	MSCS Cluster Resource Gro...	Caused By	MSCS Cluster Node in ...		CA
MSCS Cluster Resource Group in Unknown State (caused ...	MSCS Cluster Resource Gro...	Caused By	MSCS Cluster Node D...		CA
MSCS Cluster Resource Group in Unknown State (caused ...	MSCS Cluster Resource Gro...	Caused By	MSCS Cluster Node in ...		CA
MSCS Cluster Resource Group Offline (caused by) MSCS ...	MSCS Cluster Resource Gro...	Caused By	MSCS Cluster Node D...		CA
MSCS Cluster Resource Group Offline (caused by) MSCS ...	MSCS Cluster Resource Gro...	Caused By	MSCS Cluster Node in ...		CA

Show — Displaying 9 of 9

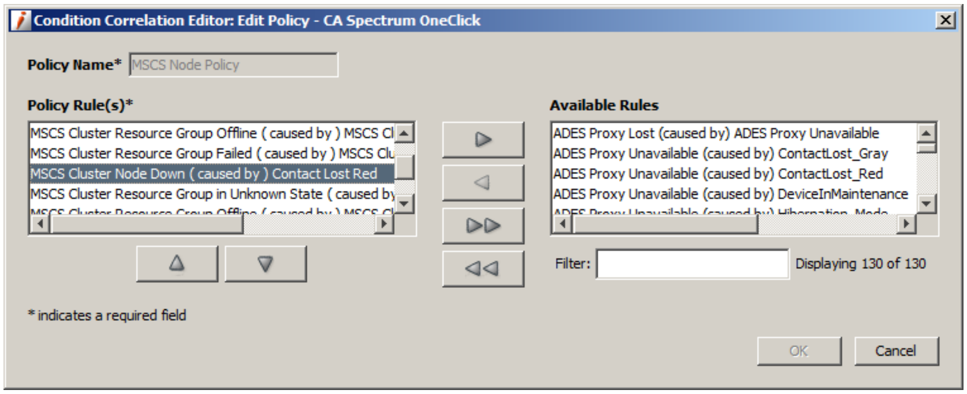
3. Select the policy that you want to modify, and click the Edit button.

   The Edit Policy window opens.

4. Move the appropriate "Cluster Node Down" rule to the right. As defined in the original out-of-box policies, these rules are:

   ■ IBM Cluster Node Down (caused by) Contact Lost Red

   ■ MSCS Cluster Node Down (caused by) Contact Lost Red



Condition Correlation Editor: Edit Policy - CA Spectrum OneClick

Policy Name* MSCS Node Policy

Policy Rule(s)*

MSCS Cluster Resource Group Offline (caused by) MSCS Cl
MSCS Cluster Resource Group Failed (caused by) MSCS Clu
MSCS Cluster Node Down (caused by) Contact Lost Red
MSCS Cluster Resource Group in Unknown State (caused by

Available Rules

ADES Proxy Lost (caused by) ADES Proxy Unavailable
ADES Proxy Unavailable (caused by) ContactLost_Gray
ADES Proxy Unavailable (caused by) ContactLost_Red
ADES Proxy Unavailable (caused by) DeviceInMaintenance

Filter: Displaying 130 of 130

* indicates a required field

5. Click OK.

   The Cluster Node Down rule is no longer enabled in the policy. Any new cluster node failures result in both Cluster Node Down and Contact Lost alarms, and no correlation occurs. Existing alarms and symptoms do not change.

Note: For more information, see the *Condition Correlation User Guide*.

How to View and Modify Threshold Values

Cluster Manager uses self monitors that the cluster technology AIM configures on the SystemEDGE agent. The self monitors are threshold-based and track various resources and activities of the managed cluster components. When a threshold is violated, a CA Spectrum event and possibly an alarm is created. Configuration parameters for the self monitors are defined and stored on the SystemEDGE agent but can be modified from within CA Spectrum.

The following procedure describes how to modify self-monitor parameters for your cluster technology AIM from within CA Spectrum.

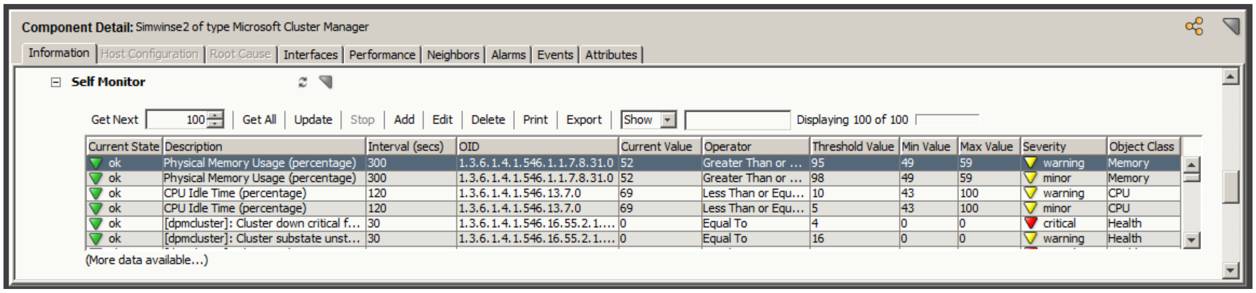
Follow these steps:

1. Select the Cluster Manager model in the Universe hierarchy or topology.

   The Component Detail panel displays information for the selected Cluster Manager.

2. In the Information tab in the Component Detail panel, expand the System Resources, Self Monitor subview.

   The expanded subview appears, as follows:



Current State	Description	Interval (secs)	OID	Current Value	Operator	Threshold Value	Min Value	Max Value	Severity	Object Class
ok	Physical Memory Usage (percentage)	300	1.3.6.1.4.1.546.1.1.7.8.31.0	52	Greater Than or ...	95	49	59	warning	Memory
ok	Physical Memory Usage (percentage)	300	1.3.6.1.4.1.546.1.1.7.8.31.0	52	Greater Than or ...	98	49	59	minor	Memory
ok	CPU Idle Time (percentage)	120	1.3.6.1.4.1.546.13.7.0	69	Less Than or Equ...	10	43	100	warning	CPU
ok	CPU Idle Time (percentage)	120	1.3.6.1.4.1.546.13.7.0	69	Less Than or Equ...	5	43	100	minor	CPU
ok	[dpmcluster]: Cluster down critical f...	30	1.3.6.1.4.1.546.16.55.2.1....	0	Equal To	4	0	0	critical	Health
ok	[dpmcluster]: Cluster substate unst...	30	1.3.6.1.4.1.546.16.55.2.1....	0	Equal To	16	0	0	warning	Health

(More data available...)

   Note: Control the columns that appear by right-clicking the table column heading and using the Columns tab. You can also undock the subview.

3. Select a row, and click Edit.

   The Edit Self Monitor Table Entry appears.

4. Modify the Threshold Value and any other values of interest, and click OK.

   The new values are saved in the table and on the AIM.

Appendix B: Troubleshooting

This section contains the following topics:

Unsupported Cluster AIM Configuration

Symptom:

I see the following alarm after I attempt to model my cluster environment:

UNSUPPORTED CLUSTER AIM CONFIGURATION

Solution:

You can manage a cluster node by a single cluster technology AIM only. If you inadvertently attempt to manage a cluster node by multiple cluster technology AIMs, Cluster Manager issues this alarm on the cluster model. Children are not created for the cluster model.

Check your AIM configurations. Modify the configuration of your AIMs so that each cluster and cluster node is registered with a single AIM only.

Note: For more information, see the *CA Virtual Assurance for Infrastructure Managers Administration Guide*.

Connections Do Not Appear in Topology

Symptom:

My cluster nodes do not show connections to other devices in the OneClick topology view.

Solution:

To produce connections between your cluster nodes and other elements in your network, any connecting devices must be modeled before the cluster nodes are modeled. When discovering and modeling your environment, run a standard CA Spectrum Discovery first to model upstream routers and switches. Then, Cluster Manager discovery can run, creating models and connections for the cluster components.

Follow these steps:

1. Verify that devices such as routers and switches that are upstream from your cluster nodes are modeled. If not, run a standard CA Spectrum Discovery to model these connecting devices.
2. If the connecting devices are modeled after your cluster environment is modeled, run Discover Connections on each of the affected devices.

   Note: For information on Discover Connections, see the *Modeling and Managing Your IT Infrastructure Administrator Guide*.

Glossary

active node

An *active node* is a system in a cluster environment where application processes (as part of a resource group) are currently running. Within CA Spectrum Cluster Manager, an active node has resource groups as children. A solid workstation icon represents an active node in the Cluster Manager hierarchy.

application insight module (AIM)

The 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.

cluster

A *cluster* is a group of locally attached machines that provide distributed processing power and high availability. A cluster appears to clients as a single system image and IP address.

Cluster Manager discovery

Cluster Manager discovery is the modeling within CA Spectrum of your cluster components. After the cluster technology AIM is modeled successfully, Cluster Manager obtains information about the cluster components in your environment from the AIM. Using a list of machines that is obtained from the AIM, Cluster Manager uses AutoDiscovery to model each cluster node. All supporting cluster components (clusters, resource groups, and resources) are also modeled.

cluster node

A *cluster node* is an independent computer system that participates in a cluster. A cluster node can be active or inactive. The active node has application processes (as part of a resource group) currently running. An inactive node is a system that is allocated to a cluster but not currently processing any resources.

failover/failback (MSCS)

Failover is a transfer process where resource groups that are hosted on a particular node that fails move to another node in the cluster. The reverse process is "failback". Failback occurs when the failed node becomes active again, and the groups that were failed over to other nodes transfer back to the original node.

fall over/fall back (IBM PowerHA)

Fall over is a transfer process where resource groups that are hosted on a particular node that fails move to another node in the cluster. The reverse process is "fall back”. Fall back occurs when the failed node becomes active again, and the groups that moved to other nodes transfer back to the original node.

IBM PowerHA Cluster Manager

The *IBM PowerHA Cluster Manager* is the CA Spectrum model that represents a host that contains the HACMP AIM. The HACMP AIM monitors the IBM PowerHA cluster elements (clusters, nodes, resource groups, and resources) in your environment.

inactive node

An *inactive node* is an available cluster node that has no resource groups currently running on it. In CA Spectrum, unlike a model in maintenance mode or hibernation mode, the inactive node model is fully functional. Data is gathered for the node, and any alarm activity or events for the node post to the model. Within the Cluster Manager hierarchy, an inactive node does not have any resource groups as children. A transparent icon represents an inactive node.

Microsoft Cluster Manager

The *Microsoft Cluster Manager* is the CA Spectrum model that represents a host that contains the MSCS AIM. The MSCS AIM monitors the Microsoft Clusters Service elements (clusters, nodes, resource groups, and resources) in your environment.

migration

Migration is the movement of a resource group from one node to another. Different terms are used to describe migration depending on the cluster technology; for example, failover, fall over, failback, and fallback.

proxy management

Proxy management is the act of managing network devices using an alternate management source in place of or in addition to the device itself. For example, CA Spectrum can manage your cluster environment by contacting cluster nodes directly or through a cluster technology AIM.

resource

A *resource* is a logical component or entity (for example, a file system or an application) that runs on only one node at a time. A resource can move from one cluster node to another.

resource group

A *resource group* is a collection of resources that forms a functional unit existing on a single cluster node.

virtual technology manager

A *virtual technology manager* is the SystemEDGE agent with a virtual technology AIM loaded. Virtual Host Manager uses virtual technology managers to manage virtual devices. For more information, see the *Virtual Host Manager Solution Guide*.

Index