

CA Spectrum®

Remote Operations Suite User Guide

Release 9.4



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 © 2014 CA. All rights reserved. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.

CA Technologies Product References

This guide references 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: Introduction	7
About Remote Operations Suite	7
Distributed Concepts in the Remote Operations Suite	9
Management Visibility in a Remote Operations Environment.....	11
 Chapter 2: Setting Up Remote Operations Suite	 13
Install the Remote Operations Suite	13
Set the Landscape Handle for the SpectroSERVER	16
Selecting a Main Location Server	16
Configure the Remote Operations Server	17
Configure Topology Forwarding.....	17
Configure Alarm Forwarding.....	19
Configure and Connect to the Central SPECTRUM Server	20
Fault Tolerance.....	21
 Chapter 3: Using Remote Operations Suite	 23
View Remote Operations Server Information	23
Update Remote Operations Server Topology Data	24
RemoteOperationsManagedElement Model Type	26
Search for Models	27
Device Management	28
Fault Isolation.....	28
 Chapter 4: Alarms	 31
Remote Operations Alarms	31
View Remote Operations-Related Alarms	33
Remote Operations Forwarding Events	35
Remote Operations Alarming Events.....	36
Remote Operations Clearing Events	36
Remote Operations Message Events	36
 Index	 37

Chapter 1: Introduction

This section contains the following topics:

[About Remote Operations Suite](#) (see page 7)

[Distributed Concepts in the Remote Operations Suite](#) (see page 9)

[Management Visibility in a Remote Operations Environment](#) (see page 11)

About Remote Operations Suite

Remote Operations Suite is the remotely deployed component of a CA Spectrum remote deployment. Remote Operations Suite is a stand-alone CA Spectrum management system that delivers all the standard CA Spectrum management capabilities. These capabilities include traditional fault-tolerant CA Spectrum management.

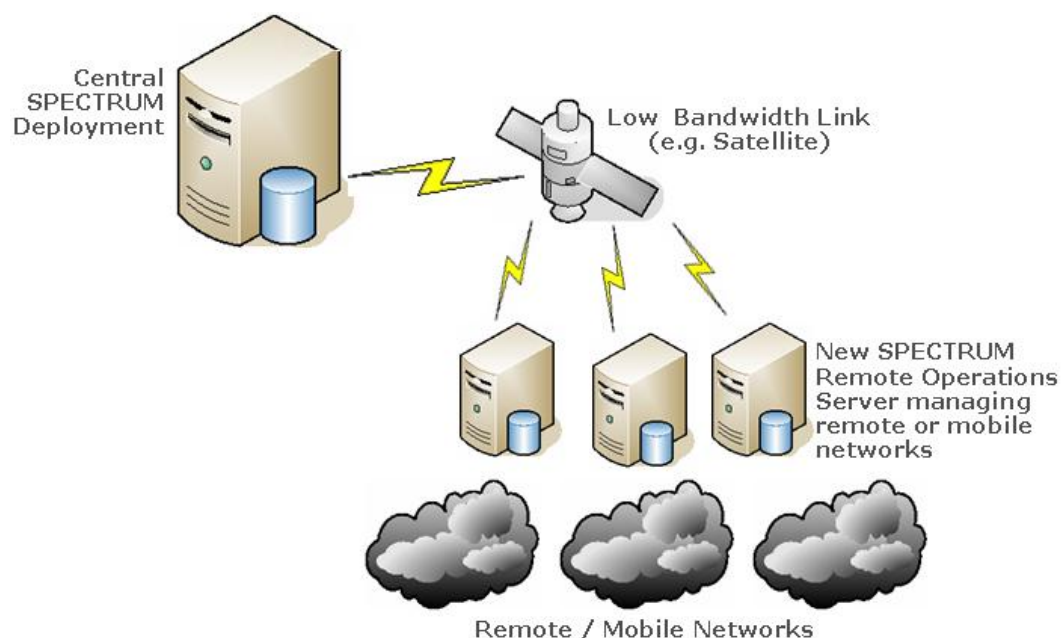
Remote Operations Suite supports operations in remote or mobile tactical environments. The remote component communicates with a designated Central SPECTRUM server to deliver real-time, or on-demand network topology. Remote Operations Suite also delivers the operational status of the managed remote site, mobile network over unreliable, or limited bandwidth communication links.

Note: In the environments where higher-speed communications links are more readily available, deploy the traditional CA Spectrum distributed architecture.

Remote Operations Suite performs the following functions:

- Enables the network manager at the remote or mobile site to manage the local network infrastructure
- Delivers all the standard CA Spectrum management capabilities (for example, network discovery, root cause analysis, impact analysis, alarming/alerting)
- Connects to another CA Spectrum deployment situated in global network operations or central command to deliver real-time inventory and operational status of the remote network
- Enables an administrator to determine the information that the remote site sends to the central site to be low-impact on the limited bandwidth (and often costly) communications links

The following architecture shows the Remote Operations Suite deployment:



Note: Remote Operations Suite uses the OneClick Console. For more information about OneClick, see the *Operator Guide*.

Remote Operations Suite includes the following components:

Remote Operations Server

Is the remotely deployed CA Spectrum installation of a Remote Operations Suite deployment. The Remote Operations Server is a lightweight, stand-alone CA Spectrum Management system that performs traditional fault tolerant CA Spectrum management, including fault management and root cause analysis for the network it manages. The Remote Operations Server communicates with its designated Central SPECTRUM Server through the installed Remote Operations Connector component. This architecture enables the delivery of network topology and operational alarm status over unreliable or limited bandwidth communication links.

Central SPECTRUM Server

Is a separate installation of CA Spectrum that includes the Remote Operations Manager component. This component listens for new connections from Remote Operations Servers. A single Central SPECTRUM Server with the Remote Operations Manager component installed can integrate with multiple Remote Operations Servers. The integrated servers let you discover and monitor managed elements in the Universe hierarchy of the Remote Operations Server.

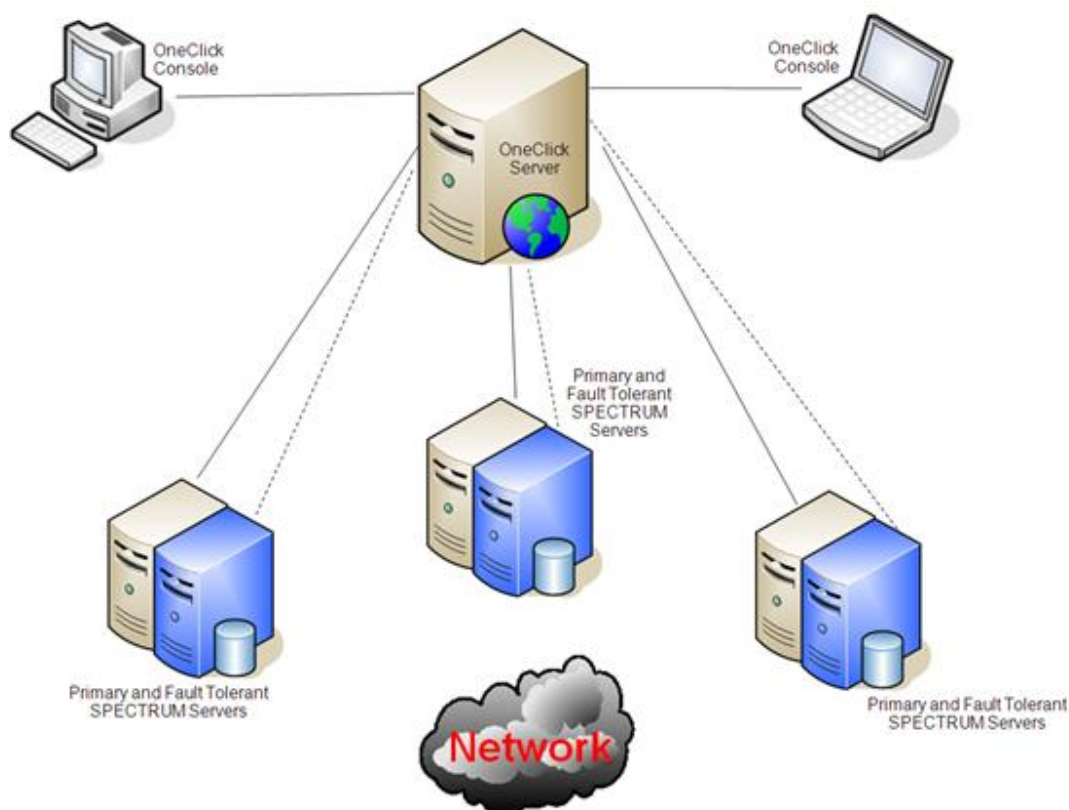
The Remote Operations Manager component on the Central SPECTRUM Server communicates with the Remote Operations Connector component on all connected Remote Operations Servers. The remote server instructs connectors to forward all current topology data. Each Remote Operations Connector component receives the requested information and returns the topology data to the Remote Operations Manager component on the Central SPECTRUM Server, where the topology is modeled in the database.

Distributed Concepts in the Remote Operations Suite

The distributed capability of a Remote Operations Suite environment differs from the distributed capability of a traditional CA Spectrum environment. Remote Operations Suite has unique features to support distributed deployments.

A traditional CA Spectrum Distributed SpectroSERVER (DSS) environment deploys multiple CA Spectrum servers, which are sometimes referred to as SpectroSERVERs or landscapes. Each SpectroSERVER manages a different portion of the network. In this environment, you can see a combined or rolled-up view of the entire network using the OneClick Console as an aggregation point. OneClick provides monitoring and administration capabilities for each CA Spectrum server in the distributed environments. You can also designate primary and secondary CA Spectrum servers for the fault tolerance.

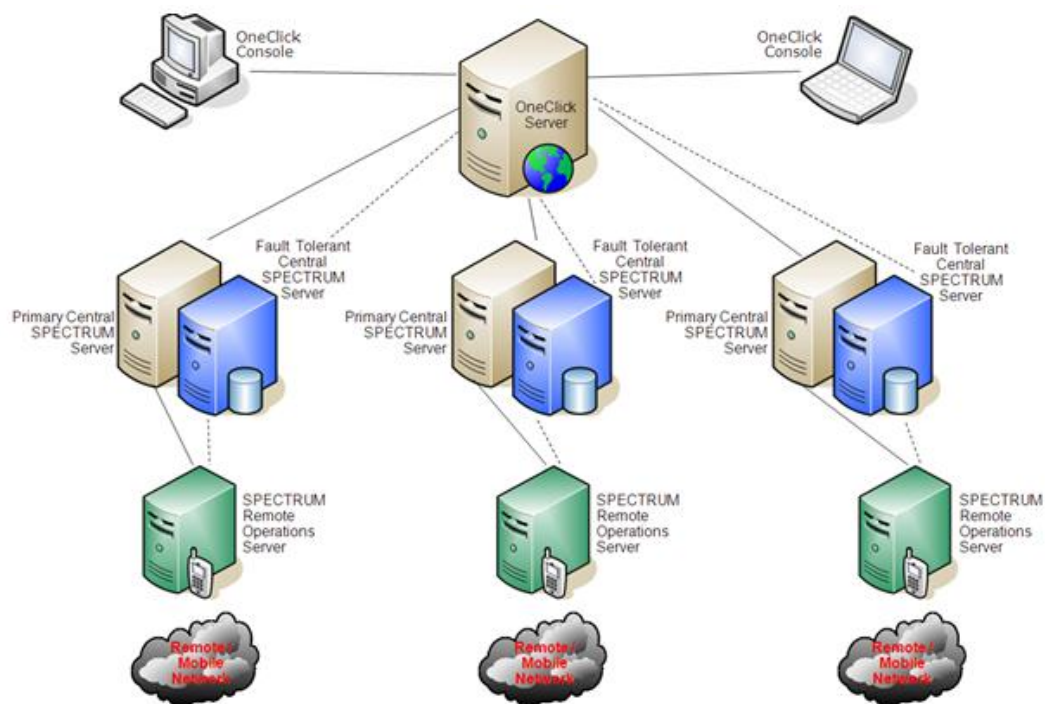
The following architecture shows a traditional CA Spectrum distributed deployment:



Remote Operations Suite also lets you deploy multiple Remote Operations Servers to manage a set of remote or mobile network devices. You can configure each Remote Operations Server to forward inventory information (for example, device and interface information) and the associated alarm data to a designated primary Central SPECTRUM Server. The primary Central SPECTRUM Server acts as the aggregation point for multiple Remote Operations Servers. Administrators at the central site have access to all of the information that has been forwarded from the Remote Operations Servers, by viewing each one on the primary Central SPECTRUM Server.

Fault tolerance features are also supported in a distributed Remote Operations configuration. You can configure each Remote Operations Server to connect to both a primary Central SPECTRUM Server and a backup Central SPECTRUM Server. All topology and alarm data is forwarded to the primary Central SPECTRUM Server. If the connection to the primary central SPECTRUM server is lost, the Remote Operations Server automatically sends a full topology and alarm update to the designated backup Central SPECTRUM Server. The Remote Operations Server then begins forwarding alarm information to the backup server. Once the connection to the primary Central SPECTRUM Server is restored, data forwarding to the backup Central SPECTRUM Server stops. The Remote Operations Server sends a full topology and alarm update to the primary Central SPECTRUM Server, and normal alarm forwarding resumes.

The following diagram shows a distributed Remote Operations deployment:



Management Visibility in a Remote Operations Environment

When a Remote Operations Server manages a network asset directly, you have access to all information that has been gathered about the device, regardless of the various methods CA Spectrum uses to collect that information. Direct management is therefore equivalent to management by a traditional CA Spectrum server. A difference appears in the available management data when the device is managed by a Remote Operations Server, but the information is viewed from a connected Central SPECTRUM Server.

When a Remote Operations Server forwards its topology to a designated Central SPECTRUM Server, the devices are represented in the Central SPECTRUM Server as "lightweight" models. Viewed locally by operators using the Remote Operations Server, the same models are "complete" models, providing complete local visibility. But the Central SPECTRUM Server only displays the essential information about these devices. You can still clearly identify the managed devices and their subcomponents. In addition, all alarms impacting the managed assets can be transferred from the Remote Operations Server to the Central SPECTRUM Server.

Less information is available from the Central SPECTRUM Server because Remote Operations Suite must operate over low-speed, unreliable connections. The communications that occur between the Remote Operations Server and the Central SPECTRUM Server are therefore optimized to conserve bandwidth.

The Remote Operations Server communicates only the information that is required to provide the Central SPECTRUM Server with a real-time view of its managed topology and operational alarm state.

Chapter 2: Setting Up Remote Operations Suite

This section contains the following topics:

[Install the Remote Operations Suite](#) (see page 13)

[Configure the Remote Operations Server](#) (see page 17)

[Fault Tolerance](#) (see page 21)

Install the Remote Operations Suite

Installing Remote Operations Servers resembles the procedure for installing CA Spectrum. The installers are similar. However, a few additional steps are required.

Designating a Main Location Server is required as part of the installation. Be sure to read [Selecting a Main Location Server](#) (see page 16) before you begin the installation.

Follow these steps:

1. Start the installation on Windows, Linux, or Solaris.
The Install dialog opens.
 2. Select the Install CA Spectrum option.
The Introduction dialog opens.
 3. Click Next to proceed.
The License Agreement dialog opens.
 4. Scroll through and read the license agreement, accept the agreement, and click Next.
The Destination Host dialog opens.
 5. Enter the name of the host system where you are installing CA Spectrum and click Next.
The SRAdmin Authentication dialog opens.
- Note:** If the 'Unable to connect to CA Spectrum Remote Administration Daemon (SRAdmin)' dialog appears, install SRAdmin before continuing with the installation. To install SRAdmin, click Install on this dialog.

6. Enter a username and password as follows, and click Next:

- For a Solaris or Linux installation, enter a username with root access. Or, you can use a sudoers file for root permissions.

Note: If you have root access when starting this installation, you are not prompted for a user name and password.

- For a Windows installation, enter a username that has Administrator rights, and verify the domain name (if applicable).

The Destination Location dialog opens.

7. Click Next to install CA Spectrum in the default directory. The default directory is C:\win32app\SPECTRUM on Windows and /usr/SPECTRUM on Solaris and Linux.

To install in a location other than the default directory, click Choose, select a location, and click Next.

The installer reports that it is extracting installation information.

The Select Destination Language dialog opens.

8. Select one of the supported languages to install in addition to English, and click Next.

Localized CsEvFormat, CsPCause and EventTables will be installed for the selected language.

The Select Options dialog opens.

9. Select Remote Operations Server as the Installation Type.
10. Select to install both the SpectroSERVER and OneClick from the list, and click Next.

Important! The Connector must be installed on a system with both OneClick and the SpectroSERVER installed.

The Host Evaluation dialog opens.

11. Scroll down to verify that no warnings appear, and click Next to proceed.

The CA Spectrum Installation Owner dialog opens.

12. Enter a username and password, and click Next. This username is used to create the initial CA Spectrum user (for the SpectroSERVER) and becomes the installation owner. For a OneClick installation, the username also determines the SpectroSERVERs to which the OneClick web server connects.

For more information, see the *Installation Guide*.

Note: For first-time installations, the default CA Spectrum password for the installation owner is spectrum.

Important! When installing OneClick, be sure to specify a CA Spectrum username to which the administrative license is associated. This user needs access to all models in CA Spectrum (ADMIN access). We recommend that you specify the installation owner that you specified during the SpectroSERVER installations. This user must also exist on the installation host and does not have to be a Windows administrative user.

The Main Location Server dialog opens.

Important! Be sure to read [Selecting a Main Location Server](#) (see page 16) before you select a server. For more information about location servers and the Main Location Server, see the *Distributed SpectroSERVER Administrator Guide*.

13. Enter a hostname for the Main Location Server and click Next. The Main Location Server should be installed on a separate server.

Note: CA Spectrum must be able to resolve the hostname, regardless of whether you provide a fully qualified hostname.

The Web Server Port Number dialog shows the default value.

14. (Optional) Enter a port number other than the default, and click Next.

Note: The default port is 80 for Windows and 8080 for Solaris and Linux.

Important! During a typical SpectroSERVER installation, you are prompted to supply a landscape handle. The Remote Operations Server installation does not prompt for this value. Instead, the installer supplies a default value of 16. In some situations, multiple SpectroSERVERs are deployed with the Remote Operations Server. You can then change the landscape handles of selected SpectroSERVERs. For more information, see [Set the Landscape Handle for the SpectroSERVER](#) (see page 16).

15. Click Next.

The Review Settings dialog opens.

16. Scroll down to ensure all the settings are what you selected and click Next.

The Installing CA Spectrum dialog appears. After CA Spectrum is installed, the status changes to 'Installation successful,' and the Next button is enabled.

17. Click Next.

The Installation Complete dialog opens.

18. Click Done.

The configuration dialog appears for a brief moment and closes.

CA Spectrum is configured for your system.

19. Click Close on the initial Install dialog. Log out, and log back in.

CA Spectrum is installed.

Next, you must [Configure the Remote Operations Connector](#) (see page 17).

Set the Landscape Handle for the SpectroSERVER

The Landscape Handle dialog that prompts you during CA Spectrum installation does not appear during Remote Operations Server installation. Instead, the handle setting for the SpectroSERVER defaults to 16. To use a different value for the landscape handle, you must set it. Unique landscape handles are crucial if you are configuring a distributed SpectroSERVER environment. Use the default handle setting for Multiple Remote Operations Servers if a Remote Operations Server does not report to another Remote Operations Server as its MLS.

Landscape handles can be assigned by using a utility named `lh_set`.

Important! Run the `lh_set` utility before you run the SpectroSERVER for the first time. Otherwise, CA Spectrum assigns a default landscape handle that is the same every time that CA Spectrum assigns it. As a result, duplicate landscape handles can be created when multiple landscapes are configured. Such landscapes can never be accessed simultaneously from the same application.

Follow these steps:

1. Navigate to the `SS` directory.
2. Enter the following command:

```
../SS-Tools/lh_set <landscape handle>
```

You can specify the new landscape handle in either decimal or hexadecimal notation. If you use decimal notation, the `lh_set` utility converts your entry into a hexadecimal landscape handle.

Note: For more information, see the *Installation Guide*.

Selecting a Main Location Server

During Remote Operations Suite installation, you are prompted to select a Main Location Server. The *main location server (MLS)* is the primary SpectroSERVER used to coordinate the information and events from all other SpectroSERVERs connected in a DSS environment. Typically, a Remote Operations Server deployment does not use the same architecture as a typical DSS deployment.

In a Remote Operations Suite deployment, select the Remote Operations Server as the Main Location Server.

Important! Do not select the designated primary Central SPECTRUM Server as the MLS.

The Remote Operations Server OneClick points to the Remote Operations SpectroSERVER as the MLS. The interactivity to the full CA Spectrum environment comes from configuring the Remote Operations Server Connector on the server VNM model to point to a SpectroSERVER in the standard CA Spectrum environment.

If your environment uses Remote Operations Servers in a DSS deployment, select your MLS, but in such a case, the MLS should not be one of your Full Production SpectroSERVERs.

Configure the Remote Operations Server

As soon as the installation completes and you have logged out of the server and logged back in, you are ready to enable the Remote Operations Connector component. This component links the Remote Operations Server to the Remote Operations Manager on the Central SPECTRUM Server. Configure the Remote Operations Connector with the information required to send the topology and alarm information to the Central SPECTRUM Server.

Follow these steps:

1. Log in to the OneClick server that is associated with the Remote Operations Suite deployment.
2. Launch the CA Spectrum Control Panel.
3. Start the SpectroSERVER process, which is equivalent to starting the Remote Operations Suite.
4. In OneClick, locate the new Remote Operations Server in the Explorer tab of the Navigation panel.
5. Expand the landscape, and expand the Universe.
6. Select the Virtual Network Manager (VNM) model.

Information about the VNM model appears in the Component Detail panel.

We recommend configuring the Connector parameters in the following order:

- a. [Topology Forwarding](#) (see page 17)
- b. [Alarm Forwarding](#) (see page 19)
- c. [Central SPECTRUM Server - General](#) (see page 20)

Configure Topology Forwarding

The Remote Operations Connector provides a representation of all modeling data in the Universe hierarchy of the associated Remote Operations Server. The Universe hierarchy includes containers, devices, ports, and applications. The Remote Operations Connector sends the topology information to the Remote Operations Manager component of the Central SPECTRUM Server. By default, the entire network topology under the Universe hierarchy is forwarded.

Configure the topology forwarding feature to selectively forward topology components. You can designate the components of the network topology that you want the Remote Operations Connector to forward to the Central SPECTRUM Server.

Follow these steps:

1. Locate the Remote Operations Connector configurations as described in [Configure the Remote Operations Server](#) (see page 17) and expand the Topology Forwarding subview.

The Topology Forwarding configuration options display.

2. Click set next to Hierarchy and select the aspects of the selected Remote Operations Server hierarchy you want to forward to the Central SPECTRUM Server:

- Entire Universe hierarchy (including all containers)
- Devices Only

The selected value displays next to Hierarchy.

3. Click set next to Device Sub-Components and select the Remote Operations Server subcomponents to forward to the Central SPECTRUM Server:

- All Device Sub-Components (ports and applications)
- Interfaces Only
- Applications Only

Note: Remote Operations Connector always forwards all device models to the Central SPECTRUM Server. To forward alarms on port and application models to the Central SPECTRUM Server, configure the Remote Operations Connector to forward these models as well. For example, if only device and interface models are sent to the Central SPECTRUM Server, then only device and interface alarms are forwarded. Alarms on application models are not forwarded.

The selected value appears next to Device Sub-Components.

Note: Do not click Update Remote Operations Topology after an initial configuration of the product. The Remote Operations Server's topology data is sent to the Central SPECTRUM Server once you establish the initial connection.

Topology forwarding is configured.

More information:

[Update Remote Operations Server Topology Data](#) (see page 24)

Configure Alarm Forwarding

The Remote Operations Servers generates the alarms. The alarms are forwarded to the Remote Operations Manager component on the Central SPECTRUM Server by the Remote Operations Connector.

Configure the alarm forwarding feature to specify the severity of alarms that should be forwarded to the Central SPECTRUM Server. You can also filter alarm forwarding, which is based on alarm probable cause IDs. The Remote Operations Connector only forwards alarms that are configured for sending to the Central SPECTRUM Server. Any alarm that does not match the alarm forwarding filter is not forwarded.

Follow these steps:

1. Locate the Remote Operations Connector configurations as described in [Configure the Remote Operations Server](#) (see page 17) and expand the Alarm Forwarding subview.

The Alarm Forwarding configuration options display.

2. Click the set link and select Yes, to select which alarm severities to send to the Central SPECTRUM Server. By default, the critical, major, minor, and maintenance alarm severity options are enabled.

The value of each alarm displays next to the alarm.

Note: Suppressed, maintenance, and initial conditions on CA Spectrum models typically do not generate actual alarms. Fewer alarms improve the performance of the SpectroSERVER process during network outages. The forwarding of suppressed, maintenance, or initial alarms by the Remote Operations Server results in the generation of these alarms in the SpectroSERVER. Verify that the alarms have been generated by opening the Alarm Management subview of the VNM model. Examine the Disable Initial Alarms, Disable Suppressed Alarms, and Disable Maintenance Alarms settings. These alarm management attributes must be set to “No” to enable alarms of that severity to be forwarded by the Remote Operations Server.

3. Click Add under the Probable Cause Filter option to specify any alarm probable cause codes to forward to the Central SPECTRUM Server.

The Add dialog appears.

4. Enter the probable cause code in the Enter PCause ID field and click OK.

The probable cause code displays in the Probable Cause Filter list.

Note: If any probable cause codes are listed in the Probable Cause Filter list, then only alarms that match a probable cause ID in that list are forwarded to the Central SPECTRUM Server. All others are not forwarded. If the Probable Cause Filter list is empty, then no filtering of alarms that are based on probable cause code is performed.

Alarm forwarding is configured.

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

Configure and Connect to the Central SPECTRUM Server

Configure each Remote Operations Connector with the name of the Central SPECTRUM Server host to connect to the Central SPECTRUM Server. The Remote Operations Connector requires information about where to forward alarm and topology data.

Note: Alarm forwarding must be configured before you set the primary and backup Central SPECTRUM Server hostnames.

Follow these steps:

1. Locate the Remote Operations Connector configurations as described in [Configure the Remote Operations Connector](#) (see page 17) and expand the General subview.

The General configuration options display.

2. Verify that the Remote Operations Server ID is correct. (The Remote Operations Server ID defaults to the local server name). If it is not correct, click set, enter the correct Remote Operations Server ID, and press Enter.

The Remote Operations Server ID displays next to Remote Operations Server ID.

3. (Optional) Click set next to Backup Central SPECTRUM Server Host Name to enter the hostname of a backup Central SPECTRUM Server, and press Enter.

Note: This hostname must not be the fully qualified hostname.

The backup hostname displays next to Backup Central SPECTRUM Server Host Name.

4. Click set next to Primary Central SPECTRUM Server Host Name, enter the hostname of the primary Central SPECTRUM Server, and press Enter.

Note: This hostname must not be the fully qualified hostname. The server that you designate as the Primary Central SPECTRUM Server can be the MLS. For more information, see [Selecting a Main Location Server](#) (see page 16). Make sure that the Remote Operations Server ID matches the Remote Operations Server local machine name.

The primary hostname displays next to Primary Central SPECTRUM Server Host Name.

Important! Initial topology and alarm data are immediately sent to the Central SPECTRUM Server once the primary Central SPECTRUM Server hostname is set. Set the primary Central SPECTRUM Server hostname last.

Subsequent topology updates occur only when contact with the Central SPECTRUM Server is reestablished after a disconnect, or with an [on-demand topology update](#) (see page 24).

Fault Tolerance

If primary and backup Central SPECTRUM Server host names are defined, the Remote Operations Server automatically starts forwarding topology and alarm information to the backup server if the connection to the primary server goes down. When this switchover happens, a full topology and alarm update is sent to the backup server and normal alarm forwarding begins.

Note: Be sure that the primary and backup Central SPECTRUM Servers are already in a fault tolerant environment before defining the host names for these servers.

Once the connection to the primary server is restored, the Remote Operations Server stops sending data to the backup server, a full topology, and alarm update is sent to the primary server, and normal alarm forwarding resumes.

Note: Manually clear the residual alarms. Delete any unnecessary RemoteOperationsManagedElement models that exist in the backup server after the Remote Operations Server stops forwarding data to it.

Chapter 3: Using Remote Operations Suite

This chapter assumes that you are the administrator at your central site, using the Central SPECTRUM Server.

This section contains the following topics:

[View Remote Operations Server Information](#) (see page 23)

[Update Remote Operations Server Topology Data](#) (see page 24)

[RemoteOperationsManagedElement Model Type](#) (see page 26)

[Search for Models](#) (see page 27)

[Device Management](#) (see page 28)

[Fault Isolation](#) (see page 28)

View Remote Operations Server Information

View information that is related to the connected Remote Operations Servers and subcomponents, from the Remote Operations Manager component on the Central SPECTRUM Server.

Follow these steps:

1. Expand Remote Operations Manager in the Explorer tab of the Navigation panel.
Remote Operations Servers currently connected display.
2. Expand each Remote Operations Server to reveal its subcomponent hierarchy.

Information and alarm data associated with the selected Remote Operations Server or Remote Operations subcomponent display in the Contents and Component Detail panels.

Name	Red Heart	Yellow Triangle	Yellow Square
My SPECTRUM	7	20	4
Favorites			
Global Collections			
Global Collection Hierarchy			
Configuration Manager (3)			
eHealth Manager (1)			
VPN Manager			
tech(0x00000)	7	20	4
Correlation Manager (1)	2	2	
Enterprise VPN Manager (5)			
Remote Operations Manager(1)	4	7	2
br07d	4	7	2
Universe (62)	3	7	2
Service Management (3)			
TopOrg			
Universe (76)	3	7	1
World			
LostFound			
Multicast Manager			
Policy Manager			
QoS Manager			
Secure Domain Manager			
Telco EMS Manager			

Update Remote Operations Server Topology Data

The Remote Operations Connector does not keep the Central SPECTRUM Server up to date with topology and modeling changes that occur on the Remote Operations Server. The Remote Operations Connector forwards topology data to the Central SPECTRUM Server only when an initial connection to the Central SPECTRUM Server is made and when the connection is reestablished after a disconnect.

You can also manually update the Remote Operations Server topology data at any time, and instruct the Remote Operations Server or Remote Operations Servers, to send the topology data to the Central SPECTRUM Server.

Note: Each time the topology data is updated, if the *Model_Name* of any models in the Remote Operations Server has changed, the corresponding lightweight Remote Operations models are also updated. Each time the topology data is updated, the alarm status for all newly-forwarded and existing managed elements is also updated.

To update topology data for all connected Remote Operations Servers

1. Select the Remote Operations Manager in the Navigation panel.
Information displays in the Contents panel.
2. Select the Information tab in the Component Detail panel and expand the Configuration subview.
The Update Remote Operations Topology button is displayed.
3. Click Update Remote Operations Topology.
The Start Remote Operations Topology Update dialog opens.
4. Click Yes to start the Remote Operations Topology Update.
The Start Remote Operations Topology Update dialog displays if the Remote Operations topology update was successful.
5. Click OK.
The topology data is updated for all connected Remote Operations Servers.

To update topology data for a single Remote Operations Server

1. Expand the Remote Operations Manager node in the Navigation panel.
All connected Remote Operations Servers display.
2. Select the single Remote Operations Server for which the topology data should be updated.
Information displays in the Contents panel.
3. Select the Information tab in the Component Detail panel and expand the Configuration subview.
The Update Remote Operations Topology button is displayed.
4. Click Update Remote Operations Topology.
The Start Remote Operations Topology Update dialog opens.
5. Click Yes to start the Remote Operations Topology Update.
The Start Remote Operations Topology Update dialog displays if the Remote Operations topology update was successful.
6. Click OK.
The topology data is updated for the selected Remote Operations Server.

You can also update the topology data for a single Remote Operations Server from the computer where that Remote Operations Server resides.

To update topology data for a single Remote Operations Server on the machine where the Remote Operations Server resides

1. Select the Remote Operations Server for which the topology data should be updated in the Navigation panel.

Information displays in the Contents panel.

2. Select the Information tab in the Component Detail panel and expand the Configuration subview.

The Update Remote Operations Topology button is displayed.

3. Click Update Remote Operations Topology.

The Start Remote Operations Topology Update dialog opens.

4. Click Yes to start the Remote Operations Topology Update.

The Start Remote Operations Topology Update dialog displays if the Remote Operations topology update was successful.

5. Click OK.

The topology data is updated for the selected Remote Operations Server.

RemoteOperationsManagedElement Model Type

The Central SPECTRUM Server can discover any or all managed network elements in the Universe hierarchy of the Remote Operations Server.

The Central SPECTRUM Server stores all of the Remote Operations-related data in the modeling database. It uses the model type RemoteOperationsManagedElement to model all network entities that are managed by a Remote Operations Server. All subcomponent relationships between two RemoteOperationsManagedElement models (for example, a "port" being a subcomponent of a "device") are modeled in the CA Spectrum database as associations, using the RemoteOperationsContains relation.

The RemoteOperationsManagedElement model type contains the following attributes:

RemoteOperationsServerId

Identifies the Remote Operations Server where the RemoteOperationsManagedElement is stored.

RemoteOperationsServerModelHandle

Identifies the RemoteOperationsManagedElement in its associated Remote Operations Server, using a unique model handle.

RemoteOperationsServerModelName

Identifies the model name given to the element inside the Remote Operations Server.

RemoteOperationsServerModelType

Identifies the model type used to model the element inside the Remote Operations Server.

You can copy and paste a RemoteOperationsManagedElement model anywhere in CA Spectrum's topology views (Universe, World, or TopOrg), to arrange your network containment.

Search for Models

Search for models if you do not know the exact hierarchy where a particular model exists.

Follow these steps:

1. Select the Locator tab in the Navigation panel on the Central SPECTRUM Server and expand Remote Operations.
All of the models for the managed elements display in the Contents panel.
2. Double-click All Remote Operations Managed Elements.
All of the server models display in the Contents panel.
3. Double-click All Remote Operations Servers.
All of the server models display in the Contents panel.
4. To search for managed elements that are based on the model name of the managed element or by the server name on which it resides, expand Remote Operations Managed Elements By and do the following actions:
 - Double-click Remote Operations Model Name to search by the name of the model.
 - Double-click Remote Operations Server to search by the name of the Remote Operations Server on which it resides.

The Search dialog opens.

5. Enter the model name for the managed element, and click OK.
6. Enter the server name for the managed element, and click OK.

The managed element displays in the Contents panel.

Note: Click Landscapes to specify the landscapes from which OneClick exports data in a distributed environment. Move the landscapes whose data you want to export data into Show Landscapes. Move any landscapes whose data you do not want to export into Hide Landscapes in the Landscape Filter.

Device Management

Remote Operations Suite limits the number of models that can be created in a CA Spectrum database. Specifically, the Remote Operations Server is limited to managing 100 device models. As a result the Remote Operations Server is limited to managing 100 network devices. The 100 device limit includes device models that have an IP address and are derived from the device model type. Devices that are modeled as hosts or as pingables are not included in this limit.

You can determine whether the Remote Operations Server can manage all of your device models using some simple arithmetic.

Example: 590 Devices

This example shows how the Remote Operations Server can manage 590 devices:

A customer network comprises 10 routers, 60 switches, 10 firewalls, 10 devices that CA Spectrum has automatically modeled using the Generic SNMP Device (GnSNMPDev) model type, approximately 500 servers and workstations, and many other devices CA Spectrum has modeled using the “pingable” device model type.

In this example, the models that would be included in the device limit would total only 90. The 10 routers, 60 switches, 10 firewalls, and the 10 devices that are modeled with GnSNMPDev would be included. The 500 workstations and servers and the other devices that are modeled as pingables do not affect the 100 device limit.

Fault Isolation

If the Central SPECTRUM Server loses contact with a Remote Operations Server, it generates a red alarm on the corresponding Remote Operations Server model. All RemoteOperationsManagedElement models that are associated with the disconnected Remote Operations Server model display a suppressed (gray) condition, indicating that their status is unknown.

The Central SPECTRUM Server cannot manage the RemoteOperationsManagedElement models in a suppressed state. When the Central SPECTRUM Server reestablishes contact with the Remote Operations Server, the red alarm is cleared. The state of all corresponding RemoteOperationsManagedElement models is reevaluated.

By default, the Central SPECTRUM Server waits for 30 seconds for a keepalive signal, or heartbeat, from the Remote Operations Server before generating the red alarm. You can change this default setting using the following parameter in the ".vnmrc" file of the Central SPECTRUM Server:

ros_heartbeat_timeout

Specifies the maximum number of seconds the Remote Operations Manager waits for a heartbeat from the Remote Operations Server, before a contact lost alarm is raised. This parameter must be configured on Central SPECTRUM Server.

The heartbeat parameter has the following format:

ros_heartbeat_timeout=# of seconds

Default: 30 seconds

Note: When contact with a Remote Operations Server is lost, the previously existing alarms on all RemoteOperationsManagedElement models still appear in the OneClick Alarms tab.

Chapter 4: Alarms

This section contains the following topics:

[Remote Operations Alarms](#) (see page 31)

[View Remote Operations-Related Alarms](#) (see page 33)

[Remote Operations Forwarding Events](#) (see page 35)

Remote Operations Alarms

When the Remote Operations Server forwards an alarm to the Central SPECTRUM Server, it includes two important pieces of information: the title of the alarm, and the actual text of the event that prompted alarm generation.

The restrictions of tactical deployments and geography can mean that the version of CA Spectrum that is installed and running on the Remote Operations Server is slightly different from the version that is running on the Central SPECTRUM Server. In such a case, the two servers do not have the same fault detection intelligence. Therefore, the Central SPECTRUM Server lacks the alarm support files. The alarm support files are required to generate the identical alarm type as was generated on the Remote Operations Server.

To ensure the Central SPECTRUM Server handles all alarm types that the Remote Operations Server sends, the Central SPECTRUM Server uses a set of Remote Operations-specific alarm types. One alarm type for each alarm severity. When an alarm is forwarded from the Remote Operations Server, the Central SPECTRUM Server generates the appropriate Remote Operations-specific alarm, which is based on the severity of the forwarded alarm.

This generic alarm is displayed in the OneClick Alarms tab like all other alarms. Instead of displaying a generic alarm title, the Alarm Details tab displays the title of the alarm that was forwarded from the Remote Operations Server. In addition, the Central SPECTRUM Server appends the actual event text that is forwarded from the Remote Operations Server to the event that generates the forwarded alarm. This event text is also displayed in the Alarm Details tab, like all other event text.

Example: Alarm Title

This example shows an alarm title from the Remote Operations Server:

DEVICE HAS STOPPED RESPONDING TO POLLS

Example: Probable Cause Text

This example shows the body of the Remote Operations critical alarm probable cause:

CRITICAL ALARM ON REMOTE OPERATIONS-MANAGED ELEMENT

SYMPTOMS:

A critical alarm for this Remote Operations-managed element has been forwarded to SPECTRUM from a SPECTRUM Remote Operations Server.

PROBABLE CAUSES:

A critical alarm for this Remote Operations-managed element has been forwarded to SPECTRUM from a SPECTRUM Remote Operations Server.

RECOMMENDED ACTIONS:

1) Check the event associated with this alarm for more details.

Example: Actual Event Text

In the following example, the event that is associated with the alarm displays the actual event text that was generated in the Remote Operations Server:

{d "%w- %d %m-, %Y - %T"} - A critical alarm has been forwarded to SPECTRUM from SPECTRUM Remote Operations Server TEAM_A. See below for alarm details:

{d "%w- %d %m-, %Y - %T"} - Device Router1 of type Rtr_Cisco has stopped responding to polls and/or external requests. An alarm will be generated. (event [{e}])
(event [{e}])

The following image shows each part of the alarm as it appears in the OneClick Console:

The screenshot displays the OneClick Console interface. The top section shows a list of alarms filtered by severity. Below this, the 'Component Detail' section provides a detailed view of a selected alarm. Annotations highlight specific parts of the alarm details:

- Indicates the alarm title:** Points to the 'Title' column in the alarm list and the 'WIDE-AREA LINK CONTACT LOST' title in the component detail.
- Indicates the probable cause text:** Points to the 'Probable Cause' section in the component detail.
- Indicates the actual event text:** Points to the 'Actual Event' section in the component detail.

Severity	Date/Time	Name	Title	Network Address	Secure Domain	Type	Available Filters
Critical	Jun 12, 2008 12:03:14 PM EDT	192.168.100.8	WIDE-AREA LINK CONTACT LOST			RemoteOperatio...	tracy (0x3000000)
Critical	Jun 12, 2008 12:03:14 PM EDT	192.168.95.144	WIDE-AREA LINK CONTACT LOST			RemoteOperatio...	tracy (0x3000000)
Major	Jun 12, 2008 12:03:14 PM EDT	192.168.100.8	HIGH MEMORY UTILIZATION			RemoteOperatio...	tracy (0x3000000)
Major	Jun 12, 2008 12:03:14 PM EDT	acrimac151677	HIGH CPU UTILIZATION			RemoteOperatio...	tracy (0x3000000)
Major	Jun 13, 2008 10:03:05 AM EDT	uniper-96.3.net	HIGH CPU UTILIZATION			RemoteOperatio...	tracy (0x3000000)

Component Detail: 192.168.100.8 of type RemoteOperationsManagedElement

Alarm Details: Information | Impact | Host Configuration | Root Cause | Links | Performance | Alarm History | Troubleshoot | Events

WIDE-AREA LINK CONTACT LOST
 Jun 12, 2008 12:03:14 PM EDT
 A critical alarm has been forwarded from Remote Operations Server wickd. See below for alarm details:
 The contact status of WA Link model (name - 192.168.100.8, type - WA_Link) is in a "lost" state. [Open](#)

Severity: Critical
Impact: 0
Acknowledged: set
Clearable: Yes
Trouble Ticket ID: set

Symptoms: A critical alarm for this Remote Operations ManagedElement has been forwarded to SPECTRUM from a Remote Operations Server.

Probable Cause: A critical alarm for this Remote Operations ManagedElement has been forwarded to SPECTRUM from a Remote Operations Server.

Actions: 1) Check the event associated with this alarm for more details.

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

View Remote Operations-Related Alarms

You can view the Remote Operations-related alarms on all models in the Remote Operations hierarchy.

Important! Configure the Remote Operations Connector on each Remote Operations Server to forward alarms to the Central SPECTRUM Server. For more information about forwarding alarms to the Central SPECTRUM Server, see [Configure Alarm Forwarding](#) (see page 19).

To view only the Remote Operations-related alarms on the Central SPECTRUM Server, select the Remote Operations Manager model in the Explorer tab of the Navigation panel. Click the Alarms tab in the Contents panel.

Information such as alarm symptoms and possible alarm causes displays in the Contents and Component Detail panels for all models in the Remote Operations hierarchy.

The screenshot displays the Remote Operations Manager interface. The top panel, titled 'Contents: Remote Operations Manager of type RemoteOperationsManager', shows a list of alarms filtered by severity. The bottom panel, titled 'Component Detail: 192.168.100.8 of type RemoteOperationsManagedElement', provides a detailed view of a specific alarm.

Alarms List:

Severity	Date/Time	Name	Title	Network Address	Secure Domain	Type	Landscape
Critical	Jun 12, 2008 12:03:14 PM EDT	192.168.100.8	WIDE-AREA LINK CONTACT LOST			RemoteOperatio...	tracy (0x3000000)
Critical	Jun 12, 2008 12:03:14 PM EDT	192.168.95.144	WIDE-AREA LINK CONTACT LOST			RemoteOperatio...	tracy (0x3000000)
Major	Jun 12, 2008 12:03:14 PM EDT	192.168.100.9	HIGH MEMORY UTILIZATION			RemoteOperatio...	tracy (0x3000000)
Major	Jun 12, 2008 12:03:14 PM EDT	aprimac151677	HIGH CPU UTILIZATION			RemoteOperatio...	tracy (0x3000000)
Major	Jun 13, 2008 10:03:05 AM EDT	uniper-95.3.net	HIGH CPU UTILIZATION			RemoteOperatio...	tracy (0x3000000)

Component Detail: 192.168.100.8 of type RemoteOperationsManagedElement

Alarm Details:

- Severity:** Critical
- Impact:** 0
- Acknowledged:** set
- Clearable:** Yes
- Trouble Ticket ID:** set

Symptoms: A critical alarm for this Remote Operations ManagedElement has been forwarded to SPECTRUM from a Remote Operations Server.

Probable Cause: A critical alarm for this Remote Operations ManagedElement has been forwarded to SPECTRUM from a Remote Operations Server.

Actions: 1) Check the event associated with this alarm for more details.

Note: If the topology data on the Central SPECTRUM Server is not synchronized with the topology data on the Remote Operations Server or subcomponent, the alarm data does not update. Perform an on-demand Topology synchronization to ensure that your topology and alarm data is current. For more information about synchronizing alarm data, see [Update Remote Operations Server Topology Data](#) (see page 24).

Remote Operations Forwarding Events

When an alarm is forwarded to the Central SPECTRUM Server for processing, a Remote Operations Forwarding Event is generated on the corresponding lightweight Remote Operations model (RemoteOperationsManagedElement). The Remote Operations Forwarding Event contains the following varbinds:

RemoteOperationsServerId

Identifies the Remote Operations Server where the RemoteOperationsManagedElement is stored.

RemoteOperationsServerModelHandle

Identifies the RemoteOperationsManagedElement in its associated Remote Operations Server, using a unique model handle.

RemoteOperationsServerEventCode

Identifies the standardized CA Spectrum event/alarm code for the event.

RemoteOperationsServerEventSeverity

Identifies the severity of the event/alarm. Possible values include critical, major, minor, maintenance, suppressed, initial, and message.

RemoteOperationsServerEventType

Identifies the type of event. Possible values include message, alarm_set, and alarm_cleared.

RemoteOperationsServerEventCommentData

Displays a textual description of the event that caused an alarm to be generated or cleared.

RemoteOperationsServerEventTitle

Identifies the textual title (abstract) of the alarm.

Note: CA Spectrum does not log the Remote Operations Forwarding Event. CA Spectrum applies event rules to the Remote Operations Forwarding Event that determine the type of alarm or message event that is generated and logged. These event rules are stored in the following file: <\$\$SPECROOT>/SS/CsVendor/Spectrum_ROS/EventDisp.

Remote Operations Alarming Events

A Remote Operations Forwarding Event is mapped to the Remote Operations Alarming Event by the event rules if the value of the RemoteOperationsServerEventType varbind is equal to "alarm_set". The following types of Remote Operations Alarming Events are defined:

- Remote Operations Critical Alarm Event
- Remote Operations Major Alarm Event
- Remote Operations Minor Alarm Event
- Remote Operations Maintenance Alarm Event
- Remote Operations Suppressed Alarm Event
- Remote Operations Initial Alarm Event

The value of the RemoteOperationsServerEventSeverity varbind determines which Remote Operations Alarming Event is generated. CA Spectrum logs the event. The event is used to generate the appropriate alarm. All varbind values in the Remote Operations Forwarding Event are copied to the new event.

Remote Operations Clearing Events

A Remote Operations Forwarding Event is mapped to the Remote Operations Clearing Event by the event rules if the value of the RemoteOperationsServerEventType varbind is equal to "alarm_cleared". This event clears any existing alarm on a model that has the same RemoteOperationsServerEventCode and RemoteOperationsServerEventSeverity values. All varbind values in the Remote Operations Forwarding Event are copied to the new event.

Note: When clearing events, the RemoteOperationsServerEventCode that is sent is not the actual event code that was generated in the Remote Operations Server. Rather, the code for the event that generated the original alarm is sent.

Remote Operations Message Events

A Remote Operations Forwarding Event is mapped to the Remote Operations Message Event by the event rules if the RemoteOperationsServerEventType varbind is equal to "message". This event is for informational purposes only and is not used to generate an alarm. However, this event is logged to CA Spectrum. All varbind values in the Remote Operations Forwarding Event are copied to the new event.

To create your own event and alarm types, modify the EventDisp file, which is located in <SPECROOT>/SS/CsVendor/Spectrum_ROS.

Index

A

- about • 26
- alarms
 - about • 31
 - fault isolation • 28
 - forwarding • 19
 - viewing • 33
- architecture • 9

C

- Central SPECTRUM Server
 - about • 7
 - backup • 20
 - host name • 20
 - primary • 20
- components • 7
- configuring
 - alarm forwarding • 19
 - Central SPECTRUM Server host name • 20
 - Remote Operations Server • 17
 - topology forwarding • 17

D

- devices • 28
- Distributed SpectroSERVER (DSS) environment • 9

F

- fault isolation • 28
- fault tolerance • 21

M

- modeling • 26
- models
 - about • 11
 - creating • 28
 - searching for • 27

N

- network management • 11

P

- probable cause filter list • 19

R

- Remote Operations Alarming Events • 36
- Remote Operations Clearing Events • 36
- Remote Operations Connector
 - about • 7
- Remote Operations Forwarding Events • 35
- Remote Operations Message Events • 36
- Remote Operations Server
 - bout • 7
 - configuring • 17
- Remote Operations Suite • 9
- RemoteOperationsManagedElement models
 - and fault isolations • 28
 - and fault tolerance • 21
- RemoteOperationsServerEventCode varbind • 35, 36
- RemoteOperationsServerEventCommentData varbind • 35
- RemoteOperationsServerEventSeverity varbind • 35, 36
- RemoteOperationsServerEventTitle varbind • 35
- RemoteOperationsServerEventType varbind • 35, 36
- RemoteOperationsServerId varbind • 35
- RemoteOperationsServerModelHandle varbind • 35

S

- searches • 27

T

- topology
 - forwarding • 17, 20
 - updating • 20, 24

V

- viewing
 - alarms • 31, 33
 - Remote Operations Server information • 23
- VNM model • 17