

CA Spectrum®

Cisco Device Management Guide

Release 9.3



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.

Copyright © 2013 CA. All rights reserved. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.

CA Technologies Product References

This document references CA Spectrum® Infrastructure Manager (CA Spectrum).

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: Cisco Device Support Overview	7
Device Support	7
MIB Sources.....	8
Chapter 2: Cisco Unified Computing System	9
Cisco UCS Overview.....	9
Solution Architecture	10
Features.....	10
Automated Device Discovery and Modeling.....	11
Connectivity	15
Enhanced Fault Management	16
Dedicated UCS Views	19
Intelligent Trap Forwarding.....	20
Chassis Management	20
Chapter 3: Cisco Catalyst	22
Cisco Catalyst Device Support	22
Cisco Catalyst Board Fault Isolation Overview	23
The Catalyst Device with Downstream Devices Example.....	23
The Catalyst Device with Downstream Devices Example.....	24
The Catalyst with Downstream Devices with Multiple Management Paths Example	25
Chapter 4: Cisco Technology Support	27
Router Redundancy.....	27
HSRP Group Modeling.....	27
HSRP Group Membership	28
Change the State of the HSRPMode Attribute	29
SNMPv3 Device Discovery.....	30
Syslog Trap Support.....	31
Add Syslog Trap Mappings to CA Spectrum	33
Syslog Message Filter	34
Tunnel Interface Modeling.....	35
Configure CreateTunneLif	36
Configure Interface_Polling_Interval	36
VLAN Indexing Support	37

Chapter 5: CiscoWorks Integration	39
Introducing CiscoWorks	39
CiscoWorks Integration	40
Index	41

Chapter 1: Cisco Device Support Overview

This section contains the following topics:

- [Device Support](#) (see page 7)
- [MIB Sources](#) (see page 8)

Device Support

The CA Spectrum Cisco device certifications provide Cisco MIB and trap support, descriptive device identification, OneClick views, Cisco technology support. The CA Spectrum Cisco device certifications also provide CA Spectrum standard capabilities for specific devices and firmware.

Examples of device-family certifications include Catalyst, PIX Firewall, Wireless LAN Controller, and Aironet.

Examples of firmware-based certifications include Cisco IOS, CatOS, and Unified Computing System (UCS).

If no specific device-family certification is available for your Cisco device, then one of the following firmware-based model types is used:

- Rtr_Cisco—Models Cisco routers that are running IOS firmware.
- SwCiscoIOS—Models Cisco switches that are running IOS firmware.
- RtrCatOS—Models Cisco routers that are running CatOS firmware.
- SwCatOS—Models Cisco switches that are running CatOS firmware.
- CiscoNXOS—Models Cisco Nexus devices that are running NX-OS firmware.
- GnCiscoDev—Models Cisco devices that are not running IOS or CatOS firmware.

MIB Sources

Depending on the Cisco device firmware, chassis and board or module information is found in the following MIB sources:

OLD-CISCO-CHASSIS-MIB

Cisco has deprecated this MIB. Therefore, the information can be incomplete. To view the contents of this MIB, see the Cisco Chassis View subview in OneClick.

CISCO-STACK-MIB

The CatOS devices support this MIB. This MIB is deprecated in favor of the ENTITY-MIB. To view the contents of this MIB, see the MIB Tools utility.

Note: For more information about MIB Tools, see the *Certification User Guide*.

ENTITY-MIB

This MIB contains the latest board or module information for new devices. Older devices, however, do not populate this MIB correctly. To view the contents of this MIB, see the Entity View subview in OneClick.

Chapter 2: Cisco Unified Computing System

This section contains the following topics:

- [Cisco UCS Overview](#) (see page 9)
- [Solution Architecture](#) (see page 10)
- [Features](#) (see page 10)

Cisco UCS Overview

Cisco Unified Computing System (UCS) comprises a set of specialized devices working together, including the blades of the chassis and server. UCS supports the data center by delivering a dynamic IT infrastructure and by unifying network, computing, and virtualization resources.

CA Spectrum provides visibility into the following key components of Cisco UCS:

UCS Manager

A web services agent running on a Fabric Interconnect switch. The Cisco UCS manager supports an XML-based API for client interaction.

Fabric Interconnect (FI) Switch

- Typically two per UCS system; Cisco recommends a redundant configuration
- Runs NX-OS
- Hosts the UCS manager

Chassis

An agentless, switchless, blade server enclosure, with a maximum configuration of 40 chassis per UCS manager. Each chassis supports 8 half-width or 4 full-width server blades.

Blades

A server platform that serves as a virtualization host.

Service Profiles

Logical views of blade servers. Stored in the FI switch, they contain the blade server personality (identity and network information).

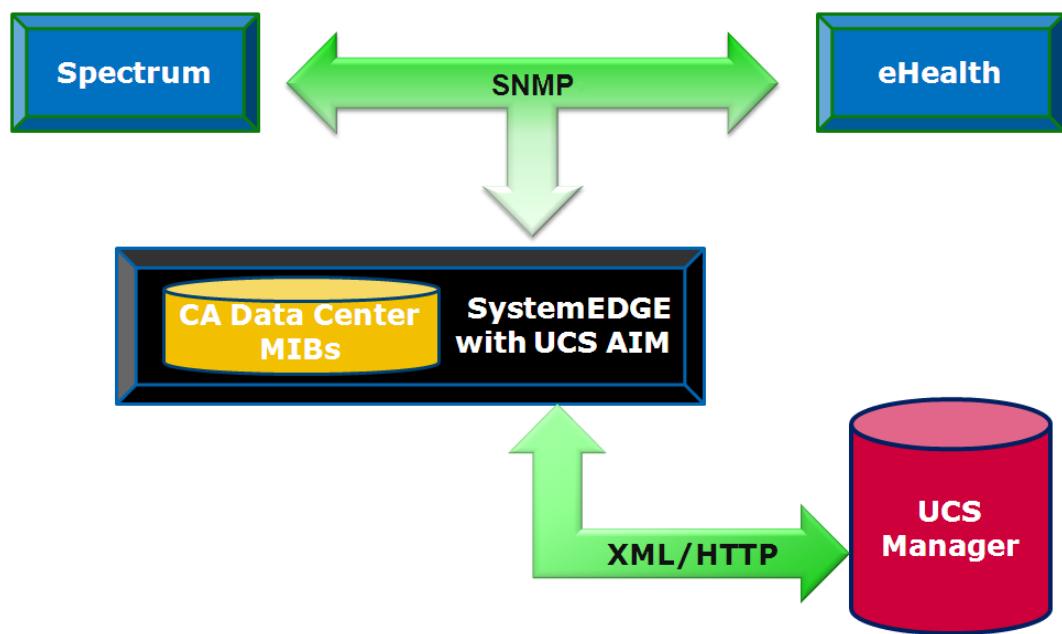
Solution Architecture

You can enable CA Spectrum support for Cisco UCS by employing a specialized SystemEDGE Application Insight Module (AIM). This AIM communicates with the UCS XML-based API to obtain information about the UCS managed environment. The data is then written to a pair of CA-developed MIBs. This solution lets other SNMP clients, such as CA eHealth, leverage the AIM.

The UCS AIM is an extension of the SystemEDGE SNMP agent and can support multiple UCS systems. The 2 CA-developed MIBs are:

- Generic data center MIB (CADATACENTERA)
- UCS-specific data center extension MIB (CACUCSEXTENSIONA)

As the following diagram shows, CA products like CA Spectrum and CA eHealth use SNMP to connect to the SystemEDGE that hosts the UCS AIM to obtain Cisco UCS details. The UCS AIM leverages XML/HTTP to connect to the UCS Manager.



Features

CA Spectrum UCS certification features include:

- Automated device discovery & modeling—Creates models for UCS components and maintains associations between blade models and any resident ESX hosts
- Connectivity—Generates accurate physical (L2) topology map of UCS system components

- Enhanced fault management—Recognizes and suppresses symptomatic alarms, and aids fault isolation with proxy management
- Dedicated UCS views—Provides visibility into UCS-specific data
- Intelligent trap forwarding—Enables alarm generation on individual UCS components
- Chassis management (non-UCS-specific)—Leverages rich chassis management feature set of CA Spectrum

Automated Device Discovery and Modeling

The certification automatically models UCS system components upon creation of the Host_SystemEDGE model hosting the UCS AIM. This model creates an application model type of cacucusaimApp upon detection of a UCS AIM MIB. In turn, this application model creates UCS system components such as Fabric Interconnects, chassis, blades, service profiles, and more.

Note: Not all UCS components are modeled, such as fabric extenders, power supplies, media adapters, or interfaces.

Next, a search is performed for previously modeled ESX hosts that are resident on any of the blades. An association is then created between the corresponding blade and ESX models to provide visibility into this hardware-to-software relationship.

Lastly, container models representing each UCS system are created. These models reside in the same container (for example, Universe) as the SystemEDGE host. Each container provides a logical topological grouping of the UCS system components.

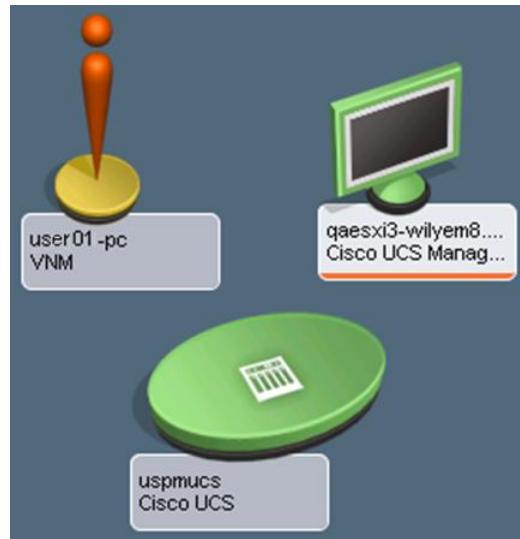
Important!

- In a given landscape, modeling multiple Host_SystemEDGE models whose UCS AIMs monitor the same UCS system is not supported.
- If the Host_SystemEDGE which hosts a UCS AIM is a virtual device, model it prior to the Host_SystemEDGE which hosts the corresponding virtual technology AIM. Otherwise, UCS containers can be erroneously created inside a physical host container of the virtual technology, disrupting CA Spectrum's fault isolation algorithms.

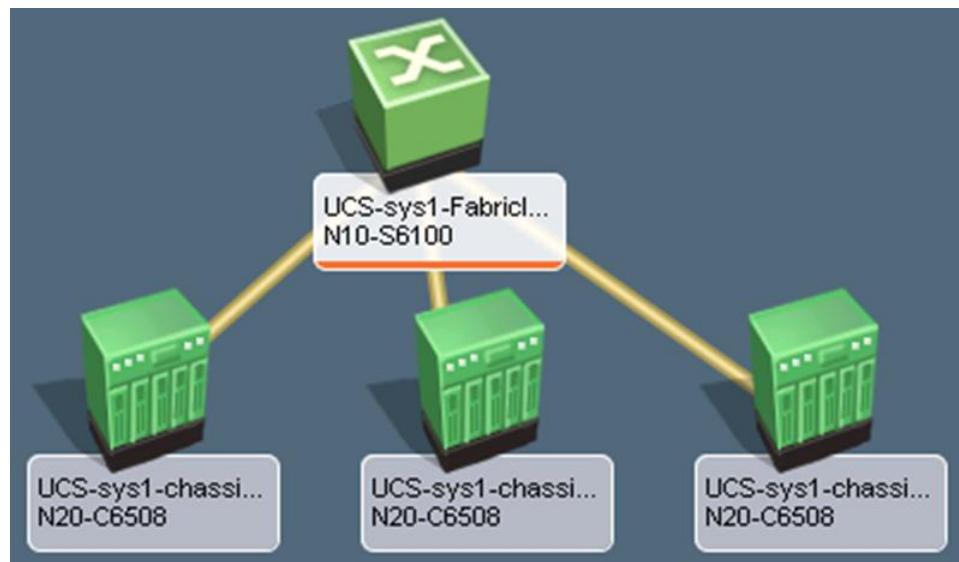
UCS Container Models

To represent a UCS container, CA Spectrum uses the standard container icon with a chassis logo. UCS containers have a model type of CiscoUCSContainer. Each container gathers together all the topologically significant models of a single UCS system (up to 2 FIs and 40 chassis). The contents of a UCS container cannot be modified.

UCS containers are displayed as in the following image:



The following image shows an example of the contents of a UCS Container:



UCS Fabric Interconnect Models

UCS Fabric Interconnects use the standard switch icon of CA Spectrum. If this device is modeled through IP address or through discovery, and if its NX-OS SNMP agent is enabled (it is disabled by default), a model of type CiscoUCSFabricInterconnect is created. Otherwise, automated UCS discovery creates a Pingable model. This model includes no device interfaces nor connectivity to upstream devices. Note that the IP address modeling can occur after UCS discovery, in which case the CiscoUCSFabricInterconnect model replaces the Pingable model.

UCS Fabric Interconnect models support dedicated UCS OneClick views and are the target models for UCS Fabric Interconnect traps and alarms.

UCS Chassis Models

UCS chassis use the standard chassis icon of CA Spectrum and have a model type of CiscoUCSChassis. The Interfaces tab in the Component Details panel of OneClick is enhanced for UCS chassis: the blades within the chassis are displayed to help with blade management.

UCS chassis also extend the fault isolation functionality of CA Spectrum to provide alarm correlation of collocated hardware resources.

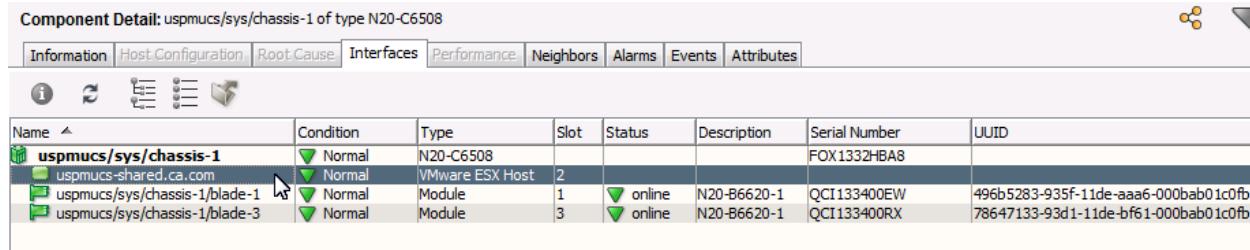
UCS chassis models support dedicated UCS OneClick views and are the target models for UCS chassis traps and alarms.

UCS Blade Models

UCS blades are modeled in CA Spectrum but, unlike Fabric Interconnect switches and chassis, are not visible inside their parent UCS container nor in any other location of CA Spectrum's topology. However, the UCS blades for each chassis are listed in the Interfaces tab of the chassis. UCS blades have a model type of CiscoUCSBlade.

CA Spectrum automatically makes associations between a blade and an ESX host resident on that blade. This association is done by performing a search for previously modeled ESX hosts and obtaining the UUID (Universally Unique Identifier) value. The blade UUIDs are then examined and when a match is discovered, the ESX host model is associated with the blade model. Only ESX hosts are supported for automatic association. CA Spectrum understands this blade (hardware) to ESX host (software) relationship and leverages it through enhanced fault isolation by displaying helpful and meaningful alarm details, such as the ESX host is out of contact because its blade failed.

Once the association is made, the ESX host model takes the place of the blade model in the Interfaces tab of the chassis model.



Name	Condition	Type	Slot	Status	Description	Serial Number	UUID
uspmucs/sys/chassis-1	Normal	N20-C6508				FOX1332HBA8	
uspmucs/shared.ca.com	Normal	VMware ESX Host	2				
uspmucs/sys/chassis-1/blade-1	Normal	Module	1	online	N20-B6620-1	QCI133400EW	496b5283-935f-11de-aaa6-000bab01c0fb
uspmucs/sys/chassis-1/blade-3	Normal	Module	3	online	N20-B6620-1	QCI133400RX	78647133-93d1-11de-bf61-000bab01c0fb

UCS blades can also be manually associated with corresponding SNMP agent models to provide visibility into the blade (hardware) to agent (software) relationship.

UCS blade models support dedicated UCS hardware-based OneClick views which include the following types of information:

- Statistical information such as CPU load, memory, and storage utilization
- Image inventory (BIOS & Firmware) and BIOS H/W configuration
- Physical interfaces of the blade server
- Service profile details

The UCS blade models are the target models for UCS blade traps and alarms.

More Information

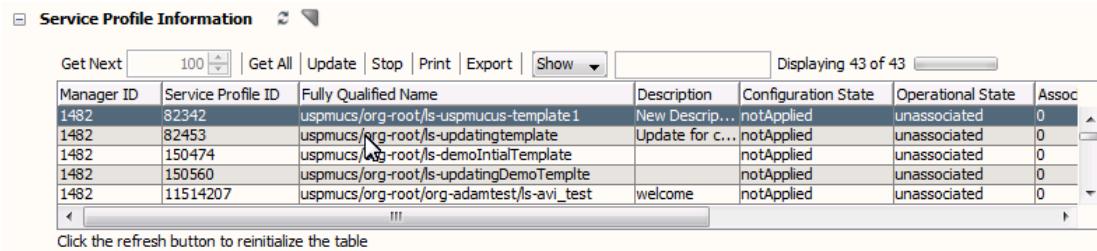
[Manual Blade/SNMP Device Association](#) (see page 21)

UCS Service Profile Models

Blade servers that are provisioned in the Cisco Unified Computing System are specified by a service profile. A service profile is a software definition of a server and its LAN and SAN network connectivity. UCS service profiles have a model type of CiscoUCSServiceProfile.

Server, network, and storage administrators create service profiles. Service profiles are stored in the Cisco UCS 6100 Series Fabric Interconnects. When a service profile is deployed on a blade server, the UCS manager automatically configures the blade server, its network adapters, fabric extenders, and fabric interconnects to support the configuration specified in the service profile.

CA Spectrum creates models for each service profile that is defined by a UCS Manager. They can be viewed from the OneClick Locator tab which now includes a Service Profile Model Class search option. In addition, service profile details are displayed in various OneClick views. Select the Cisco UCS Manager, Managed Environment and the Service Profile Information option on the Host_SystemEDGE model that is hosting the UCS AIM. You can then see the name, ID, description, associated blade, and various states of all the service profiles in the UCS systems that the Host_SystemEDGE manages.

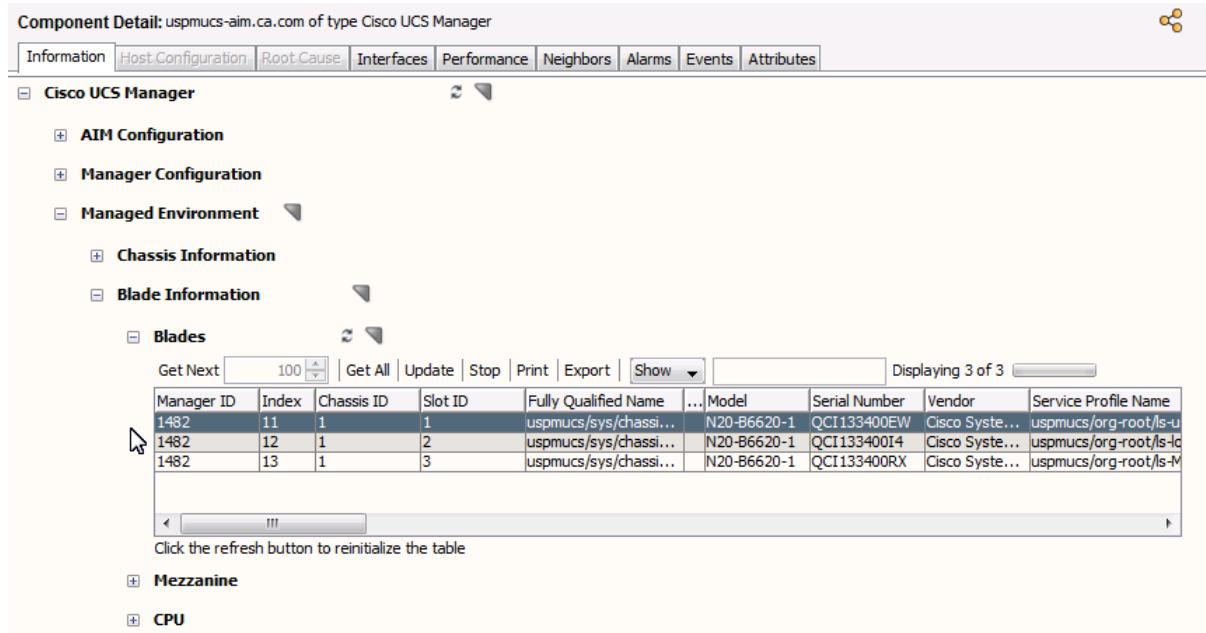


Service Profile Information

Manager ID	Service Profile ID	Fully Qualified Name	Description	Configuration State	Operational State	Assoc
1482	82342	uspmucs/org-root/ls-uspmucus-template1	New Descrip...	notApplied	unassociated	0
1482	82453	uspmucs/org-root/ls-updatingtemplate	Update for c...	notApplied	unassociated	0
1482	150474	uspmucs/org-root/ls-demoInitialTemplate		notApplied	unassociated	0
1482	150560	uspmucs/org-root/ls-updatingDemoTemplate		notApplied	unassociated	0
1482	11514207	uspmucs/org-root/org-adamtest/ls-avi_test	welcome	notApplied	unassociated	0

Click the refresh button to reinitialize the table

CA Spectrum also displays the service profile that is associated with each blade that is installed in each UCS Manager Chassis.



Component Detail: uspmucs-aim.ca.com of type Cisco UCS Manager

Cisco UCS Manager

- AIM Configuration
- Manager Configuration
- Managed Environment
 - Chassis Information
 - Blade Information
 - Blades
- Mezzanine
- CPU

Blades

Manager ID	Index	Chassis ID	Slot ID	Fully Qualified Name	Model	Serial Number	Vendor	Service Profile Name
1482	11	1	1	uspmucs/sys/chassi...	N20-B6620-1	QCI133400EW	Cisco Syst...	uspmucs/org-root/ls-u...
1482	12	1	2	uspmucs/sys/chassi...	N20-B6620-1	QCI133400I4	Cisco Syst...	uspmucs/org-root/ls-...
1482	13	1	3	uspmucs/sys/chassi...	N20-B6620-1	QCI133400RX	Cisco Syst...	uspmucs/org-root/ls-M...

Click the refresh button to reinitialize the table

The UCS service profile models are the target models for UCS service profile alarms.

Connectivity

UCS Fabric Interconnect models participates in connectivity by providing the boundary switching node between the upstream devices and the blade servers in the chassis.

Upstream from the UCS Fabric Interconnect

The upstream connections from the Fabric Interconnect interface are done through standard bridging tables. These connections require the following steps:

- Enabling the native NX-OS SNMP agent in the Fabric Interconnect .
- Modeling the device ,either by IP address or through discovery.

More Information

[UCS Fabric Interconnect Models](#) (see page 13)

Downstream from the UCS Fabric Interconnect

The downstream FCoE connections from a UCS Fabric Interconnect to its constituent chassis are shown as standard CA Spectrum L2 connections. These connections are created programmatically and not through standard bridging tables nor the UCS MIBs.

Enhanced Fault Management

Enhanced Fault Management for UCS involves two types of alarms:

- Fault Alarms
 - Indicate a problem with L2 availability
 - Are enhanced with special correlation logic
- Proxy Lost Alarms
 - Indicate that updated UCS information cannot be obtained from the SystemEDGE UCS AIM host
 - Include a Proxy Unavailable alarm for the host itself

UCS Fault Management enhancements also include chassis- and blade-level availability alarms and trap-generated alarms that indicate infrastructure and environment issues.

UCS leverages the benefits of alarm correlation:

- Pinpoint root cause
- Suppress extraneous alarms
- Correlate symptoms to root cause
- Show impact

UCS alarm correlation occurs at both the chassis level and the UCS System level.

Chassis-Level alarm correlation uses a domain that includes a chassis, its blades, and all SNMP blade agent models in the case of fault (loss of contact) alarms. If contact is lost for each of these domain entities (in other words, the chassis, the blades and the SNMP blade agents) a single Chassis Down alarm is generated on the chassis. The entire set of Contact Lost alarms is correlated with it.

In the case of proxy lost alarms, chassis-level alarm correlation uses a smaller domain that includes a chassis and its blades. Here, Proxy Lost alarms for all blades are correlated with the chassis Proxy Lost alarm.

UCS System-Level alarm correlation uses a domain that includes the SystemEDGE host, the FIs, and the child chassis and blades. If communication is lost between CA Spectrum and the SystemEDGE host, a Proxy Lost alarm is present on all the FIs, chassis, and blades. A Proxy Unavailable alarm is present on the host.

The Proxy Lost alarms for all the components are correlated with the host Proxy Unavailable alarm. These correlations are performed hierarchically. The Proxy Unavailable alarm is itself correlated with the alarm that indicates the reason for the communication failure. For example, it indicates contact lost, management lost, or maintenance mode. This top-level, overarching alarm is then visible to you in the alarm window.

Root Cause Isolation Examples

Root cause isolation resembles the following examples:

- A UCS chassis is inadvertently powered off, affecting the blades (and services running on them). Therefore, the individual Contact Lost alarms on all blades are correlated with the Chassis Down alarm to point the fault to the chassis.
- CA Spectrum loses contact with the SystemEDGE host. Therefore, the Proxy Lost alarms on all FIs, chassis, and blades are hierarchically correlated with the host's Proxy Unavailable alarm.

Top Screenshot: Alarm Details

qaesxi3-wileyem8.ca.com of type Cisco UCS Manager

Alarm Details | Information | Impact | Host Configuration | Root Cause | Interfaces | Performance | Alarm History | Neighbors | Events | Path View

CISCO UCS SERVER HOST UNAVAILABLE

Sep 27, 2010 10:02:56 AM EDT

A Cisco UCS Server Unavailable event has occurred, from Host_systemEDGE device, named qaesxi3-wileyem8.ca.com.

A Cisco UCS Server has become unavailable.

Unavailability Reason = management_lost

Bottom Screenshot: Symptoms Table

qaesxi3-wileyem8.ca.com of type Cisco UCS Manager

Alarm Details | Information | Impact | Host Configuration | Root Cause | Interfaces | Performance | Alarm History | Neighbors | Events | Path View

Symptoms The selected alarm resulted in 5 symptoms.

Severity	Date/Time	Name	Alarm Title	Network Address	Severity
Major	Sep 27, 2010 10:02:56 AM EDT	sys/chassis-1	CISCO UCS SERVER HOST PROXY LOST FOR CHASSIS	138.42.183.180	Major
Major	Sep 27, 2010 10:02:56 AM EDT	sys/switch-A	CISCO UCS SERVER HOST PROXY LOST FOR FABRIC INTERFACE		Major
Major	Sep 27, 2010 10:02:56 AM EDT	sys/chassis-1/blade-1	CISCO UCS SERVER HOST PROXY LOST FOR MODULE		Major
Major	Sep 27, 2010 10:02:56 AM EDT	sys/chassis-1/blade-3	CISCO UCS SERVER HOST PROXY LOST FOR MODULE		Major
Major	Sep 27, 2010 10:02:56 AM EDT	sys/chassis-1/blade-2	CISCO UCS SERVER HOST PROXY LOST FOR MODULE		Major

Chassis and Blade Availability Alarms

Chassis availability alarms include Chassis Down and Blade Status Unknown (which is correlated with Chassis Down).

Blade availability alarms include Blade Removed and Blade Failed (the blade is present but has a failed status). Both of these alarms are correlated with an existing Blade Status Unknown alarm on the parent chassis. Note that blade models are subject by default to a two-hour age-out to allow for blade replacement.

Service Profile Alarms

Not only do we display all the service profile details, we also create CA Spectrum models for each service profile. CA Spectrum actively monitors the state of the service profile and generates events and alarms based on the operational state of each service profile.

Trap-Generated Alarms

UCS supports trap-generated alarms that indicate infrastructure and environment issues. Discrimination is used where appropriate. Examples include Blade Added, Blade Removed, Power Supply Inoperable, and Temperature Warning.

Dedicated UCS Views

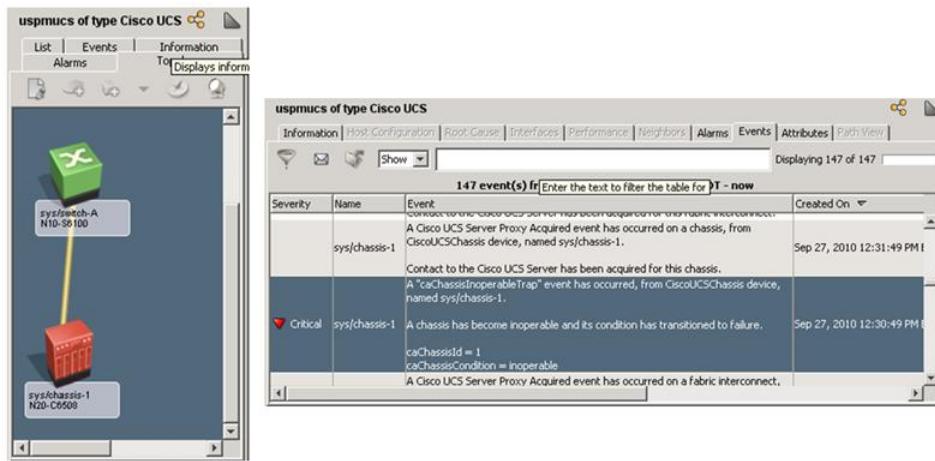
Dedicated UCS views are available for (device type in parentheses):

- SystemEDGE host (Cisco UCS Manager)
This includes tables views of the managed environment.
- Fabric Interconnect (Cisco UCS Switch)
- Chassis (Cisco UCS Chassis)
- Blade (Cisco UCS Blade)
- Service Profile (N/A)

OneClick views show hardware details such as memory DIMMs, mezzanine cards, fabric interconnect extenders, and interfaces.

Intelligent Trap Forwarding

All UCS traps are generated from the UCS AIM and thus arrive into CA Spectrum from the SystemEDGE host. Therefore, CA Spectrum employs a forwarding mechanism to generate the event/trap on the correct UCS component. Determination of the correct component is achieved through examination of trap variable values. If the applicable component cannot be found, the trap event is asserted on the SystemEDGE host.



Chassis Management

UCS leverages the rich set of chassis management features that are available in CA Spectrum:

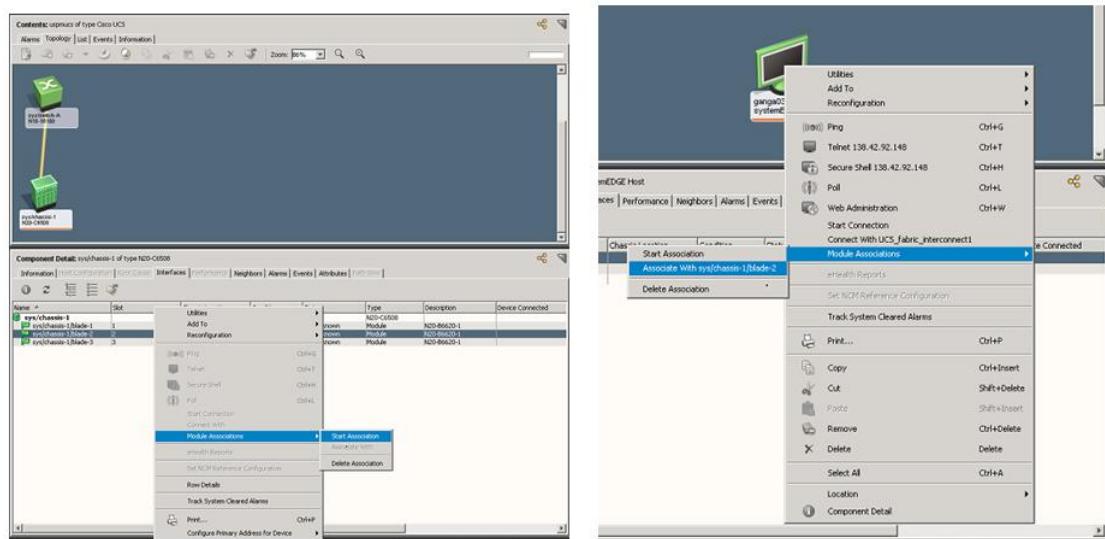
- Manual blade/SNMP device association
- Blade and managed device visibility
- Locator searches

For more information, see the "Chassis-Based Support" section of the *Certification User Guide*.

Manual Blade/SNMP Device Association

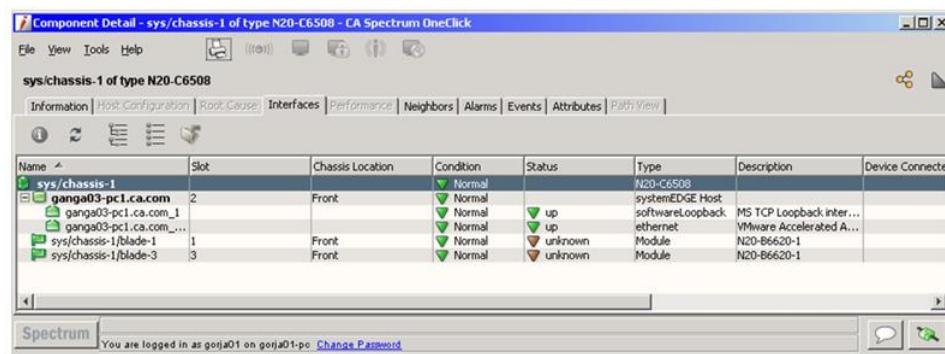
Manual blade/SNMP device association binds an individual blade of a chassis to an SNMP-capable blade agent model. This association enables quick determination of the system/chassis location from the agent model. The SNMP model is not moved into the UCS container, but it takes the place of the blade in the Interfaces tab of the chassis.

To bolster this integration, the SNMP agent model is incorporated into chassis fault correlation. Blade/agent association also enables SNMP model identification through chassis-based Locator searches.



Blade and Managed Device Visibility

Through the inclusion of associated SNMP devices, the extended Interfaces tab offers visibility into the blades of the chassis and managed devices.



Locator Searches

Chassis-based searches are listed under the Chassis node on the Locator tab of CA Spectrum, and facilitate the quick location of chassis and their components.

Searches include:

- All Chassis
- All Chassis Managed Devices
- All Modules
- Managed Devices By Chassis Name
- Modules By Chassis Name

Chapter 3: Cisco Catalyst

Cisco Catalyst Device Support

CA Spectrum supports Catalyst device families 1200, 1400, 1900, 2820, 3000, 3200, 4000, 4500, 5000, and 6500 with multiple enhanced certifications.

For the Catalyst 2900 and Catalyst 3500 device families, the specific enhanced certification is dependent on the supported MIB set.

CA Spectrum models Catalyst 2900 series devices as follows:

- The HubCat29xx model type models Catalyst 2900 series switches that run the IOS firmware and support the CISCO-C2900-MIB.
- The SwCiscolOS model type models Catalyst 2900 series switches that run the IOS firmware, but does not support the CISCO-C2900-MIB. Catalyst 2970 and Catalyst 2948g devices fall into this category.
- The SwCat4xxx model type models Catalyst 2900 series switches that run the CatOS firmware.

CA Spectrum models Catalyst 3500 series devices as follows:

- The HubCat29xx model type models Catalyst 3500 series switches that run the IOS firmware and support the CISCO-C2900-MIB.
- The SwCiscolOS model type models Catalyst 3500 series switches that run the IOS firmware, but does not support the CISCO-C2900-MIB. Catalyst 3550 series falls into this category.

Cisco Catalyst Board Fault Isolation Overview

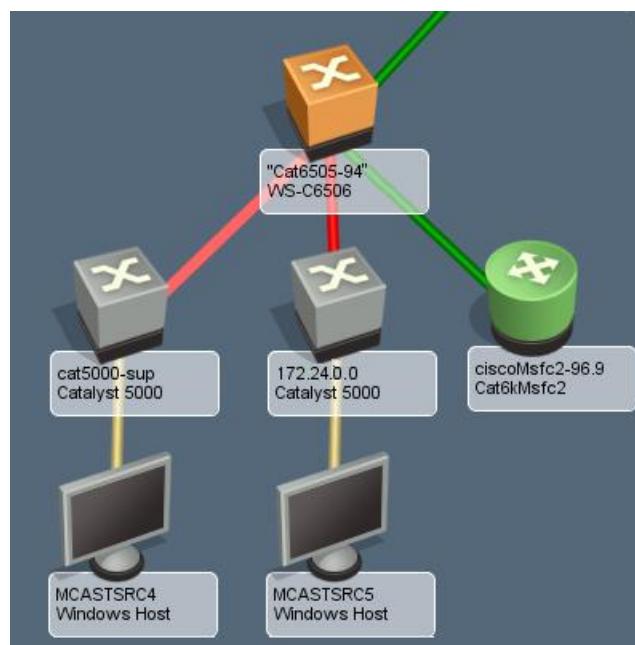
CA Spectrum supports boards being pulled or failing.

In a traditional fault isolation scenario, when a board in a chassis-based device fails, CA Spectrum generates critical alarms on all downstream device models. The device model that has the failed board retains its normal condition. However, this behavior does not give an indication as to which device is actually the fault.

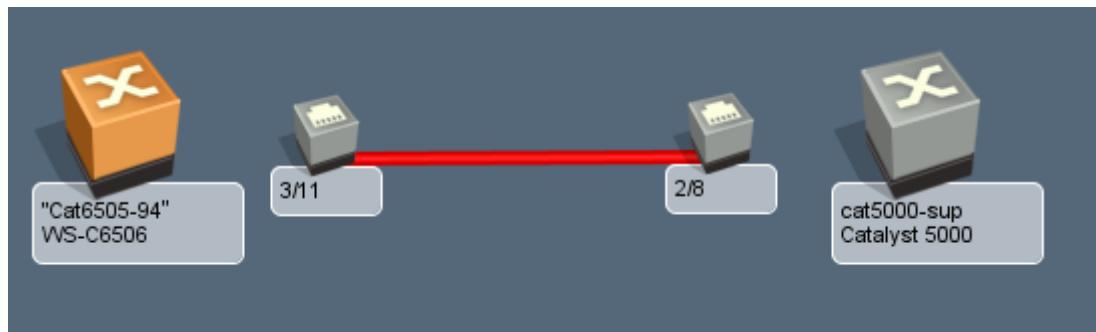
In the same scenario, Catalyst chassis-based devices that support the CISCO-STACK-MIB have enhanced fault isolation functionality to suppress the downstream device models, generate a major alarm on the device model which has the failed board, and generates a critical alarm on the board model. The ports that are associated with the board model are also suppressed giving a clear indication to not only which device is at fault, but also the board that is at fault.

The Catalyst Device with Downstream Devices Example

In the following example, the connected devices have Enable Live Links set to TRUE. When the Catalyst board is pulled, the devices that are connected to ports through that board go down. This event triggers CA Spectrum to determine the cause of the fault. In this example, two downstream switches and hosts are affected.

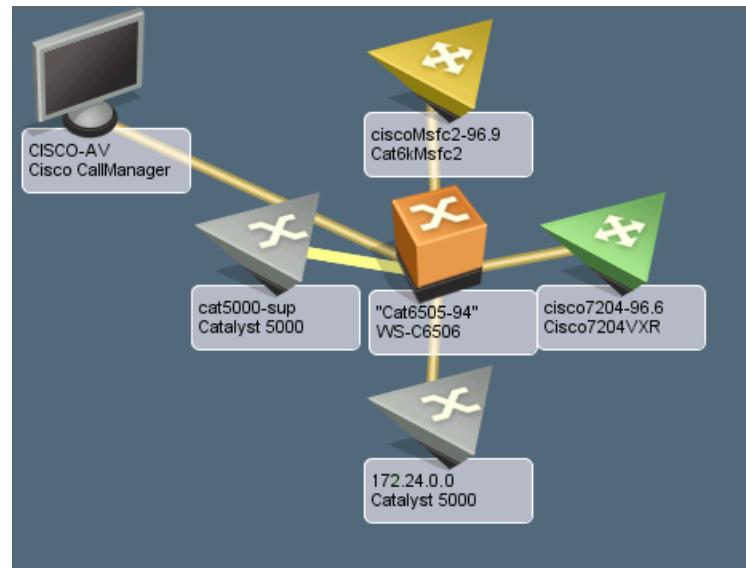


The following illustration shows the Link Information view. The Link Information view shows the root cause of the alarm.

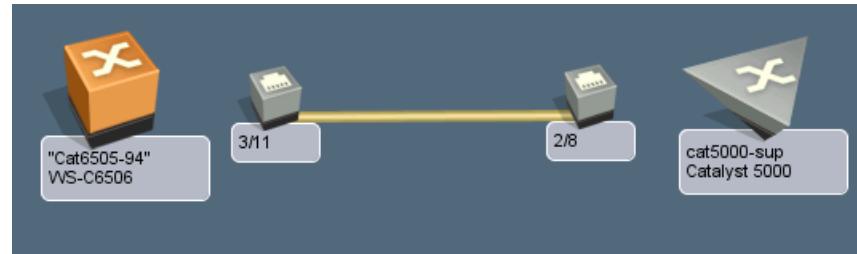


The Catalyst Device with Downstream Devices Example

In the following example, the connected devices have Enable Live Links set to FALSE. Traps are received when the Catalyst board is pulled, and the devices that are connected to ports through that board go down. This event triggers CA Spectrum to determine the cause of the fault. In this example, two downstream switches (off-page references) and hosts (not in view) are affected.

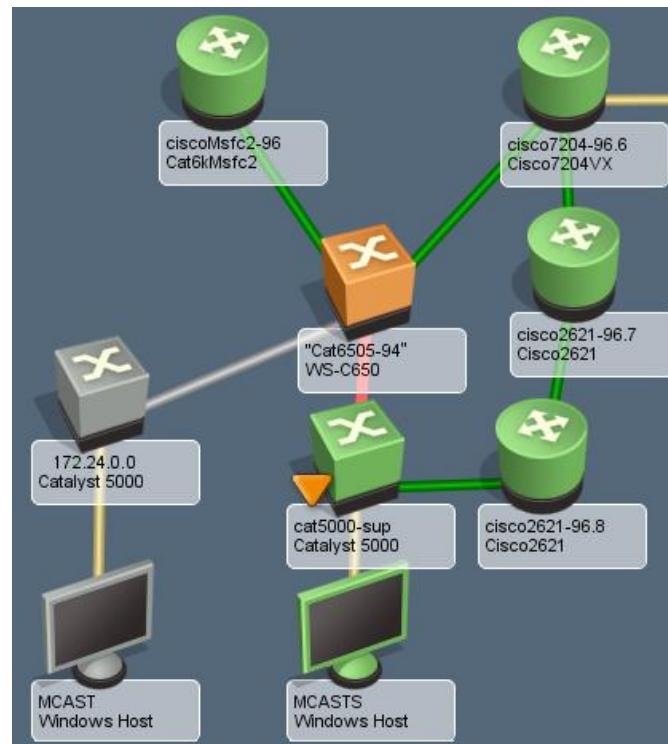


The following illustration shows the Link Information view. The Link Information view shows the root cause of the alarm.



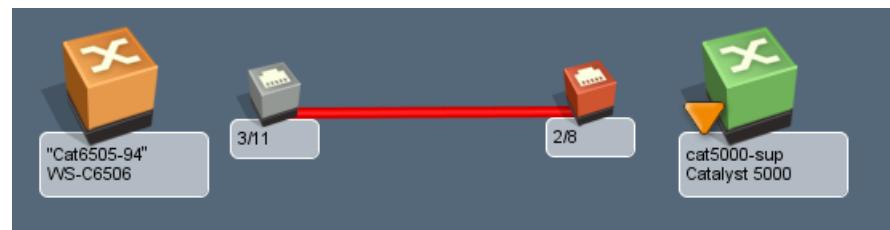
The Catalyst with Downstream Devices with Multiple Management Paths Example

In the following example, the connected devices have Enable Live Links set to TRUE. When the Catalyst board is pulled, the devices that are connected to ports through that board go down. This event triggers CA Spectrum to determine the cause of the fault. In this example, one downstream switch and host are affected.



Note: The switch with the second management path stays contacted and alarms its port.

The following illustration shows the Link Information view. The Link Information view shows the root cause of the alarm.



Chapter 4: Cisco Technology Support

This section contains the following topics:

- [Router Redundancy](#) (see page 27)
- [SNMPv3 Device Discovery](#) (see page 30)
- [Syslog Trap Support](#) (see page 31)
- [Tunnel Interface Modeling](#) (see page 35)
- [VLAN Indexing Support](#) (see page 37)

Router Redundancy

The CISCO-HSRP-MIB lets you manage Cisco IOS proprietary Hot Standby Router Protocol (HSRP).

HSRP lets the host appear to be using a single router and maintain the connectivity even if the actual first hop router fails. Multiple routers participate in this protocol. Together, they simulate a single virtual router with a static IP address that is known as the virtual IP address. The end hosts forward their packets to the virtual router.

The router that forwards packets is known as the active router. If the active router fails, the standby router replaces the active router. HSRP provides a mechanism for determining the active and standby routers, using the IP addresses on the participating routers. If an active router fails, the standby router takes over without a major interruption in the connectivity of the host.

HSRP Group Modeling

CA Spectrum creates models for every HSRP group that it discovers. CA Spectrum identifies them by the virtual IP address. This virtual IP address is added to the Redundancy Excluded Address of the active router of the HSRP group. Each HSRP group model knows the active and standby routers in the HSRP group.

OneClick gives the visibility in the HSRP group membership, using the following two router redundancy spotlight methods:

Explorer Search

Provides a view that highlights HSRP group members with Active and Standby labels, as applicable. You can select a container in the Explorer tab, select the Topology tab in the Contents panel, click the spotlight icon, and select Router Redundancy.

Locater Search

Displays the available searches for HSRP group models. You can open the Router Redundancy directory in the Locater tab. For each model, the Contents panel contains information about the HSRP group model, including Virtual IP, Group ID, group membership, and so on.

HSRP Group Membership

CA Spectrum monitors each HSRP group, looking for state and membership changes. CA Spectrum polls the HSRP group tables of the active router on the active router device model's polling interval. CA Spectrum also responds to the state change traps sent by the device.

If a router fails over, a major alarm is asserted on the HSRP group model, indicating that Router Redundancy has been lost and there is no longer a standby router. CA Spectrum clears this alarm when a new standby router is detected.

Note: The Information tab for the group model provides a Report Election Change setting. If you enable this setting, CA Spectrum generates an alarm every time a new active router is selected. CA Spectrum does not clear this alarm.

Change the State of the HSRPMode Attribute

Limit the volume of SNMP requests to the network devices that are running with the HSRP deployment to prevent a degradation of network performance. You can set the state of the HSRPMode attribute to one of the following three states:

Off

The HSRP table is not polled.

Passive

The HSRP table is polled once at the activation. Otherwise, CA Spectrum relies on updates from traps to update this information.

Active

The HSRP table is polled every poll interval in addition to the passive processing.

Follow these steps:

1. From the Locater, expand Application Models.
2. Select By Name.
The Search dialog opens.
3. In the Search dialog, type 'CiscoHSRPApp' in the Model Type name text box.
A list of all of the CiscoHSRPApp devices is displayed.
4. Select all of the devices in the list and right-click to select Utilities, Attribute Editor.
The Attribute Editor dialog opens.
5. In the left pane, expand User Defined and click the add hyperlink.
The Attribute Selector dialog opens.
6. Type 'HSRPMode' in the filter tex box and click OK.
The attribute HSRPMode is added under User Defined.
7. Select HSRPMode, and click the right arrow to move it to the right pane.
You can now set the state of the HSRPMode attribute in the right pane.
8. In the left pane, expand SNMP Communication to select *Poll Interval (sec)*, and click the right arrow to move it to the right pane.
You can now set a value for the Poll Interval in the right pane.
9. In the right pane, clear No Change, and set a value for the Poll Interval and set the state of the HSRPMode to Off, Passive, or Active.

You have changed the state of the HSRPMode and set the value for the Poll Interval on all the device models in your landscape.

SNMPv3 Device Discovery

When you discover SNMPv3 devices on the Cisco switches with VLANs, you cannot use the community_string@VLAN_ID format to an index bridging information for each VLAN. Create the contexts instead.

For CA Spectrum to read the bridging information, create these contexts using the following format:

```
vlan-<VLAN_ID>
```

Example: Create an SNMP v3 User

This example creates an SNMPv3 user context, using the format CA Spectrum can read:

```
(enable) set snmp user <level1-vlan> nonvolatile  
(OUTPUT) Snmp user was set to level1-vlan authProt no-auth  privProt no-priv
```

Example: Create an SNMP Group

This example creates an SNMP group context, using the format CA Spectrum can read:

```
(enable) set snmp group <v3-level1-vlan> user <level1-vlan> security-model v3  
nonvolatile  
(OUTPUT) Snmp group was set to v3-level1-vlan user level1-vlan and version v3,  
nonvolatile.
```

Example: Create an SNMP Access Group

This example creates an SNMP access group context, using the format CA Spectrum can read:

```
(enable) set snmp access <v3-level1-vlan> security-model v3 noauthentication read  
<defaultUserView> write <defaultUserView> notify <defaultUserView> nonvolatile  
(OUTPUT) Snmp access group was set to v3-level1-vlan version v3 level  
noauthentication, readview defaultUserView, writeview defaultUserView, notifyview  
defaultUserView context match: exact, nonvolatile.  
(enable) set snmp access <v3-level1-vlan> security-model v3 noauthentication read  
<defaultUserView> write <defaultUserView> notify <defaultUserView> context <v3-level1-vlan>  
prefix nonvolatile  
(OUTPUT) Snmp access group was set to v3-level1-vlan version v3 level  
noauthentication, readview defaultUserView, writeview defaultUserView, notifyview  
defaultUserView context: v3-level1-vlan, context match: prefix, nonvolatile.
```

Syslog Trap Support

The System Message Log (syslog) protocol lets you send text messages from the Cisco devices to the network management software. The text messages are sent to the CA Spectrum Event Manager as SNMP traps. Syslog trap support lets the router device identify the text messages and escalate them to alarms as required. Syslog trap support also lets the Cisco Router model icon communicate alarm severity information.

If an alarm occurs as indicated by the Cisco device icon, the CA Spectrum Alarm Severity and a syslog message appear in the Alarm Log.

The syslog messages are classified based on the severity that ranges from 0 to 7 (most severe to least severe). The alarms display in the Alarm Log. Because these alarms are associated with Cisco device models, the corresponding model icon changes color and flashes, depending on the alarm severity.

The following table lists the severity codes and their descriptions:

Severity	Description
0	Emergency—System is unusable
1	Alert—Immediate action required
2	Critical—Critical condition
3	Error—Error condition
4	Warning—Warning condition
5	Notification—Normal but significant condition
6	Informational—Informational message only
7	Debugging—Message that appears during debugging only

The following table maps syslog message severity to the CA Spectrum alarm severity:

Alarm Severity	Color
0-1	Red
2-3	Orange
4	Yellow

Messages with an alarm severity of 5 through 7 do not generate an alarm because they are of a minor importance. Facility(hardware device, protocol, or a module or system software) lists the messages.

A facility code is an abbreviation of the facility to which the message refers. A facility can be a specific hardware device, a protocol, or software. Within each facility, messages are listed in terms of the severity, from the highest (0) to the lowest (7). A *mnemonic* is an uppercase string that uniquely identifies the message.

An explanation and a recommended action follow each message. Messages appear only when the system remains operational. The following line is an example of a syslog message:

01/01/2001,18:31:15:SYS-5-MOD_INSERT:Module 5 has been inserted.

This message is interpreted as follows:

- 01/01/2001,18:31:15 is the date and time of the error (this information appears if set for system log messaging).
- SYS is the facility type.
- 5 is the severity level, indicating it is a normal but significant condition.
- MOD_INSERT is the mnemonic that uniquely identifies the message.
- "Module 5 has been inserted" is the message text that describes the condition.

The System Message Log (syslog) program saves the system messages in a log file or directs the messages to other devices. Syslog software lets you do the following functions:

- Save logging information for monitoring and troubleshooting
- Select the type and destination of the logging information

By default, the switch logs normal but significant system messages to its internal buffer and sends these messages to the system console. You can specify how system messages must be saved based on the type of facility and the severity level. Messages can be time-stamped to improve real-time debugging and management.

Add Syslog Trap Mappings to CA Spectrum

CA Spectrum includes three text files that SpectroSERVER uses to map Cisco syslog traps to CA Spectrum events.

The following table shows the syslog text files:

Device Syslog Message	Text File
Cisco Router	<\$SPECROOT>/SS/CsVendor/Cisco_Router/Rtr.txt
Catalyst Switch	<\$SPECROOT>/SS/CsVendor/Ctron_CAT/Switch.txt
Cisco PIX	<\$SPECROOT>/SS/CsVendor/CiscoPIX/Pix.txt

Each line of these text files contains information to map syslog messages to CA Spectrum events. The lines have the following format (for each field, a single space is the delimiter):

<facility> <severity> <mnemonic> <event code>

Follow these steps:

1. Add a line to the file that contains the previous information.

For example, to add support for the %SPE-3-SM_DOWNLOAD_FAILED syslog message for Cisco Routers, add the following line to the Rtr.txt file: SPE 3 SM_DOWNLOAD_FAILED 0xfffff0001, where 0xfffff0001 is an arbitrary code that you select.

2. Create Event Format and the Probable Cause files for the event and alarm.

In this case, create Eventfffff0001 and Probfffff0001. You can enter any text in these files. The following variable data can be read from the Event Message and displayed in the Event Format file:

{S 1}- Facility
 {T T1_210017 2}- Severity
 {S 3}- Mnemonic
 {S 4} - Message

3. Add the event-to-alarm mapping. Using the previous example, add the following line:

0xfffff0001 E 50 A 2,0xfffff0001

Note: You must have an EventDisp file in the same directory as the Rtr.txt file.

An orange alarm is generated if SpectroSERVER receives this syslog trap.

Note: You can do this configuration while the SpectroSERVER is running. The SpectroSERVER checks for changes to the *.txt files every minute.

Syslog Message Filter

The Cisco Syslog Message Filter OneClick view lets you filter unwanted syslog messages. Filtering syslog messages blocks unwanted alarms or events. SS/CsVendor/SYSLOG contains eight files that correspond to different filter categories. To select the filter category to which a mnemonic belongs, move the mnemonic to the required SS/CsVendor/SYSLOG file.

The following table shows SS/CsVendor/SYSLOG files and corresponding filters:

File	Corresponding Filter
Syslog0	Protocol_Filter
Syslog1	System_Filter
Syslog2	Environment_Filter
Syslog3	Software_Filter
Syslog4	Security_Filter
Syslog5	Hardware_Configuration_Filter
Syslog6	Connection_Configuration_Filter
Syslog7	PIX_Firewall_Filter

Note: The mnemonics are interchangeable with any of the filters.

The filters are as follows:

Protocol_Filter

Affects the Syslog0 file. Set this filter to True to filter all syslog messages whose facilities deal with protocols. For example, BGP, OSPF, SNMP, SPANTREE.

System_Filter

Affects the Syslog1 file. Set this filter to True to filter all syslog messages whose facilities deal with the system. For example, CBUS, MEMSCAN.

Environment_Filter

Affects the contents of the Syslog2 file. Set this filter to True to filter out all syslog messages that deal with environment variables. For example, LCFE, LCGE.

Software_Filter

Affects the contents of the Syslog3 file. Set this filter to True to filter out all syslog messages that deal with internal software. For example, PARSER, RSP, GRPGE.

Security_Filter

Affects the contents of the Syslog4 file. Set this filter to True to filter out all syslog messages that deal with the security of the system. For example, RADIUS, SECURITY.

Hardware_Configuration_Filter

Affects the contents of the Syslog5 file. Set this filter to True to filter out all syslog messages that deal with the hardware configuration of the device. For example, IOCARD, MODEM, DIALSHELF.

Connection_Configuration_Filter

Affects the contents of the Syslog6 file. Set this filter to True to filter out all syslog messages that deal with connection configuration of the device. For example, MROUTE, ISDN, X25.

Pix_Firewall_Filter

Affects the contents of the Syslog7 file. Set this filter to True to filter out all syslog messages that deal with the Cisco PIX Firewall device.

Tunnel Interface Modeling

CA Spectrum supports the Cisco IPSec tunnel interface management for the Cisco devices that support CISCO-IPSEC-FLOW-MONITOR-MIB and CISCO-IPSEC-MIB. These MIBs are available for Cisco firmware versions 12.1 (4) or later.

CA Spectrum supports the following IPSEC VPN management features:

- The modeling of tunnel interfaces (site-to-site)
- The automatic connectivity mapping
- The interface model identification
- The interface model aging
- Link down trap correlation
- Status monitoring of tunnel interfaces

The following attributes control IPSEC VPN management:

- CreateTunnelLif
- Interface_Polling_Interval

Configure CreateTunneLIf

The CreateTunneLIf attribute indicates if tunnel interface models are created for each IPSec tunnel that is defined on the device. If TRUE, it specifies that CA Spectrum reads the external tables during the interface reconfiguration. These external tables define the tunnel interfaces present. CA Spectrum creates appropriate tunnel interface models as a subinterface of the related physical interface.

Follow these steps:

1. Navigate to the Locater tab, expand the Application Models folder, and double-click By Device IP Address.
The Search dialog opens.
2. Enter the IP address of the Cisco IPSec-capable device you want to configure and click OK.
The device appears in the Contents panel.
3. Select the CisclPSSecExtAp device in the Contents panel.
4. Select the Attributes tab in the Component Detail panel.
5. Select CreateTunneLIf in the left pane and click the right arrow button to move it to the right pane.
6. Double-click CreateTunneLIf in the right pane to change its value.

Note: Setting CreateTunneLIf to No disables Cisco IPSec tunnel modeling.

Configure Interface_Polling_Interval

The Interface_Polling_Interval attribute defines the tunnel table polling interval in seconds. If set to 0, the table is not polled.

Follow these steps:

1. Navigate to the Locater tab, expand the Application Models folder, and double-click By Device IP Address.
The Search dialog opens.
2. Enter the IP address of the Cisco IPSec-capable device you want to configure and click OK.
The device appears in the Contents panel.
3. Select the device in the Contents panel.
4. Select the Attributes tab in the Component Detail panel.

5. Select `Interface_Polling_Interval` in the left pane and click the right arrow button to move it to the right pane.
6. Double-click `Interface_Polling_Interval` in the right pane to change its value.

VLAN Indexing Support

CA Spectrum can test whether the VLAN indexing community string is supported on a particular Cisco device. The VLAN indexing community string prevents authentication failure traps.

If a Cisco device supports the VLAN indexing community string, the `VLANIndexingSupported` (0x4a0037) attribute value is set to Supported 1.

If a device of Cisco does not support the VLAN indexing community string, the `VLANIndexingSupported` (0x4a0037) attribute value is set to an enumeration `NotSupportedException` 0. Further VLAN index reads are not made. This configuration prevents authentication failure traps from being generated.

Test the device, if a Cisco device was not tested due to lack of VLANS information for the device. Perform a Discovery on that device, or to enable the VLAN overlay, set the `VLANIndexingSupported` (0x4a0037) attribute value to Test 2.

If the configuration of a device changes to support the VLAN indexing community string, change the attribute value to `VLANIndexingSupported` (0x4a0037) on the `Transparnt_App` model for that device through the Attribute Editor.

Chapter 5: CiscoWorks Integration

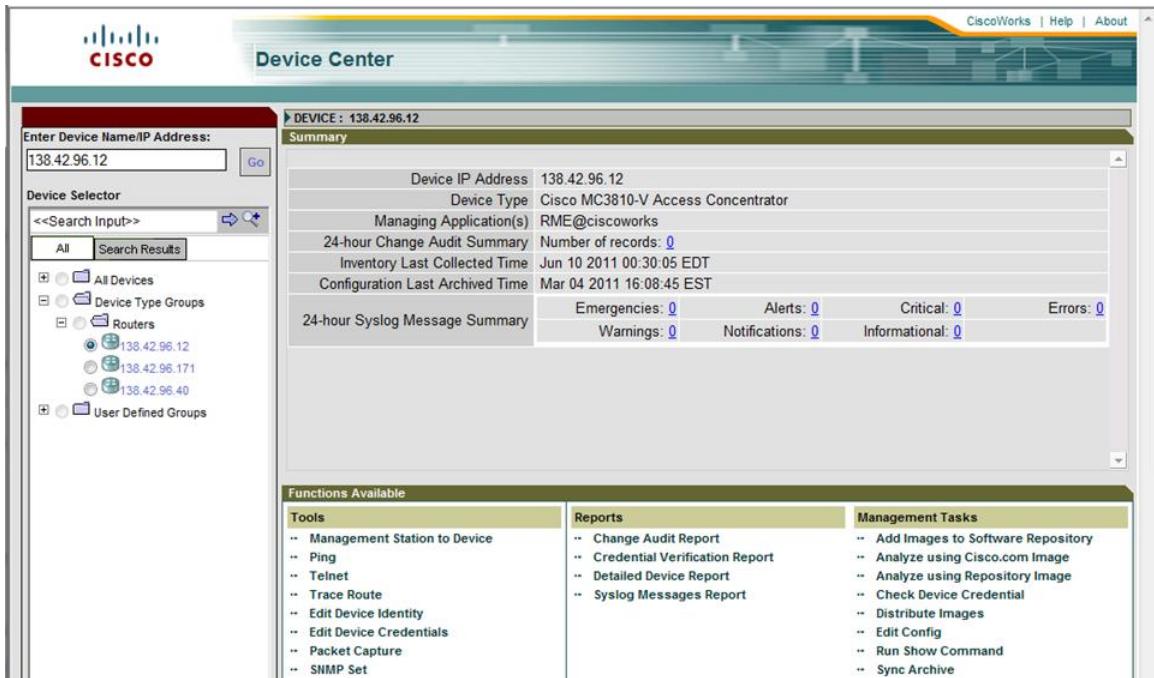
This section contains the following topics:

- [Introducing CiscoWorks](#) (see page 39)
- [CiscoWorks Integration](#) (see page 40)

Introducing CiscoWorks

With CA Spectrum r9.2.1, CA Spectrum integrates seamlessly with CiscoWorks application of Cisco. CiscoWorks provides a powerful tool to manage Cisco devices.

You can now select a Cisco device and launch directly to the Device Center page in CiscoWorks.



The screenshot shows the CiscoWorks Device Center interface. At the top, there is a navigation bar with links for CiscoWorks, Help, and About. The main title is "Device Center" with a sub-title "DEVICE : 138.42.96.12". The left sidebar contains a "Device Selector" with a search input field, a "Device IP Address" field containing "138.42.96.12", and a "Go" button. Below this is a tree view of "Device Type Groups": "All Devices" (selected), "Device Type Groups" (selected), "Routers" (selected), and "User Defined Groups". Under "Routers", there are three entries: "138.42.96.12", "138.42.96.171", and "138.42.96.40". The main content area is titled "Summary" and displays the following information for the selected device (138.42.96.12):

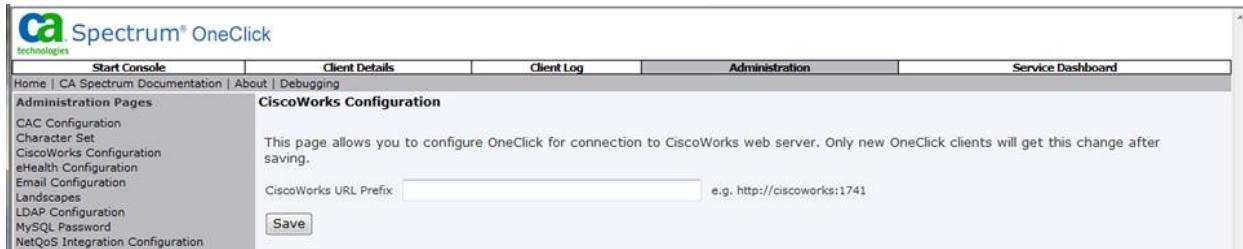
Device IP Address	138.42.96.12
Device Type	Cisco MC3810-V Access Concentrator
Managing Application(s)	RME@ciscoworks
24-hour Change Audit Summary	Number of records: 0
Inventory Last Collected Time	Jun 10 2011 00:30:05 EDT
Configuration Last Archived Time	Mar 04 2011 16:08:45 EST
24-hour Syslog Message Summary	Emergencies: 0 Alerts: 0 Critical: 0 Errors: 0 Warnings: 0 Notifications: 0 Informational: 0

Below the summary is a "Functions Available" section with three columns: "Tools", "Reports", and "Management Tasks".

Tools	Reports	Management Tasks
<ul style="list-style-type: none">-- Management Station to Device-- Ping-- Telnet-- Trace Route-- Edit Device Identity-- Edit Device Credentials-- Packet Capture-- SNMP Set	<ul style="list-style-type: none">-- Change Audit Report-- Credential Verification Report-- Detailed Device Report-- Syslog Messages Report	<ul style="list-style-type: none">-- Add Images to Software Repository-- Analyze using Cisco.com Image-- Analyze using Repository Image-- Check Device Credential-- Distribute Images-- Edit Config-- Run Show Command-- Sync Archive

CiscoWorks Integration

The OneClick Administration web page provides access to a CiscoWorks Configuration page. In this page, you can set the CiscoWorks web server name and port and can save this information in a file that is called `ciscoworks-config.xml` file in the `devman/config` directory. The menu picks are created only if the server name is set in the configuration file.



Index

A

- adding
 - new Syslog messages • 33
 - Syslog trap mappings to CA Spectrum • 33

B

- board fault isolation • 22

C

- Catalyst chassis-based devices • 22
- Catalyst device families • 22
- Catalyst device support • 22
- Catalyst examples • 23, 24, 25
- configuring
 - create TunnelLIf • 36
 - interface polling interval • 36
- Create TunnelLIf attribute • 36

D

- device support
 - about • 7
 - Cisco catalyst • 22
 - SNMPv3 device discovery • 30

E

- Enable Live Links • 23, 24, 25
- Explorer Search • 27

F

- filtering Syslog messages • 34

H

- hot standby router protocol • 27
- HSRP group membership • 28
- HSRP group modeling • 27

I

- interface polling interval • 36
- IPSEC VPN management • 35

L

- Locater Search • 27

R

- router redundancy • 27
- router redundancy spotlight methods • 27

S

- SNMPv3 devices • 30
- syslog
 - message filter • 34
 - message severity codes • 31
 - messages • 31
 - text files • 33
 - trap support • 31

T

- tunnel interface modeling • 35

V

- VLAN indexing • 37