VMware Smart Assurance Service Assurance Manager Operator Guide

VMware Smart Assurance 10.0.0

vmware®

You can find the most up-to-date technical documentation on the VMware website at:

https://docs.vmware.com/

If you have comments about this documentation, submit your feedback to

docfeedback@vmware.com

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Copyright © 2019 VMware, Inc. All rights reserved. Copyright and trademark information.

Contents

1 Preface 6

Purpose 6

Audience 7

VMware Smart Assurance Service Assurance Manager installation directory 7

VMware Smart Assurance Service Assurance Manager 7

Related documentation 8

Suggestions for searching PDF files 9

Conventions used in this document 9

Pathname conventions 10

Graphical conventions 10

Manager 10

Where to get help 10

Your comments 11

2 Introduction 12

Overview 12

Notification concepts 13

Global Console overview 14

Watch4net 34

3 Starting a Session 36

Overview 36

Run MSA server 36

Opening the Global Console 37

Opening an additional Global Console 39

Opening a Web Console 40

Closing a console and ending a session 41

Attaching to different or multiple Manager s 42

4 Examining Notifications 44

Accessing notifications 44

About notifications 44

Displaying notification properties 49

Adjusting the contents of a Notification Log view 55

Using filters 58

5 Examining Topology 61

Accessing topology 61

Available topological information and its representation 62
Topology Browser Console or view 62
Finding an instance or device 65
Using the Containment dialog box 67

6 Examining Maps 69
Accessing maps 69
Available topological information and its representation 71
Representing notifications in maps 73
Types of maps 75
Adjusting the appearance of a map 79
Customizing map backgrounds 80
Viewing large maps: Overview window 82
Filtering maps 83

7 Examining Summaries 85
Accessing summary information 85
About summaries 86
Adjusting the contents of a Summary view 87

8 Examining Status Tables 92
Accessing Status Table information 92
About Status Table information 92
Configuring a Status Table view 93

9 Responding to Notifications 96
The notification life cycle 96
Taking action 102
Saving and recording information 118
HyperNotif Statistics 123

10 Customizing Your Console 125
Changing the console appearance 125
Adjusting Java properties 126
Tailoring your console with views 133
Saving a console 138

11 Troubleshooting 141
Common issues and resolutions 141
Common issues for Companion UI 143

12 Wildcard Patterns 145

Types of wildcard patterns 145

Preface

1

As part of an effort to improve its product lines, VMware periodically releases revisions of its software and hardware. Therefore, some functions described in this document might not be supported by all versions of the software or hardware currently in use. The product release notes provide the most up-to-date information on product features.

Contact your VMware technical support professional if a product does not function properly or does not function as described in this document.

Note This document was accurate at publication time. Go to VMware Online Support docs.vmware.com to ensure that you are using the latest version of this document.

This chapter includes the following topics:

- Purpose
- Audience
- VMware Smart Assurance Service Assurance Manager installation directory
- VMware Smart Assurance Service Assurance Manager
- Related documentation
- Suggestions for searching PDF files
- Conventions used in this document
- Pathname conventions
- Graphical conventions
- Manager
- Where to get help
- Your comments

Purpose

The VMware Smart Assurance Service Assurance Manager Operator Guide describes how to use the Global Console to access event information and diagnostic results that the Service Assurance Global Manager abstracted and consolidated from underlying domains.

Audience

This guide is intended for administrators who are responsible for deploying, installing, and configuring the Global Manager. IT managers who seek to understand the role of the Global Manager in the context of an VMware Smart Assurance solution may also find this guide useful.

In addition to the configuration guides for specific components, administrators should also read the VMware Smart Assurance Service Assurance Manager Deployment Guide and the VMware Smart Assurance System Administration Guide Guide.

VMware Smart Assurance Service Assurance Manager installation directory

In this document, the term BASEDIR represents the location where VMware Smart Assurance software is installed:

- For UNIX, this location is: /opt/InCharge/<*productsuite*>.
- For example, on UNIX operating systems, VMware Smart Assurance Service Assurance Manager is, by default, installed to /opt/InCharge/SAM/smarts.

  Optionally, you can specify the root of BASEDIR to be something other than /opt/InCharge (on UNIX) but you cannot change the <*product*> location under the root directory.

  The VMware Smart Assurance System Administration Guide provides more information about the directory structure of VMware Smart Assurance software.

VMware Smart Assurance Service Assurance Manager

The VMware Smart Assurance Service Assurance Manager includes the following products:

- Service Assurance Manager (Global Manager), includes Business Impact Manager (BIM) and Failover System
- Global Console
- Business Dashboard
- Companion UI
- SAM Native Adapters:
  - Service Assurance Manager Notification Adapters (E-Mail Notifier Adapter, Script Notifier Adapter, SNMP Trap Notifier Adapter, Log File Notifier Adapter)
  - Adapter Platform (Adapter Platform server, Syslog Adapter, SNMP Trap Adapter, sm_ems command-line interface)
  - VMware Smart Assurance Adapter for UIM/O
  - XML Adapter

Related documentation

In addition to this document, VMware Corporation provides a help system for command line programs as well as product documentation.

Help for command line programs

Descriptions of command line programs are available as HTML pages. The index.html file, which provides an index to the various commands, is located in the BASEDIR/smarts/doc/html/usage directory.

VMware Smart Assurance documentation

Readers of this guide may find the following related documentation helpful:

- Smarts Foundation EMC Data Access API (EDAA) Programmer Guide
- VMware Smart Assurance Common Information Model (ICIM) 1.11 Reference for Non-Service Assurance Manager Products
- VMware Smart Assurance Common Information Model (ICIM) Reference for Service Assurance Manager
- VMware Smart Assurance Foundation Documentation Portfolio
- VMware Smart Assurance System Administration Guide
- VMware Smart Assurance ASL Reference Guide
- VMware Smart Assurance Perl Reference Guide
- VMware Smart Assurance Dynamic Modeling Tutorial
- VMware Smart Assurance MODEL Reference Guide

VMware Smart Assurance Service Assurance Manager documentation

The following documents are relevant to users of the
VMware Smart Assurance Service Assurance Manager:

- VMware Smart Assurance Service Assurance Manager Release Notes
- VMware Smart Assurance Open Source License and Copyright Information
- VMware Smart Assurance Service Assurance Manager Introduction
- VMware Smart Assurance Installation Guide for SAM, IP, ESM, MPLS, and NPM Managers
- VMware Smart Assurance Service Assurance Manager Deployment Guide
- VMware Smart Assurance Service Assurance Manager Configuration Guide
- VMware Smart Assurance Service Assurance Manager Operator Guide

- VMware Smart Assurance Service Assurance Manager Dashboard Configuration Guide
- VMware Smart Assurance Business Impact Manager User Guide
- VMware Smart Assurance Failover System User Guide
- VMware Smart Assurance Service Assurance Manager Notification Adapters User Guide
- VMware Smart Assurance Service Assurance Manager Adapter Platform User Guide
- VMware Smart Assurance Adapter for Unified Infrastructure Manager/Operations Configuration Guide
- VMware Smart Assurance XML Adapter User Guide
- VMware Smart Assurance Notification Module User Guide
- VMware Smart Assurance Service Assurance Manager Troubleshooting Guide
- VMware Smart Assurance Companion UI Online Help
- VMware Smart Assurance Companion UI Open Source License and Copyright Information for GPLv3 as Included with a Distribution of SLES 11
- VMware Smart Assurance Service Assurance Manager Documentation Portfolio

  The VMware Smart Assurance Documentation Catalog provides documentation resources for other VMware Smart Assurance products.

Suggestions for searching PDF files

You can search across multiple PDF files by using the Adobe Acrobat Reader software:

1. If the documentation is not accessible to all users of the VMware Smart Assurance product, copy the contents of the BASEDIR/smarts/doc/pdf directory to a central location, such as a shared drive on your LAN, so that operators and others can view the documentation.
2. To search throughout the documentation library, open the Acrobat Reader software:
3. Select **Edit > Search**, and type a word or phrase.
4. Select **All PDF Documents** in, in the **Where would you like to search** option, and type the pathname of the location where the PDF documents reside.

   If you have more than one VMware Smart Assurance product installed, you can set up cross-product document searches by copying files from the BASEDIR/smarts/doc/pdf directory for each product into this common documentation directory path.

Conventions used in this document

VMware uses the following convention for special notices:

Note NOTICE is used to address practices not related to personal injury.

Typographical conventions

VMware uses the following type style conventions in this document:

Bold	Use for names of interface elements
Italic	Use for full titles of publications referenced in text
`Monospace`	Use for: ■ System output, such as an error message or script ■ System code ■ Pathnames, filenames, prompts, and syntax ■ Commands and options
`Monospace italic`	Use for variables.
`Monospace bold`	Use for user input.
[ ]	Square brackets enclose optional values
|	Vertical bar indicates alternate selections — the bar means “or”
{ }	Braces enclose content that the user must specify, such as x or y or z
...	Ellipses indicate nonessential information omitted from the example

Pathname conventions

Directory pathnames are shown with forward slashes (/).

Graphical conventions

Under UNIX, the consoles appear with slight differences. For example, in views that display items in a tree hierarchy such as the Topology Browser an open circle appears for UNIX.

Manager

Unless otherwise specified, the term Manager is used to refer to VMware Smart Assurance programs such as Domain Managers, Global Managers, and adapters.

Where to get help

VMware support, product, and licensing information can be obtained as follows:

Product information

For documentation, release notes, software updates, or information about VMware products, go to VMware Online Support at:

docs.vmware.com

Technical support

Go to VMware Online Support. You will see several options for contacting VMware Technical Support. Note that to open a service request, you must have a valid support agreement. Contact your VMware sales representative for details about obtaining a valid support agreement or with questions about your account.

Your comments

Your suggestions will help us continue to improve the accuracy, organization, and overall quality of the user publications. Provide your feedback of this document to:docs.vmware.com.

Introduction

2

This guide is intended for operators who are responsible for acting upon the failures reported by the VMware Smart Assurance Service Assurance Manager(Service Assurance) product.

This chapter includes the following topics:

- Overview
- Notification concepts
- Global Console overview
- Watch4net

Overview

In a typical Operations center, there are several operators who may perform monitoring duties and assist with or perform problem resolution. In order to perform their duties, operators need information about their managed domains and the events that occur. For example, they may need information about topological relationships, sources of notifications, and how the events affect other infrastructure devices.

Note Console access is controlled by the user profile that is associated with a user account. Therefore, users might have access to different types of consoles and console operations. For example, a user might be able to browse for details but not be able to acknowledge a notification or add a view to a console. Also, certain features are controlled by your VMware Smart Assurance license. The VMware Smart Assurance Service Assurance Manager Configuration Guide provides additional console operations information.

Using the Global Console, an operator with access to the appropriate console operations can:

- Investigate topological information, including detailed information about an element's internal components. Topological information is presented in a topological tree format and map representations.
- Monitor notifications and identify the causes of each failure and systems that the failure affects.
- Respond to notifications. For example, operators can take ownership of notifications, open trouble tickets, or ping a device.

- Save information, print information, and record tracking comments in notification audit logs.

  In addition, users can perform administrative tasks such as configuring Global Managers and managing underlying Domain Managers if they have administrative privileges and access to those console operations.

  If you have installed Watch4net 6.2 along with Service Assurance Manager 9.2, you can access various console components from within Watch4net. For more information on installing and configuring Watch4net, refer to the
  VMware Smart Assurance SolutionPack Installation and Configuration Guide.

  Global Console overview on page 20 contains a discussion of the layout and features of the Global Console. *Notification concepts on page 19* includes a general discussion of notifications.

Notification concepts

Service Assurance notifications are generated when abnormal conditions occur in your underlying managed domains. The underlying domains, such as VMware Smart Assurance IP Availability Manager and VMware Smart Assurance IP Performance Manager, pass the notifications and any relevant event or topological information to the Service Assurance Global Manager. The Global Manager, in turn, consolidates, abstracts, and passes the notifications to clients such as the Global Console or adapters.

Notifications are objects in the Global Manager or Adapter Platform. Notifications represent the events received from Domain Managers, adapters, or other underlying sources or notifications received from Global Managers or Adapter Platforms. Each notification consists of a set of attributes that describe properties of the notification, such as the severity of the notification and a textual description of the event. (Notification Log columns contains a list of visible attributes.)

A notification list configured by your administrator determines which notifications appear in your console and are reflected in a map. Your administrator can use special filters to organize notifications by some useful criteria and then associate the filtered list with your user profile. As a result, your console may display all or a subset of possible notifications. As an operator, you can further refine your display by setting additional filters provided as console options.

The severity of notifications is reflected in severity icons, color-coded rows and indicator bars underneath map icons. *“About notifications” on page 56* and *“Displaying notification properties” on page 62* contains a description of notifications, severity icons, their color coding, and how to display their properties. *“Representing notifications in maps” on page 88* includes a description of map icons and their color coding.

Note If a notification list does not include an event, notifications for the event will not appear in your console or be reflected in the map icons. For example, if a notification list excludes all events from a specific router, the router always appears with a normal state in the map. (If your console does not accurately reflect observed conditions, contact your administrator.)

Service Assurance information is archived at time intervals specified by the administrator and can be viewed later using a text editor. The archives include notifications that are acknowledged and their related audit logs. Once notifications are archived, they no longer display in the Global Console. The VMware Smart Assurance Service Assurance Manager Configuration Guide includes information about archival parameters and the archived files.

Service Assurance notifications

Most of the notifications that appear in the Global Console are generated by underlying Managers. However, the Global Manager will generate a Session Disconnected notification when an underlying Manager disconnects from it. Also, if Business Impact Manager is deployed, the Global Manager will generate business impact notifications. Chapter 11 Troubleshooting includes information about disconnect situations. The VMware Smart Assurance Business Impact Manager User Guide includes information about business impact notifications.

Detailed descriptions of diagnostic results for specific VMware Smart Assurance applications like VMware Smart Assurance IP Availability Manager, VMware Smart Assurance IP Performance Manager, and VMware Smart Assurance IP Discovery Manager are described in their respective user guides.

Types of managers

Depending upon your Service Assurance deployment, a Global Manager can be: a Service Assurance Global Manager or SAM Adapter Platform.

A Domain Manager can be: an IP Availability Manager, IP Performance Manager, Discovery Manager, or Application Connectivity Monitor Manager.

The term Manager refers to either a Global Manager or Domain Manager.

Global Console overview

The Global Console is a collection of consoles:

- The Notification Log Console presents notifications in tabular format.

  From the Notification Log Console for a selected notification, you can also open the Notification Properties workspace in a browser. The workspace may contain one or more apps that provide detailed information about the notification. Online help in the Companion UI provides complete information about the available apps and features.

- The Map Console graphically represents your topology in a map format. In the map, icons change color when they are affected by one or more abnormal conditions.
- The Topology Browser Console represents the topology in a hierarchical format and provides topological information.
- The Summary View Console represents overviews or summaries of notifications organized by meaningful criteria.

- The Status Table Console represents the status of underlying infrastructure elements as they affect the collection objects (ServiceOffering, ServiceSubscriber, or any group created by your administrator) specified in the Status Table.
- The Web Console provides Global Console functionality in a standard web browser.
- The Domain Manager Administration Console enables administrators to discover topology and manage underlying Domain Managers.

  The VMware Smart Assurance IP Manager Concepts Guide contains information about discovery. Information about polling and thresholds accessed by the Domain Manager Administration Console for specific VMware Smart Assurance applications is provided in their respective user guides.
- The Global Manager Administration Console enables administrators to configure Global Managers.

  The VMware Smart Assurance Service Assurance Manager Configuration Guide includes information about the Global Manager Administration Console.
- The Topology Builder Console enables administrators to modify and refine the topology stored in the VMware Smart Assurance repository.

  This console is available if Business Impact Manager is deployed. The VMware Smart Assurance Business Impact Manager User Guide includes information about the Topology Builder Console.

  The following consoles display information from or manage:
- Global Managers — A Notification Log Console, Map Console, Summary Console, Status Table Console, Global Manager Administration Console, Topology Builder Console for Business Impact Manager, and views.
- Domain Managers — A Domain Manager Administration Console.

  A Topology Browser Console or view can display information from Global Managers and Domain Managers.

  After you log in, one or more consoles appear, depending upon your user profile. For example, if your user profile is configured for the Notification Log Console and Map Console, then two consoles will appear after you log in. Since Domain Managers do not maintain user profiles, if you log in to a Domain Manager, the Topology Browser Console appears first.

  You can also customize a console for your operational needs, save it, and continue to use it. For example, you can add one or more views to a console.

  The layout of each console, including menu options and toolbar buttons, is briefly described in the subsequent sections. More complete information about individual menu options is provided in subsequent chapters. Menu options and toolbar buttons might be disabled or not appear if you do not have access to those console operations.

Tool tips are available for each console. A tool tip provides information about console components, notifications, map icons, and summaries. To activate a tool tip, hold the cursor over the object. For example, in the Topology View topology tree, if you hold the cursor over a Global Manager, the tool tip provides the IP address and port number. If the text in an attribute field of the Notification Log is truncated, the full text is displayed in the tool tip.

The status bar for each console displays status Ready for example, and the following information:

- For a locally saved console, the directory path and its filename.
- For a remotely saved console, the Manager or IP address where it is saved, username, and the console name.

  If you logged in using a default user profile, the console name Notification Log appears unless the name has been modified by an administrator.
- For an unsaved console, the text "Not saved" appears.

  To quickly open menus in the consoles, press Alt + underlined character. For example, to open the File menu, press Alt + F.

View concepts

VMware Smart Assurance information is displayed in the following views:

- Notification Log
- Map
- Topology Browser
- Summary View
- Status Table
- Notification Properties
- Containment

  Depending on your VMware Smart Assurance deployment, you will see these views in a Global Console window, Web Console window (available through a Web Browser), in a Business Dashboard configured by your administrator, or in a third-party Web Portal product.

  You or your administrator can configure views to display certain information, for example, by applying filters. These views can be saved and associated with user accounts and user profiles. Views that are saved in HTML (as Java applets) for display in web browsers are called dashboard viewlets. Dashboard viewlets are available when the VMware Smart Assurance Business Dashboard is installed.

  You can display more than one view in a Global Console window. For example, if you wish, you can include a Notification Log view along with a Map and a Status Table in a console. *“Tailoring your console with views” on page 158* includes additional information about managing view display.

  In a view, to perform actions such as saving or deleting, or to access menu options, you need to activate the view. To do so, click anywhere in the view. The active view has a black border.

Availability of Dashboard viewlets

Generally, views that are available for the Global Console are available for the Web Console (as views), Business Dashboard (as dashboard viewlets), and third-party Web Portal products (as dashboard viewlets). Table 1 on page 22 indicates which views can be implemented as dashboard viewlets.

Table 2-1. View availability

Views	Available as Dashboard viewlets?
Notification Log view	Yes
Map	Yes
Summary view	Yes
Status Table view	Yes
Notification Properties view	Yes
Containment view	Yes
Topology Browser view	No

Layout of a Notification Log Console

The Notification Log Console is designed specifically for viewing notifications. It consists of one view, the Notification Log view. Figure 1 on page 23 illustrates one example of a Notification Log Console for an administrator. Your Notification Log Console may look slightly different.

Notification Log menus and shortcut menus summarizes menu options for the Notification Log Console. Notification Log Console toolbar buttons summarizes toolbar buttons.

The notification list configured by your administrator is included in the title of the Notification Log view. For example, the title "Notification Log - Default" identifies a notification list named Default.

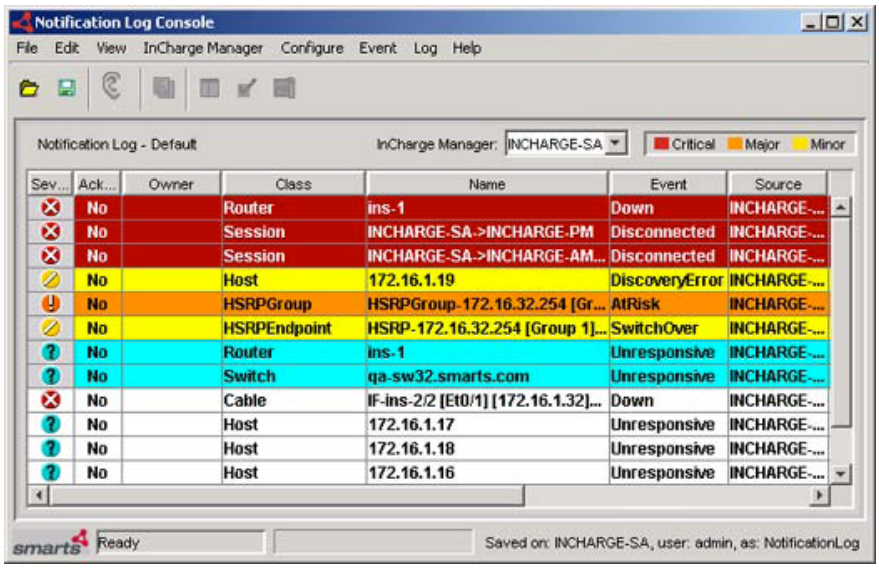
The Manager menu lists attached Global Managers. You can view notifications for a different attached Global Manager by selecting it from the menu. Domain Managers are not listed in the menu.

The notification legend and icons in the Severity column provide the color indicators that reflect the notifications' severity.

You can also customize the Notification Log view with a filter. The filter enables you to select attributes and specify wildcard characters to control which notifications appear in the view.

Figure 1 on page 23 provides an example of a Notification Log Console for an administrator.

Figure 2-1. Notification Log Console for an administrator



Notification Log menus and shortcut menus

Table 2 on page 24 summarizes the menus that are available for the Notification Log Console or view. The two menu items, Event and Log, are specific to the Notification Log. The Configure menu is displayed depending on your user access control privileges.

Table 2-2. Notification Log menus and their options

Menu	Option	Description
File	New	Opens a new console.
	Open	Opens an existing console, locally saved or remotely saved.
	Close	Closes an individual console.
	Save	Saves an unsaved console on a local or remote host. Saves a saved console to a previously-specified destination.
	Save As	Saves a console on a local or remote host.
	Layout	Arranges multiple views in a console and changes console title.
	Exit	Ends the session and closes all consoles.
Edit	Find Instance	Searches for any topological element in any class including application services, service offerings, service subscribers, and systems.
	Find System	Searches for a system (infrastructure element).
	Recipients	Opens the Recipient Editor dialog box for email or pager tools.
View	Java Console	Displays console debugging information, including store exceptions, errors reading attributes, and stack traces.
	Message Log	Displays communications sent from a Manager to the console.
	Toolbar	Toggles the display of the toolbar buttons.
	Status	Toggles the display of the status bar.
	Add View	Inserts a view in the current console.

Table 2-2. Notification Log menus and their options (Continued)

Menu	Option	Description
	Copy View	Copies a view in the current console or to another new console.
	Save View As dashboard Viewlet	Saves a view as a dashboard viewlet for the Web pages or third-party Web Portal products; Business Dashboard must be installed.
	Delete View	Removes a view from the current console.
	Listen to Context	Configures a view for context sharing.
	Refresh	Redisplays the console.
Manager	Attach	Connects to a Manager.
	Detach	Disconnects from a Manager.
Configure	Groups	Creates groups or child groups of infrastructure elements. The VMware Smart Assurance Service Assurance Manager Configuration Guide includes information about creating groups.
	Global Manager Administration Console	Opens a Global Manager Administration Console for configuring Global Managers.
	Domain Manager Administration Console	Opens a Domain Manager Administration Console for managing underlying Domain Managers.
	Topology Builder	Opens a Topology Builder Console. The VMware Smart Assurance Business Impact Manager User Guide includes information about the Topology Builder Console.
Event	Companion UI	Opens the Notification Properties workspace in a browser for a selected notification. The workspace may contain one or more apps that provide detailed information about the notification. The VMware Smart Assurance SolutionPack Installation and Configuration Guide provides configuration information for the VMware Smart Assurance Companion UI.
	Properties	Displays notification properties for a selected notification.
	Acknowledge	Acknowledges a selected notification.
	Unacknowledge	Removes acknowledgement.
	Take Ownership	Assigns a username to a selected notification for problem resolution.
	Release Ownership	Removes a username.
	Add to Audit Log	Adds comment entries to notification audit log.
	Audit Log	Opens the audit log.
	Browse	Opens the Topology Browser view for the current Global Manager that contains the selected element in a secondary window.
	Browse Detail	Opens the Topology Browser view for the underlying Manager that contains the selected element in a secondary window.
	Containment	Displays an element's components.
	Show Map	Opens the Map Console in a secondary window.
	Mail	Opens the email tool for a selected notification.

Table 2-2. Notification Log menus and their options (Continued)

Menu	Option	Description
	Page	Opens the pager message tool for a selected notification.
Log	Select Columns	Controls which columns are displayed in the Notification Log view.
	Save log contents to file	Saves the contents of the Notification Log view locally as a text file.
	Sort Columns	Sorts columns in the Notification Log view.
	Filter	Specifies a filter for the Notification Log view.
	Log Properties	Changes the title of the Notification Log view and specifies continuous or scheduled display updates of notifications.
	Freeze Display	Stops the display from changing in the Notification Log view.
Help	About Global Console	Lists Global Console information: version, contact, and outsourcing information.

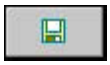
Shortcut menus are also available when you right-click on selected entities. Table 3 on page 26 summarizes the options and selection criteria.

Table 2-3. Notification Log shortcut menus

Selection criteria	Option	Shortcut menu options
Right-click on or near the view title	Same as Log menu options. For a Notification Log view launched from a summary, only the Select Columns option is available.	
Right-click a column heading	Hide Column	Hides a column from display.
	Insert Column	Inserts a column to the left of the selected column.
Right-click a notification	Same as Event menu options with the addition of maintenance tracking options, if enabled: Schedule Maintenance and Repair Time. Plus, the Server Tools and Client Tools options for tools if they are enabled. The VMware Smart Assurance Service Assurance Manager Configuration Guide includes information on configuring tools.	

Notification Log Console toolbar buttons

In the Notification Log Console, certain menu options are provided as toolbar buttons. They are summarized in Table 4 on page 27.

Button	Description
	Opens a local console.
	Saves an unsaved console on a local or remote host. Saves a saved console to a previously-specified destination.
	Displays the Select Context(s) To Listen To dialog box for configuring context sharing.

	Opens a browser for reporting. The VMware Smart Assurance Report Manager User Guide includes additional information.
	Displays the Notification Properties dialog box for a selected notification.
	Acknowledges an active, selected notification.
	Displays the Map Console for selected notification.

Layout of a Map Console

The Map Console is designed specifically for viewing maps. When you open the Map Console (see Figure 2 on page 29), it consists of two panels.

Left panel

In the left panel, you can select a Global Manager from the Manager menu to see maps for that manager. The menu lists attached Global Managers. Domain Managers are not listed in the menu.

At the bottom of the left panel are two tabs:

- The Topology tab displays a map tree that is a hierarchical representation of the attached Global Managers, classes of infrastructure elements, logical groups such as IP networks and VLANs, business services, software services, and the instances available for each class.
- The Groups tab displays user-defined groups of topological elements if the groups exist. (Your administrator can create groups. The VMware Smart Assurance Service Assurance Manager Configuration Guide includes information on groups.)

  Different types of maps are available for the instances in each tab.

Right panel

The right panel displays the map. After you select an instance from the expanded map tree, the map displays and the selected device is surrounded by a blue box. Alternatively, if you used the Show Map option for a selected notification, this panel shows a map containing your selection.

Map menus and shortcut menus summarizes menu options for the Map Console. Map Console toolbar buttons summarizes toolbar buttons specific to the Map Console.

The left arrowhead on the panel divider hides the map tree and enlarges the right panel for a larger display area. The right arrowhead on the panel divider unhides or enlarges the map tree.

Indicators, at the top of the right panel, show if coloring by root cause is enabled and the map's layout type. *"Adjusting the appearance of a map" on page 94* includes additional information.

A history field list box lists the current map (instance and map type) and other recently viewed maps.

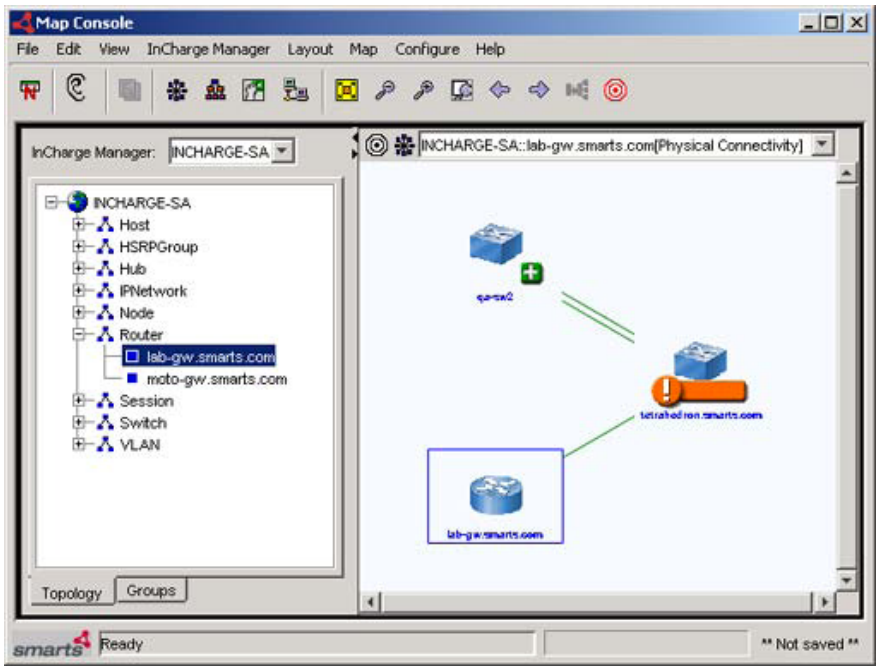
The map legend provides a list of map elements and color indicators. To view the legend, select **Map** > **Map Legend**.

You can customize individual maps with a map filter. The filter enables you to add and remove classes from a map.

Note You can customize the font and point size of the map icon text. The default map icon font is Helvetica. The default map icon font size is 12 point. The font and font size can be modified by changing the com.smarts.mapNodeText.font and the con.smarts.mapNodeText.fontsize properties. *"Adjusting Java properties" on page 151* provides detailed information.

Figure 2 on page 29 displays an example of a Physical Connectivity map.

Figure 2-2. Map Console



Map menus and shortcut menus

Table 5 on page 30 summarizes the menus that are available for the Map Console. Two menus, Layout and Map, are specific to the Map Console. The Configure menu is displayed depending on your user access control privileges.

Table 2-5. Map menus and their options

Menu	Option	Description
File	New	Opens a new console.
	Open	Opens an existing console, locally saved or remotely saved.
	Close	Closes an individual console.
	Save	Saves an unsaved console on a local or remote host. Saves a saved console to a previously specified destination.
	Save As	Saves a console on a local or remote host.

Table 2-5. Map menus and their options (Continued)

Menu	Option	Description
	Layout	Arranges multiple views in a console and changes console title.
	Exit	Ends the session and closes all consoles.
Edit	Find Instance	Searches for any topological element in any class including application services, service offerings, service subscribers, and systems.
	Find System	Searches for a system (infrastructure element).
View	Java Console	Displays console debugging information, including store exceptions, errors reading attributes, and stack traces.
	Message Log	Displays communications sent from a Manager to the console.
	Toolbar	Toggles the display of the toolbar buttons.
	Status	Toggles the display of the status bar.
	Add View	Inserts a view in the current console.
	Copy View	Copies a view in the current console or to another new console.
	Delete View	Removes a view from the current console.
	Listen to Context	Configures a view for context sharing.
	Refresh	Redisplays the console.
Manager	Attach	Connects to a Manager.
	Detach	Disconnects from a Manager.
Layout	Circular Layout	Displays circular layout of a map.
	Hierarchical Layout	Displays hierarchical layout of a map.
	Organize	Displays layout based on internal logic. **Note** For a Multiprotocol Label Switching (MPLS) VPN map.
	Orthogonal Layout	Displays orthogonal layout of a map.
	Manual Layout	Enables manual positioning of nodes in a map.
	Fit in Window	Fits the map to the size of the right panel.
Map	Save Map	Saves an individual map.
	Edit Map Filter	Specifies a filter for a map.
	Expand Map Element	Expands one or more individual nodes or elements.
	Increment Hops	Expands an entire map by one hop.
	Decrement Hops	Decreases an entire map by one hop.
	Map Legend	Displays a list of map icons and colors.
	Print Map	Prints a map.
	Overview	Opens the Overview window for magnification.
	Reset Map	Resets changes made to a map or returns to the saved map.
	Set Background	Specifies a user-defined background image for a map.

Table 2-5. Map menus and their options (Continued)

Menu	Option	Description
	Node Labels	For Network Protocol Manager (NPM) maps, enables the display of labels for routers.
	Align nodes to grid	Aligns nodes to the grid.
	Grid options	Displays map grid options.
Configure	Groups	Creates groups or child groups of infrastructure elements. The VMware Smart Assurance Service Assurance Manager Configuration Guide contains information about creating groups.
	Global Manager Administration Console	Opens a Global Manager Administration Console for configuring Global Managers.
	Domain Manager Administration Console	Opens a Domain Manager Administration Console for managing underlying Domain Managers.
	Topology Builder	Opens a Topology Builder Console. The VMware Smart Assurance Business Impact Manager User Guide and the *VMware Smart Assurance Application Services Manager Discovery Guide* contains information about the Topology Builder Console.
	Edit Map Icons	Assigns custom icons for a class or an instance.
Help	About Global Console	Lists Global Console information: version, contact, and outsourcing information.

Shortcut menus are also available when you right-click on selected entities. Table 6 on page 32 summarizes the options and selection criteria.

Table 2-6. Map shortcut menus

Selection criteria	Option	Description
Right-click an instance in the Topology tab	Available maps for display	Available maps depend upon the selected instance. **Note** *"Types of maps" on page 90* includes additional information.
	Browse	Opens the Topology Browser view for the current Global Manager that contains the selected element in a secondary window.
	Browse Detail	Opens the Topology Browser view for the underlying Manager that contains the selected element in a secondary window.
	Containment	Displays an element's components.
	Edit Map Icons	Assigns custom icons for a class or an instance.
	Server Tools	Displays a list of server tools if enabled.
	Client Tools	Displays a list of client tools if enabled.
Right-click an instance in the Groups tab	Available maps for display	Available maps depend upon the selected instance. **Note** *"Types of maps" on page 90* includes additional information.
Right-click in the background of a map	Circular Layout	Displays circular layout of a map.
	Manual Layout	Enables manual positioning of nodes in a map.

Table 2-6. Map shortcut menus (Continued)

Selection criteria	Option	Description
	Hierarchical Layout	Displays hierarchical layout of a map.
	Orthogonal Layout	Displays orthogonal layout of a map.
	Organize	For a Multiprotocol Label Switching (MPLS) VPN map, displays layout based on internal logic.
	Fit in Window	Fits the map to the size of the right panel.
	Increment Hops	Expands an entire map by one hop.
	Decrement Hops	Decreases an entire map by one hop.
	Reset Map	Resets changes made to a map or returns to the saved map.
	Edit Map Icons	Assigns custom icons for a class or an instance.
	Set Background	Specifies a user-defined background for maps.
	Align nodes to grid	Aligns nodes to the grid.
	Grid options	Displays map grid options.
Right-click a selected node in a map	Available maps for display	Available maps depend upon the selected instance. **Note** *"Types of maps" on page 90* includes additional information.
	Notification Properties	Displays notification properties.
	Browse	Opens the Topology Browser view for the current Global Manager that contains the selected element in a secondary window.
	Browse Detail	Opens the Topology Browser view for the underlying Manager that contains the selected element in a secondary window.
	Containment	Displays an element's components.
	Schedule Maintenance	Displays the Schedule Maintenance dialog box.
	Edit Map Icons	Assigns custom icons for a class or an instance.
	Expand Map Element	Expands one or more individual nodes or elements.
	Map Window	Opens another map in a secondary window.
	Server Tools	Displays a list of server tools if enabled.
	Client Tools	Displays a list of client tools if enabled.
Right-click a selected edge in a map	Notification Properties	Displays notification properties.
	Browse	Opens the Topology Browser view for the current Global Manager that contains the selected element in a secondary window.
	Browse Detail	Opens the Topology Browser view for the underlying Manager that contains the selected element in a secondary window.

Map Console toolbar buttons

In the Map Console, certain menu options are provided as toolbar buttons. They are summarized in Table 7 on page 34.

Button	Description
	Opens a Notification Log Console.
	Displays the Select Context(s) To Listen To dialog box for configuring context sharing.
	Opens a browser for reporting. The VMware Smart Assurance Report Manager User Guide includes additional information.
	Displays circular layout of a map. This is the default layout for all maps except for Business Services maps.
Button	Description
	Displays hierarchical layout of a map. This is the default layout for Business Services maps.
	Displays orthogonal layout of a map.
	Allows manual layout of a map, leaving nodes where you place them (important when you place nodes on a custom map background such as a geographic map).
	For Multiprotocol Label Switching (MPLS) VPN map, displays layout based on internal logic.
	Fits the map to the size of the right panel.
	Zoom out, shrink map.
	Zoom in, magnify map.
	Opens the Overview window.
	Shows previous map.
	Shows next map.
	Expands selected node or element. A plus sign next to a node indicates that the node or element can be expanded.
	Changes the color of map objects. Only objects experiencing root-cause events are colored.

Layout of a Topology Browser Console

The Topology Browser Console is designed specifically for viewing the topology of any Manager:

- For a Global Manager, the Topology Browser presents an abstracted topology.
- For a Domain Manager, the Topology Browser presents a complete topology.

  It also displays detailed topology if a selected topology element has an underlying topology source. It consists of one view, the Topology Browser view. Figure 3 on page 36 illustrates an example of a Topology Browser Console.

  In the left panel, you can select a Manager from the Manager menu to see the topology for that manager. You can expand each object in the topology tree and see its contents.

  If multiple Managers are attached, the console displays the Managers one at a time, classes, instances of each class, and their relationships. For each object you select, a corresponding property sheet with one or more tabs is displayed in the right panel:

- For a Manager, the Modules and Threads tabs provide information about models, programs, and process threads.
- For classes, the Description and Attributes tabs describe the class and its attributes.
- For elements (instances):
  - Attributes tab lists the attribute names, data types, values, and descriptions of the attributes.
  - Groups tab displays groups if the instance belongs to any groups.
  - Global Manager only, the Events tab displays notifications if they are generated.

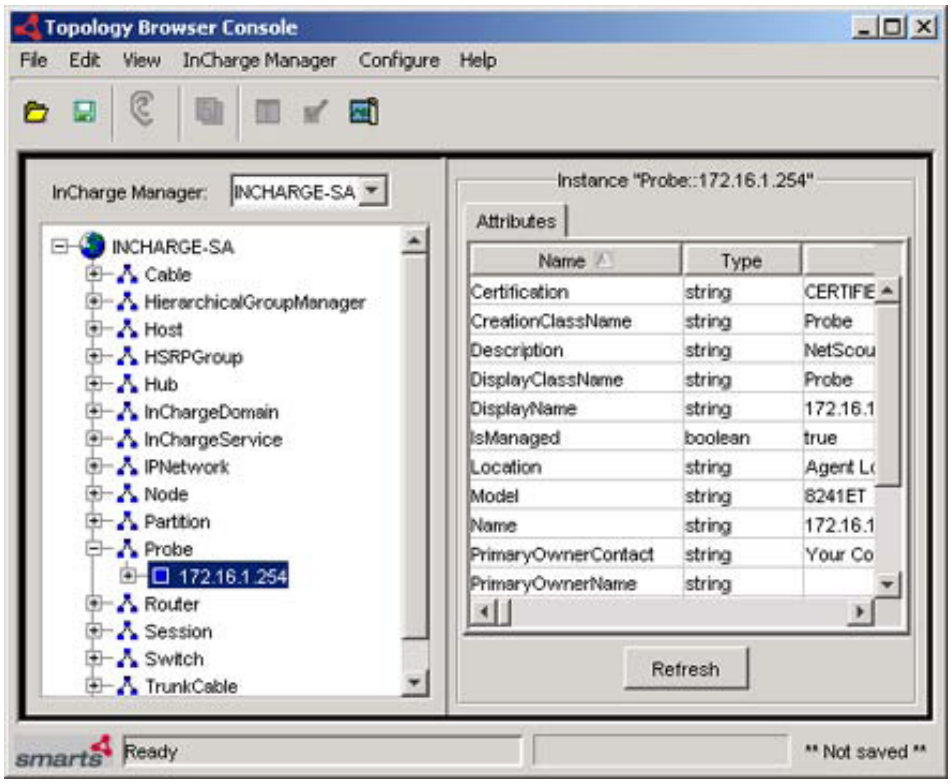
    In the Topology Browser Console, the menu options and toolbar buttons are the same as those in the Notification Log Console, except that the following do not exist for the Topology Browser Console. Table 2 on page 24 and Table 4 on page 27 provide information on Notification Log menus and their options and Notification Log Console toolbar buttons, respectively:

- Event and Log menus
- View menu options: Save as Viewlet and Listen to Context

  Topology Browser shortcut menus summarizes shortcut menu options.

  Figure 3 on page 36 illustrates a typical Topology Browser Console. In the left panel, the tree displays an instance of a probe, 172.16.1.254, and the right panel displays the Attributes tab for the probe.

Figure 2-3. Topology Browser Console



Topology Browser shortcut menus

Shortcut menus are also available when you right-click on selected entities. Table 8 on page 37 summarizes the options and selection criteria.

Table 2-8. Topology Browser shortcut menus

Selection criteria	Option	Description
Right-click in panel of the topology tree	Select	Specifies a filter for a topology tree.
	Refresh Tree	Refreshes the tree contents.
Right-click an instance in the topology tree	Make Root	Begins the tree with the selected instance as the root.
	Browse	Opens the Topology Browser view for the current Manager that contains the selected element in a secondary window.
	Browse Detail	Opens the Topology Browser view for the underlying Manager that contains the selected element in a secondary window.
	Containment	Displays an element's components.
	Show Map	Opens the Map Console in a secondary window.
	Schedule Maintenance	Displays the Schedule Maintenance dialog box.
	Server Tools	Displays a list of server tools if enabled.
	Client Tools	Displays a list of client tools if enabled.
Right-click the notification in the Events tab	Properties	Displays notification properties.

Table 2-8. Topology Browser shortcut menus (Continued)

Selection criteria	Option	Description
	Browse	Opens the Topology Browser view for the current Manager that contains the selected element in a secondary window.
	Show Map	Opens the Map Console in a secondary window.
	Server Tools	Displays a list of server tools if enabled.
	Client Tools	Displays a list of client tools if enabled.
Right-click in the Group tab	Browse	Opens the Topology Browser view for the current Manager that contains the selected element in a secondary window.
	Show Map	Opens the Map Console in a secondary window.

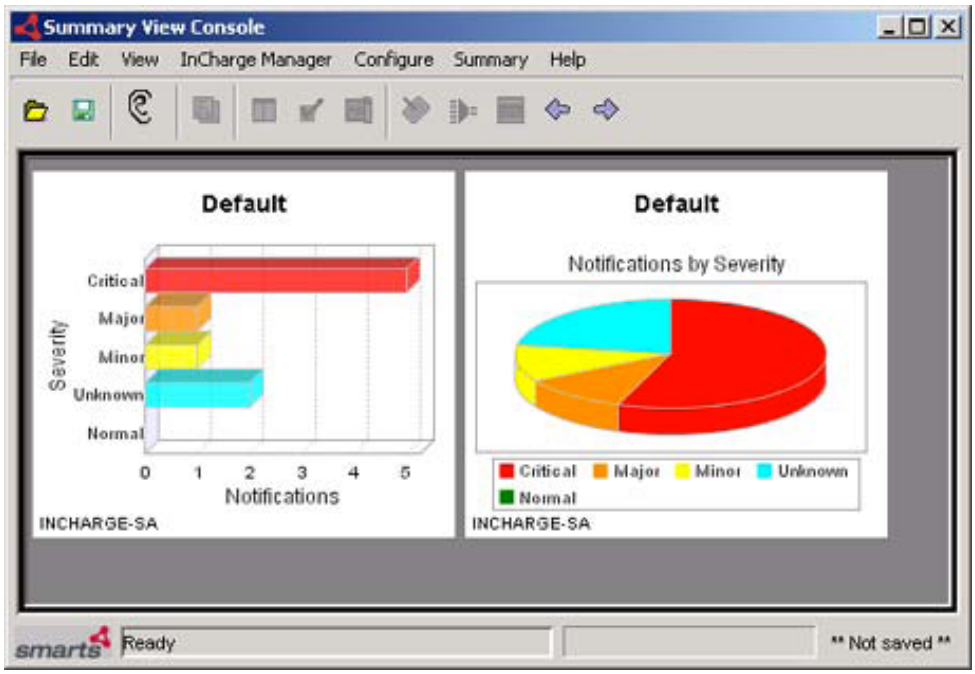
Layout of a Summary View Console

The Summary View Console is designed to present overviews or summaries of notifications. The console consists of one view, the Summary view. Each summary represents information in a horizontal bar chart or pie chart, organized by meaningful criteria. For example, a summary can organize notifications by severity. A Summary View Console can present summaries for one or more Global Managers. Figure 4 on page 38 illustrates an example of a Summary View Console.

You can customize a summary. For example, you can edit its parameters to change its contents or apply a filter. You can also display a Notification Log view or map for a selected summary in a secondary window. Chapter 7 Examining Summaries includes additional information.

In the Summary View Console, the menu options are the same as those in the Notification Log Console (see Table 2 on page 24), except that the Event and Log menus do not exist for the Summary View Console. One menu, Summary, is specific to the Summary View Console (see Table 9 on page 39). Shortcut menu options are summarized in Table 11 on page 40. Toolbar buttons are also summarized in Table 11 on page 40.

Figure 2-4. Summary View Console



Summary View menu and shortcut menus

One menu, Summary, is specific to the Summary View Console. Table 9 on page 39 provides additional information. Shortcut menu options are summarized in Table 10 on page 39.

Table 9 on page 39 summarizes the Summary menu.

Table 2-9. Summary View menus and their options

Menu	Option	Description
Summary	Edit Summary Parameters	Changes a summary's contents, its title, and its chart type (horizontal bar or pie chart), and specifies continuous or scheduled display updates of notifications, alarmed elements, and impacts.
	Filter	Specifies a filter for a selected summary.
	Show Notifications	Displays a Notification Log view for a selected summary in a secondary window.
	Move Summary Left	Moves a summary one cell to the left.
	Move Summary Right	Moves a summary one cell to the right.
	Add Summary	Adds a summary to the Summary view.
	Layout	Specifies the maximum number of summaries per row in a Summary view.
	Delete Summary	Deletes a selected summary from the Summary view.

Shortcut menus are also available when you right-click on selected entities. Table 10 on page 39 summarizes the options and selection criteria.

Table 2-10. Summary View shortcut menus

Selection criteria	Option	Description
Right-click on or near the summary title	Edit Summary Parameters	Changes a summary's contents, its title, and its chart type (horizontal bar or pie chart), and specifies continuous or scheduled display updates of notifications, alarmed elements and impacts.
	Filter	Specifies a filter for a selected summary.
	Show Notifications	Displays a Notification Log view for a selected summary in a secondary window.
	Show Map	Displays a map for a selected summary in a secondary window.
	Delete Summary	Deletes a selected summary from the Summary view.
Right-click in a view	Add Summary	Adds a summary to the Summary view.
	Layout	Specifies the maximum number of summaries per row in a Summary view.

Note Shortcut menus for a Notification Log view for a summary are described in Table 3 on page 26. A Notification Log view for a summary only supports the shortcut menu that results from right-clicking a notification.

Summary View Console toolbar buttons

In the Summary View Console, certain menu options are provided as toolbar buttons. They are summarized in Table 11 on page 40.

Button	Description
	Opens a local console.
	Saves an unsaved console on a local or remote host. Saves a saved console to a previously specified destination.
	Displays the Select Context(s) To Listen To dialog box for configuring context sharing.
	Opens a browser for reporting. The VMware Smart Assurance Report Manager User Guide includes additional information.
	Displays the Notification Properties dialog box for a selected notification.
	Acknowledges an active, selected notification.
	Displays the Map Console.
	Edits the parameters of a selected summary. Changes a summary's contents, its title, and its chart type, and specifies continuous or scheduled display updates of notifications.

	Specifies a filter for a selected summary.
	Displays a Notification Log view for a selected summary in a secondary window.
	Moves a selected summary one cell to the left.
	Moves a selected summary one cell to the right.

Layout of a Status Table Console

A Status Table Console provides a high-level overview of the status of the underlying elements that affect the operation of business entities such as business processes, customers, and lines of business.

Note The Status Table Console is available when the VMware Smart Assurance Business Dashboard is installed.

The Status Table Console displays a grid comprised of the following:

- Primary Class (y-axis) — Selection from a group of collection objects (ServiceOffering, ServiceSubscriber, or any group created by your administrator).
- Secondary Class (x-axis) — Selection from the group of corresponding instances of the Primary Class. Note that these options change as the Primary Class changes.

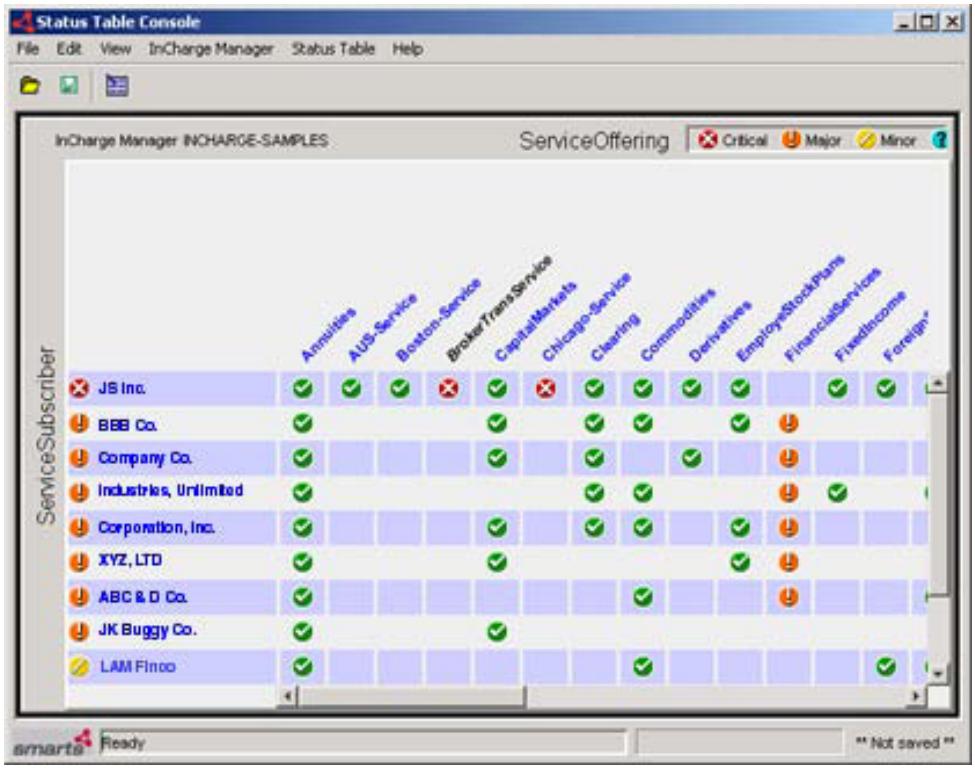
  For example, for the class, Customer, a Status Table view can show the instances and notification status of the various service offerings available to the Customer class.

  Your administrator can configure the groups (business entities) and Status Table views. *"Configuring a Status Table view" on page 113* includes information on configuring Status Table views.

  In the Status Table Console, the menu options are similar to those in the Notification Log Console (see Table 2 on page 24), except that the Event and Log menus do not exist for the Status Table Console. One menu, Status Table, is specific to the Status Table Console. Status Table menu and shortcut menus contains additional information.

  Figure 5 on page 42 illustrates instances of the Service Offerings (x-axis) provided by the Service Subscribers listed on the y-axis.

Figure 2-5. Status Table Console



Status Table menu and shortcut menus

One menu, Status Table, is specific to the Status Table Console. This menu includes one option, Configure Status Table. The Configure Status Table menu is displayed depending on your user access control privileges.

A shortcut menu is available when you right-click on the severity icon for an entity in the table, or on a class or instance name (on the x- and y-axis). Table 12 on page 43

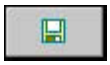
Table 2-12. Status Table shortcut menus

Selection criteria	Option	Description
Right-click the severity icon for an instance	Browse	Opens the Topology Browser view for the current Global Manager that contains the selected element in a secondary window.
	Containment	Displays an element's components.
	Notification Properties	Displays notification properties for that element.
	Show Map	Opens a map with that element as focus.
	Server Tools	Displays a submenu listing available server tools.
	Client Tools	Displays a submenu listing available client tools.

Table shortcut menu options.

Status Table Console toolbar buttons

In the Status Table Console, certain menu options are provided as toolbar buttons. They are summarized in Table 13 on page 43.

Button	Description
	Opens a local console.
	Saves an unsaved console on a local or remote host. Saves a saved console to a previously specified destination.
	Opens the Configure Status Table dialog box.
	Displays the Select Context(s) To Listen To dialog box for configuring context sharing.

Note Client and server tools can be invoked from an instance node displayed in the Status Table.

Watch4net

With the introduction of Watch4net 6.2, the user interface for Smarts products has been enhanced such that you have more choices for viewing the notifications and network activity monitored by the domain managers. You may choose from the following deployment scenarios:

1. Classic Service Assurance Manager console views — This option provides management of the Service Assurance Manager server similar to earlier releases of the product.
2. Service Assurance Manager consoles displayed inside a Watch4net outer frame — This option requires installation of the SAM Web Console and configuration of Service Assurance Manager, Watch4net, and the VMware Smart Assurance Console SolutionPack. This deployment option requires you to have separate logins for each product.
3. Service Assurance Manager with both Companion UI and Watch4net views — This option requires access to a virtual environment for installing Companion UI plus installation and configuration of SAM Web Console, Watch4net, and the VMware Smart Assurance Console SolutionPack. This deployment option provides single sign-on capability. Use of an LDAP server is recommended. For more information on enabling single sign-on for SAM, refer to the VMware Smart Assurance SolutionPack Installation and Configuration Guide.

   The VMware Smart Assurance Installation Guide for SAM, IP, ESM, MPLS, and NPM Managers provides information for installing Service Assurance Manager and Service Assurance Manager Console.

   The VMware Smart Assurance SolutionPack Installation and Configuration Guide provides information for installing Watch4net and Companion UI and for configuring all of the components as an integrated solution.

SAM views through Watch4net

You can access the following SAM views by logging into Watch4net:

- Notification Log Console
- Map Console
- Summary View Console
- Status Table Console
- Web Console

Starting a Session

3

This chapter includes the following topics:

- Overview
- Run MSA server
- Opening the Global Console
- Opening an additional Global Console
- Opening a Web Console
- Closing a console and ending a session
- Attaching to different or multiple Managers

Overview

A Global Console can be opened as an application in UNIX environment, as a Web Console in a Web Browser, or with Java Web Start.

When you open a console at the beginning of your session, you will need to log in. This involves specifying your VMware Smart Assurance username and password, broker information, and the Manager name for attachment.

If you initially attach to a Global Manager, one or more consoles display after you log in, depending upon your user profile or the default user profile. For example, if your user profile is configured for the Notification Log and Map Consoles, then two consoles will appear after you log in. If you attach to a Domain Manager, the Topology Browser Console appears first since Domain Managers do not maintain user profiles.

Run MSA server

You can run the MSA 2.0 server with the Tomcat server of SAM Console to use the MSA API.

1 Go to http://java.comand install JRE 7 on your machine and locate the top level directory of the JRE 7 installation.

2 Go to BASEDIR/local/conf and edit the *runcmd_env.sh*file to add the following lines:

```
SM_JAVA=<JAVA_HOME>/jre/bin;<JAVA_HOME>/jre/bin/client
SM_JAVAHOME=<JAVA_HOME>/jre
```

3 Copy the file, *msa20-dmt-9.1.1.0.143.war*from BASEDIR/tomcat/webapps/msa directory to BASEDIR/tomcat/webapps directory.

4 Rename *msa20-dmt-9.1.1.0.143.war* under BASEDIR/tomcat/webapps directory to *msa20-dmt.war*.

5 Start the Tomcat server by typing the following command:

```
#BASEDIR/bin/sm_tomcat start
```

6 Stop the Tomcat server by typing the following command:

```
#BASEDIR/bin/sm_tomcat stop
```

7 Go to BASEDIR/tomcat/webapps/msa20-dmt/WEB-INF/classes, and edit the *msa-sources.xml*file to add the SAM server and Broker information.

8 Start the Tomcat server by typing the following command:

```
#BASEDIR/bin/sm_tomcat start
```

9 Type the following address in your web browser:

`http://<host>:8080/msa20-dmt/msa/`

Starting the MSA 2.0 server and the Tomcat server will not start the SAM Console. Start the Global Console as described in Opening the Global Console.

Opening the Global Console

This section describes how to start a Global Console session.

Opening a Global Console in a UNIX environment

To start a new session and open a new console in a UNIX environment, use the sm_gui command:

```
% BASEDIR/smarts/bin/sm_gui
```

Logging on and attaching to a Manager

Before the console appears, you are prompted to log in and attach to a Manager:

1 For the **Broker**field, the broker hostname and port number values (that were provided during the installation process) appear. You may need to change them; check with your administrator for the correct values.

For example, in Managerdialog box, the broker hostname is smarts-broker and the port number is 426.

Figure 3-1. Manager dialog box

2 Click the **Manager**list box or the **Browse**button to display a list of active (running) Managers.

Note If the specified broker is a secure broker, when you click the **Manager**list box or the Browse button, you might be prompted to supply an VMware Smart Assuranceusername and password for the broker, depending upon the security configuration. Click **OK**and then select a Managerfrom the displayed list.

3 In the **User name**field, type your VMware Smart Assuranceusername.

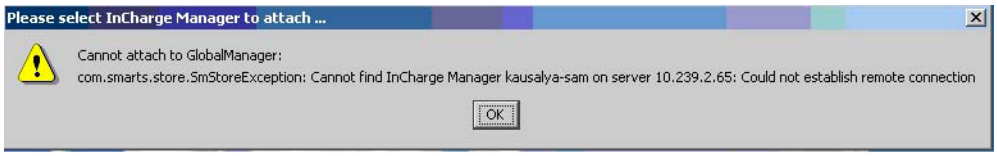
4 In the **Password**field, type your password.

5 Click **OK**.

After you click **OK**, the console appears. To close the dialog box and end the session, click **Cancel**.

Older versions of consoles will not connect to new versions of the Service Assurance Managerserver. When you attempt to connect to a new version of the Service Assurance Managerserver using an older version of the console, please select Incharge Manager to attach message appears, as illustrated in Please select InCharge Manager to attach error message. This message notifies you that the login failed and that you need to upgrade the Global Consoleto a compatible version of the Service Assurance Managerserver.

Figure 3-2. Please select InCharge Manager to attach error message



Note This message appears when the SM_REJECT_OLD_CONSOLES parameter is configured to true. The SM_REJECT_OLD_CONSOLES parameter is located in the runcmd_env.sh file. Setting the SM_REJECT_OLD_CONSOLES parameter to true prohibits Service Assurance Manager (SAM) 7.0 consoles and previous versions of the console from connecting to the SAM 7.2 server. When this parameter is set to true, SAM 7.1 consoles and subsequent versions of the console connect successfully to the SAM 7.2 or later servers.

IPv6 address environments

In environments where domains can have IPv6 addresses, domain names appear in the Manager dialog box with the text [IPv6] amended to the domain name. In IPv6 environments, two entries for each domain may exist; one entry for the domain's IPv6 address and another for the domain's IPv4 address. If either address does not exist, the connection for that address is not included in the Manager dialog box. You can only connect to domains displaying a status of Running. Where both IPv4 and IPv6 connections display a status of running, you can choose either of the connections. If you choose a connection that uses an IP version that is not available, a message appears notifying you that the selected protocol is not available.

Opening an additional Global Console

If you already started a session, you can open a new console or a saved console from your current console.

Note When opening a console saved on a server, you can select consoles saved in your user profile, saved in your user ID, and consoles saved globally.

Opening a new console

You can open a new console from any running console in a session. Select one of the following consoles:

- **File** > **New** > **Notification Log Console**
- **File** > **New** > **Map Console**
- **File** > **New** > **Topology Browser Console**
- **File** > **New** > **Summary View Console**

- **File** > **New** > **Status Table Console**

  This opens a console and attaches it to the same Managers as the running console. In the status bar, the text "Not saved" appears since it is an unsaved console. The new console is part of the same session as the running console.

  If the value “None” appears in the Manager menu, you need to select a Global Manager or a Manager from the menu, depending on the type of console. A new Summary View Console displays one default summary for each attached Global Manager.

Opening a locally saved console

To open a console saved on the host where the Global Console is running:

1 Select **File** > **Open** > **Open Local**.

2 or

3 Click the **Open Local** toolbar button. This displays the **Open Console** dialog box.

4 In the **Open Console** dialog box, select the console and click **Open**. This opens the console. The status bar displays the directory path and its filename.

Opening a remotely saved console

To open a console saved on the host where a Manager is running:

1 Select **File** > **Open** > **Open Remote** . This displays the **Open Remote Console** dialog box.

2 In the **Open Remote Console** dialog box, select the location of the saved console:

- Choose an Manager.
  - Select the console from the **Load from** list box.

3 Click **OK**. This opens the console. The status bar displays the Manager where it is saved, username, and the console name.

Opening a Web Console

You can open a Web Console, which provides Global Console functionality, in a web browser. When you open a Web Console, the console opens within the browser, not in a separate window.

The VMware Smart Assurance Installation Guide for SAM, IP, ESM, MPLS, and NPM Managersincludes browser requirement information.

Note If a message prompting you to install the latest J2SE Runtime Environment appears, click Yes (or the link) and follow the steps to install the software.

To open a Web Console:

1 Start your browser and point it at the following URL:

```
http://
                    <Tomcat
            _
            host>:8080/webconsole/InChargeApplet.html
```

2 In the **Java Security Warning**dialog box, click **Yes**or **Always**.

Yesor **Always**grants the Web Console full access to your machine. This allows the console to connect to any Managerfrom your machine, provided your login ID has authorization, and the console can save files locally.

Noallows the Web Console to run without full access to your machine.

3 Log in as described in Logging on and attaching to a Manager.

Using Java Web Start (optional)

To use Java Web Start with the Web Console, specify the following URL or select its icon if Java Web Start is installed.

To download and install Java Web Start:

1 Start your browser and point it at the following URL:

```
http://
                    <Tomcat
            _
            host>:8080/webconsole/globalConsoleCached.html
```

2 Optionally, select the option to download and install the Java Web Start product and the application.

A Java Web Start icon will install on your desktop or your Start menu. To start the Web Console after this, click this icon.

3 Log in as described in Logging on and attaching to a Manager.

If you do not have Java Web Start installed, you might be prompted to use an automatic installer or be directed to a Sun Microsystems web page, depending upon your operating system or browser.

Note The
VMware Smart Assurance Service Assurance Manager Dashboard Configuration Guideprovides detailed Web Console and Java Web Start information.

Closing a console and ending a session

If you have one or more consoles running, you can close specific consoles or end the entire session.

Closing a console

To close a console:

1 Select **File** > **Close**.

The Close command closes an individual console and the session continues. The Manager is not affected by this operation.

If the console is the last opened one, you are prompted to confirm whether to close it.

2 Click **Yes** to close it.

When you close the last console, you end the session.

Note When you close a web-browser window, the console closes. If that is the only open window for this session, the session closes. In the Web Console, you may not be prompted to confirm closing the last open console.

Ending a session

To close a session and exit a console:

1 Select **File** > **Exit**.

2 Click **Yes** to confirm. All consoles that are part of the session are closed and the session ends. The Manager is not affected by this operation.

Attaching to different or multiple Manager s

After you log in, if you need to use a different Manager, you can attach to another manager without exiting the console. If you detach from a Manager, you can attach to it again at any time.

If you need to access multiple Managers, you can attach to them, one at a time.

The attach procedure is similar to the logon procedure with some minor differences. For the attach procedure, you can use the same login username and re-enter your password or specify a different login ID. If you want to attach to a Manager using a different login ID, you do not have to start another Service Assurance session.

Detaching from a Manager

Detach from a Manager when you no longer want to interact with it. The detach operation does not stop the Manager.

To detach from an Manager:

1 Select **Manager** > **Detach**.

2 Click **Yes** to confirm the detach.

If multiple Managers are attached, the Detach Manager dialog box appears. Select the Manager you want to detach and click **OK** or click **Cancel**.

For the detached Manager, the value “None” appears in the Manager menu; other attached Managers remain listed and available. If you are using the Summary View Console, the summaries for the detached Global Manager turn gray.

Attaching to a Manager

To attach to an Manager:

1 Select **Manager** > **Attach**. This displays the **Attach Manager** dialog box.

2 The last attached Manager appears in the **Manager** menu. If you want to reattach, accept the value. Or, click the **Manager** list box or the **Browse** button to select another Manager.

Note If the specified broker is a secure broker, when you click the **Manager** list box or the Browse button, you might be prompted to supply your VMware Smart Assurance username and password, depending upon the security configuration. Click **OK** and then select a Manager from the displayed list.

3 Type your password in the **Password** field.

You do not need to change the values for the **Broker** field or the **Username** field.

If you want to specify a different login ID, you can change the values for the **User name** and **Password** fields.

4 Click **OK**.

To close the dialog box without attaching to a Manager, click **Cancel**.

The name of Manager is listed in the Manager list box. If you are using the Summary View Console, the Global Manager’s name is listed at the bottom of a summary after it is added to the view.

Examining Notifications

4

As you monitor your managed domain, you might need to examine notifications or investigate their causes. You may also need to refine the appearance of diagnostic results in your console.

This chapter includes the following topics:

- Accessing notifications
- About notifications
- Displaying notification properties
- Adjusting the contents of a Notification Log view
- Using filters

Accessing notifications

Once you start a session, events may appear as notifications in your Notification Log Console and may update summaries in your Summary View Console. Or, you can display topological information in a map or topology tree.

Once any console is opened, there are alternative methods for accessing notification information:

- Add a Notification Log view to any console. Chapter 10 Customizing Your Console includes information about views and adding views.
- Check the Events tab of the Topology Browser for any available notifications.
- Display notification properties by double-clicking an affected node
- (non-green color) in a map or on a selected notification.
- Use the **Open a Notification Log console** toolbar button to display a Notification Log view for a selected summary in a secondary window.

About notifications

When you are interpreting notifications, you should be aware of the different severity levels for notifications, and important attributes such as Source, IsRoot, and Impact that appear as columns in your console. This section also explains how to obtain more information about notification properties.

Notification information is displayed in:

- The Notification Log Console or view (including a view for a selected summary), when events occur.
- The Events tab of the Topology Browser for the object where the problem or event occurs.
- The Notification Properties view. *"Displaying notification properties" on page 62* contains additional information.
- Maps where notifications affect the state of icons. *"Adjusting the appearance of a map" on page 94* contains additional information.
- Status Table Console, for status of the underlying elements that affect the operation of business entities. Chapter 8 Examining Status Tables contains additional information.

Notification naming convention

Each notification has a unique name. A notification's name consists of the class name and instance name where the event occurred, and the event name. The notification naming convention is:

```
NOTIFICATION-ClassName_InstanceName_EventName
```

For example, the notification NOTIFICATION-Router_R1_Down identifies the event Down, which occurred in instance R1 of the Router class.

Unique notification names with this convention are displayed in the InternalEventHandle column. By default, the InternalEventHandle column is not displayed in the Notification Log Console, but you can add it by selecting **Log** > **Select Columns**. The Class, Name, and Event columns display a more readable form of this information.

The Notification Log Console will not list more than one notification with this name. If the event clears and occurs again before it is archived, the Count field is increased accordingly. *"The notification life cycle" on page 116* contains additional information about notification archival.

Notification severity

Service Assurance generates the following five levels of severity for notifications:

- Critical
- Major
- Minor
- Unknown

- Normal

  Each level has an associated severity icon, a unique color-coded icon. Notifications and console display summarizes severity and how severity appears in the Notification Log Console.

  Note The notification list configured by your administrator determines which notifications appear in your console. If the notification list does not include an event, notifications for the event will not appear in your console. If your Notification Log Console does not accurately reflect observed conditions, contact your administrator.

Table 4-1. Notifications and console display

Severity level	Description	Severity icon
Critical (red) Severity 1	A critical notification identifies a fatal condition. It requires immediate attention. When you receive multiple critical notifications, it means that Service Assurance has determined several independent fatal conditions.	
Major (orange) Severity 2	This represents a serious condition. It requires immediate attention.	
Minor (yellow) Severity 3	This represents an abnormal condition. Action is required but the condition is not serious.	
Unknown (blue) Severity 4	This represents elements and/or events that are in an unknown state because of network or management connectivity failures. It requires investigation.	
Normal (green) Severity 5	This represents a normal state and is usually displayed when an event is informational.	
Other indicators	Description	Color of item
Inactive	This indicates that the state cleared (changed to INACTIVE) and notification turns transparent.	White with black text
Selected	Clicking on a notification selects it.	Black border surrounding notification
Unmonitored or suspended	In the Notification Properties view, this indicates an event is unmonitored or suspended.	Gray text

When an event's state changes from ACTIVE (notified) to INACTIVE (cleared), the notification turns transparent (white). An inactive state means that the event is no longer occurring. If an event recurs, the Global Manager sends another notification, the state of the event returns to active, and the event counter is incremented.

Notification Log columns

In the Notification Log view, notification attributes appear as column headings. Columns in the Notification Log view lists the column names and their descriptions.

Table 4-2. Columns in the Notification Log view

Column / Attribute	Description
Acknowledged	Indicates the event has been acknowledged.
Active	Indicates if the event is active.
Category	Represents a broad categorization of the event (for example, Availability against Temperature). Valid values can be: Availability, Discovery, Error, Operational, Performance, PowerSupply, Resource, Temperature, and IMPACT.
Certainty	The certainty of this event.
Class	Display name for the event class.
ClassName	Class name of the managed element where the event occurred. One of three attributes that uniquely identifies a notification, not modifiable.
ClearOnAcknowledge	Indicates whether the event is automatically cleared from the Notification Log view when the event is acknowledged.
Count	The number of occurrences of this event starting from First Notify until Last Notify. For a momentary event (no duration), each occurrence increases the count value regardless of the current event state. For a durable event (a duration), the count value increments whenever the event reoccurs (cleared and renotified).
Element Class	The class name of the topology element associated with the event in the repository where this event resides. This may or may not have the same value as Class or may be empty.
Element Name	The name of the topology element associated with the event in the repository where this event resides. The string is empty if there is no related element. This may or may not have the same value as InstanceName.
Event	Display name for the event name.
Event State	Indicates the state of the event. Values can be ACTIVE (notified), SUSPENDED, WAS_ACTIVE, or INACTIVE (cleared).
Event Text	A longer textual description of the event.
Event Type	Indicates the nature of the event. Value can be either MOMENTARY or DURABLE. A momentary event has no duration. A durable event has a period during which the event is active and after which the event is no longer active.
EventName	Name of the event. One of three attributes that uniquely identifies a notification, not modifiable.
First Notify	First notification time. (This value is reset after an event is archived.) Events diagnosed by an underlying domain include timestamps that accurately reflect when the event occurred. The Global Manager uses this value from the event for the FirstNotifiedAt/LastNotifiedAt times when it creates the notification.
Impact	If Business Impact Manager is available, the sum of the weights for all affected elements. The default weight for each affected element is 1. Weights quantify the event impact on the infrastructure and business processes. A large numeric value indicates a large impact.
In Maintenance	Indicates whether this event occurred during a maintenance period.
InstanceName	Name of the instance where the problem was diagnosed. One of three attributes that uniquely identifies a notification, not modifiable.

Table 4-2. Columns in the Notification Log view (Continued)

Column / Attribute	Description
InternalEventHandle	A unique key (Name attribute) that identifies the notification.
IsProblem	Yes indicates if (and only if) at least one of the source event types is “PROBLEM”, and other source event types are either “PROBLEM” or “UNKNOWN”. No indicates that one or more of the source event types is “EVENT” or “AGGREGATE”. Since filtering on IsRoot can result in transient behavior when events are received from multiple underlying sources, it is recommended to filter on IsProblem instead.
IsRoot	Yes indicates that the current notification is the root event. No indicates that the current notification is not a root event and is caused by another event. It is often useful to filter on IsRoot to find those notifications that require immediate attention.
Last Change	Time of last event change.
Last Clear	Last clear time. "Never" indicates the notification has never cleared.
Last Notify	Last notification time.
Name	Display name for the event instance.
Owner	The username of the person responsible for handling the event.
Severity	A graphical severity icon (color-coded icon) that categorizes the severity level of the event from the notifier's point of view: 1 Critical indicates a fatal condition and that the scope is broad (for example, an outage to a critical resource). 2 Major indicates a serious condition. 3 Minor indicates an abnormal condition but not a serious one. 4 Unknown indicates that elements and/or events that are in an unknown state because of network or management connectivity failures. 5 Normal indicates a normal state and that an event is purely informational. Notification Log columns provides examples of the severity icons.
Source	Identifies the software component(s) that diagnosed the event, where the event originated (for example, a Global Manager, Domain Manager, SAM Adapter Platform, or SAM adapter). If there is more than one source, the attribute lists each separated by a comma. An intermediary Manager that relays an event is not listed as a source. For example, “Trap Processor” (SNMP Trap Adapter) is listed as the source of a notification and not the intermediary SAM Adapter Platform server.
SourceEventType	Indicates the type of event from an underlying source or sources. Value can be: PROBLEM, EVENT, AGGREGATE, or UNKNOWN. The default value is UNKNOWN. (Not to be confused with Event Type.)
Ticket ID	Trouble ticket ID.
UserDefined1 - 20	Twenty user-defined fields. Reserved for custom configuration.

In the Notification Properties view, the Caused By tab and Impact tab provide more information about the IsRoot and Impact attributes, respectively:

- The Caused By tab lists another event that caused a selected notification if the IsRoot value is No.

- The Impact tab lists all of the affected elements for the selected notification.

  Note The default weight can be changed by your administrator. Contact your administrator for acceptable values if you intend to specify this attribute in a notification filter.

  The VMware Smart Assurance Service Assurance Manager Configuration Guide contains complete information about attributes.

Displaying notification properties

To obtain detailed information about individual notifications, you can display notification properties information in either a dialog box, or a view, or in the Notification Properties workspace in the Companion UI. To do so, you can:

- Double-click a notification in the Notification Log view.
- Select a notification and click the **Show Notification Properties** toolbar button.
- Select **Event** > **Properties**.
- Right-click a selected notification and select the **Properties** option in the shortcut menu.
- Double-click a map icon if it is affected by active events and is no longer green. Or, right-click a selected map icon and select the **Notification Properties** option in the shortcut menu.
- Add a Notification Properties view using **View** > **Add View**.Select **Event > Companion UI**.
- Right-click a selected notification and select the **Companion UI** option in the shortcut menu.
- When you select the Companion UI for the first time, you are prompted for your CUI user name and password. VMware Smart Assurance recommends that you leave the browser open so you will not be prompted for your login credentials each time you select a notification. The Notification Properties workspace opens in a separate browser.

  Depending on the type of event and information available for display, the Notification Properties view displays up to seven types of tabs and up to five buttons. The Smarts CUI Notification Properties workspace displays as many apps as you wish. Online help in the Companion UI provides complete information about the available apps and features.

  In the Notification Properties view, the tabs are:

- General
- Audit Log
- Codebook
- Impact
- Details
- Caused By

- Aggregates

Note If a tab does not display but Fetch Details is enabled, click Fetch Details..

For the Notification Properties view, the buttons are:

- **Refresh** – Click this button to update values.
- **Browse** – Click this button to display the Topology Browser for the instance of the event.
- **Fetch Details** – Click this button to display information from underlying Managers.
- **Containment** – Click this button to display containment information.
- **Close** – Click this button to exit the dialog box.

The Notification Properties view is available regardless of the notification's state (active or inactive).

Depending upon the Global Manager's configuration, the detailed information is retrieved from the Global Manager and may include information from underlying Managers. One indication is whether or not the **Fetch Details** button appears in the view:

- If the **Fetch Details** button does not exist, the information is retrieved from the Global Manager and its underlying Managers.
- If the **Fetch Details** button exists, the information is retrieved from only the Global Manager.

To display information from the underlying Managers, click **Fetch Details**.

The Fetch Details button appears only if your administrator configured the FetchLocalNotificationProperties parameter to true. In this case, when you open the Notification Properties view, initially only the Global Manager information appears, and information from underlying servers is retrieved only when the Fetch Details button is pressed.

If the default setting (set to false) for the FetchLocalNotificationProperties parameter is used, the Notification Properties view initially displays all information, both the information from the Global Manager and information the Global Manger retrieves from the underlying servers. Set the FetchLocalNotificationProperties parameter to true in configurations where it may take the Global Manager a significant amount of time to retrieve the information from the underlying servers. This allows the initial notification properties information to appear quickly.

Note If you click the Fetch Details button and the information from the underlying servers takes a significant amount of time to appear, the Refresh button is disabled until the information from the underlying servers is displayed. During this time you can do other console operations.

General tab

The General tab lists the current values of the notification attributes.

Audit Log tab

The Audit Log tab displays the audit trail for the selected notification.

In the log, each row is an entry. To view the full entry, select the row and click **Show Full Entry**. To insert additional entries, click **Add to Audit Log**.

System actions such as archiving and user actions such as acknowledgement, ownership, and actions performed using server and automatic tools are recorded as entries in the audit log. Inserted comments cannot be edited or deleted and are archived as part of the audit log. Adding comments to a notification's audit log contains additional information.

To save a copy of the current contents of an audit log locally as a text file, click **Save table to file**. In the **Save table to file** dialog box, you can choose field delimiters, whether to include column headers, and a location for the file. Click **OK** to save the audit log. Saving audit log and containment information contains additional information.

Codebook tab

The Codebook tab only appears for a selected notification that represents a root-cause event from an underlying Manager. Such a notification, regardless of its severity, has a value of Yes for its IsRoot attribute. If a notification is notified as a root cause from multiple sources, one Codebook tab is displayed for each source. If the Codebook tab is not displayed but the Fetch Details button is enabled, click **Fetch Details** to display the tab.

The Codebook tab displays all symptomatic events used in the analysis of a root-cause event. The notification for an active symptomatic event indicates an abnormal condition in an underlying Manager. Notifications for symptomatic events are primarily displayed in this tab and might be displayed in the Notification Log Console. Their display in the console can be configured by your administrator.

In the Codebook tab, information is presented as a tree. Each tree node represents a class associated with a symptomatic event. You can expand the node to display its instance or instances.

The coloring of an active notification for a symptomatic event is determined by its underlying source or whether the event has already been imported into the Global Manager. Typically, the coloring is:

- Orange if the symptomatic event is active.
- White with black text if the event is inactive.
- Gray text if the event is unmonitored or suspended.

  In the Codebook tab, if you right-click the background area, a menu with two options appears:

- Show Active Only

  Click this menu option to display either active and inactive symptomatic event. A check mark appears when only active events are displayed.

- Collapsed

  Click this menu option to collapse the tree hierarchy. To expand the subtree, select Collapsed again. A check mark appears when the collapsed state is selected.

When the tree hierarchy is collapsed, you can right-click or double-click an instance in the tree to display the Notification Properties dialog box to display additional information.

The instance's tool tip provides information on the state of the symptomatic event. For example, use a tool tip to determine whether an event is unmonitored or suspended.

Impact tab

The Impact tab displays the objects affected by the selected notification. This tab appears for any type of event, including critical problems. Not all events affect other objects, so the Impact tab may not display.

The tab presents information in a table. To sort it, click one of the column headings. In the table, you can view the affected object's class and event.

For more information about an object, you can double-click its row to display the **Notification Properties** dialog box. Or, right-click it and select **Browse** to display a Topology Browser. You can also right-click a row and select **Show Map** to display it in a Map Console.

Caused By tab contains information on displaying the events which, in turn, cause the selected notification.

Note Client and server tools can be invoked from notifications displayed in the Notification Properties Impact tab.

Details tab

The Details tab displays the Manager (source), the object's attributes and their corresponding values relevant to the event. If a notification has multiple sources, one Detail tab appears for each source.

The tab presents information in one of three formats:

- A table of attributes and values
- A table of thresholds and their related attributes and values
- A sum or total value with a table of other attributes compared against a threshold value

  A gray line may appear in place of an attribute value in either the **Details** tab of the Notification Properties view or the **Attribute** tab in the Topology Browser.

  If a gray line appears in place of an attribute value, the value cannot be obtained by Service Assurance because:

- It is unnecessary for the underlying Manager to poll the attribute value of an external device at this time. To minimize network overhead, the Manager polls only those values it needs to analyze your devices.
- The underlying Manager has encountered an error while polling the attribute value of an external device. For example, the device might be down, or it might be up but inaccessible due to network problems. In this case, you receive a notification of the critical problem, but the value remains unavailable.

Caused By tab

The **Caused By** tab displays the events that are causing the selected notification. It also displays the objects where the events occur.

The tab presents information in a table. To sort it, click one of the column headings.

For more information about an object, you can double-click its row to display the **Notification Properties** dialog box. Or, right-click it and select **Browse** to display a Topology Browser. You can also right-click a row and select **Show Map** to display it in a Map Console.

Note Client and server tools can be invoked from notifications displayed in the Notification Properties Caused By tab.

Aggregates tab

The **Aggregates** tab appears if the selected notification is an aggregate. This tab enables you to examine the component notifications of an aggregate.

An aggregate is a notification that consists of one or more component notifications.

The tab displays the components of the aggregate, their class, object names, and the Manager (source). If a notification has multiple sources, one Aggregates tab appears for each source. To sort the table of information, click one of the column headings.

In the tab, a component notification is colored:

- According to its severity if it is active.
- White with black text if it is inactive.
- Gray text if it is unmonitored or suspended.

  For more information about a component notification, you can double-click it to display the **Notification Properties** dialog box. Or, right-click it and select **Browse** or Show Map to display a Topology Browser or a **Map Console**, respectively.

  Note Client and server tools can be invoked from notifications displayed in the Notification Properties Aggregates tab.

A map consideration

If you double-click a colored map node (or right-click a colored edge) and:

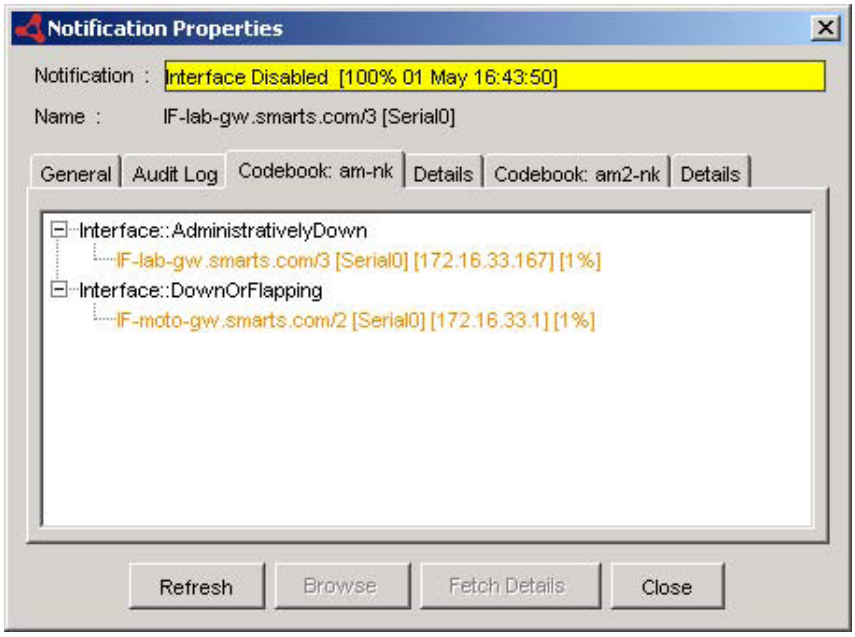
- One notification exists, the Notification Properties dialog box appears.
- Multiple notifications exist, the Active Notifications dialog box appears.

  In the Active Notifications dialog box, select the notification you want to see and click **Properties** to display the Notification Properties view or click **Close**.

Notification Properties tab examples

Codebook tab shows the active symptomatic events for an Interface Disabled notification for the interface IF-lab-gw.

Figure 4-1. Codebook tab

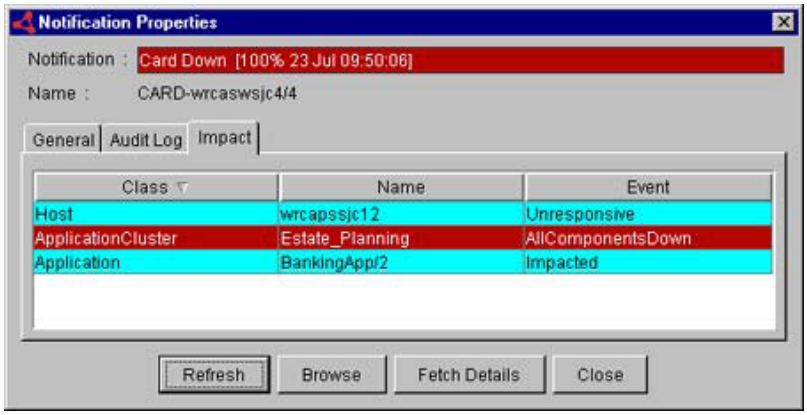


Audit Log tab shows an audit log for a Router Unresponsive notification for the router moto-gw.

Figure 4-2. Audit Log tab

Impact tab shows objects affected by a Card Down notification for the card wrcaswsjc4/4.

Figure 4-3. Impact tab



Adjusting the contents of a Notification Log view

To make it easier to examine the contents of your console(s), you can rearrange or adjust the contents. This section describes how to:

- Change the contents of a Notification Log view.
- Adjust the appearance of a Notification Log Console (for example, how to rearrange columns, sort by column, and control the display of columns).

  You can also adjust the contents by applying filters. *"Using filters" on page 72* contains additional information.

  Chapter 10 Customizing Your Console contains additional information on creating a customized console.

Changing the contents of a Notification Log view

In a single Notification Log view, you can display notifications from different Global Managers by changing the selection in the Manager menu.

Adjusting the appearance of a Notification Log Console or view

In your Notification Log Console or view, you can:

- Control which columns are displayed.
- Adjust the column width.
- Rearrange the order of columns.

Note In the following sections, some menu options are not available when you display a Notification Log view for a summary. In this case, the Notification Log view only supports the menu options that result from right-clicking a notification (see Adjusting the appearance of a Notification Log Console or view).

Notification Log columns contains descriptions of notification columns.

Controlling the column display

Certain columns may be extraneous for your work. To control which columns display:

1 Select **Log** > **Select Columns**. Or, right-click in the area near the view title and select **Select Columns** in the shortcut menu. The **Select Columns** dialog box displays.

2 To add or hide a column from your display, select or clear the appropriate checkbox.

3 Click **OK** to apply your changes.

   Optionally, you can right-click a column heading to hide it or to add another column next to it.

   - To hide a column, right-click its heading and select **Hide Column** in the shortcut menu.
   - To add a new column, right-click a column heading, select **Insert Column** in the shortcut menu, and select a new column in the submenu. The new column is inserted to the left of the selected column.

Adjusting the column width

You can adjust the column width, if necessary. To adjust the width of a column, select the divider between column titles and drag it with the mouse.

Rearranging the order of columns

To rearrange the order of columns, select a columntitle and drag it to the left or right.

To move a column, right-click a column heading, select **Insert**, and, in the submenu, select the column you want to move. The column is moved to the left of the selected column.

Sorting notifications

Two methods are available for sorting notifications:

- Click Sort
- Column Sort Order dialog box

  A Notification Log view, by default, is unsorted.

Click Sort method

To sort notifications by one column, click the column title you want to use for sorting. Note that a triangular marker appears in the column title:

- First click sorts the notifications in ascending order. The triangular marker points up.
- Second click sorts the notifications in descending order. The triangular marker points down.

- Third click disables the sort. The triangular marker is removed.

  Note If you disable the Click Sort functionality and there are other sort columns specified in the Column Sort Order dialog box, the specified sort columns determine the sort order.

  Columns that are moved and hidden from display may continue to affect the sort order.

Column Sort Order dialog box

To sort notifications by multiple columns:

1. Select **Log** > **Sort Columns**. Or, right-click in the area near the view title and select **Sort Columns** in the shortcut menu. The **Column Sort Order** dialog box displays.
2. Select the columns from the list boxes. Select **Descending** for a descending sort order; Ascending is the default.

   If you already used Click Sort, your choice appears in the dialog box. You can also specify a Click Sort column. If you clear the **Enabled** checkbox, Click Sort is disabled until the next time you click a column title or select the **Enabled** checkbox.

   The primary sort field is the **Click Sort** column or, if no Click Sort column is specified, the first field that you specify in the dialog box.

   If you need to reset your selections, click **Reset**.
3. Click **OK** to apply your changes.

   Note Except for the Click Sort selection, sorting, as determined by the selected columns in the Column Sort Order dialog box, is retained if you save a console.

Updating and freezing notifications

You can:

- Control whether the display of notifications is updated continuously or at scheduled interval.
- Freeze the notifications and prevent the display from updating.

Specifying display updates for notifications

Notifications are constantly being updated in your console by default. If you want to control how often notifications are updated, you can specify a time interval for scheduled updates.

You should consider the following before you specify a time interval:

- You should balance the update period between timely updates and the processing resources required to continually update the Notification Log Console. Check with your system administrator about an appropriate setting.

- Simultaneous displays of notifications might be inconsistent. If you specify a time interval for scheduled updates, users' actions, including your own, that occur during the interval are not updated in the display until after the interval. For example, you might acknowledge a notification that another user has already acknowledged. If this is a concern, use the time interval feature (the Update Every field) sparingly.

  To specify an interval for scheduled updates:

  a Select **Log** > **Log Properties** . Or, right-click in the area near the view title and select **Log Properties** in the shortcut menu. The **Log Properties** dialog box displays.

  b Clear the **Update Continuously** checkbox and specify the time in the **Update Every** field.

  c Click **OK .**

Freezing your display

To stop notifications from changing in the display, select **Log** > **Freeze Display**. Or, right-click in the area near the view title and select **Freeze Display** in the shortcut menu. In the left corner of the view, a box icon appears.

To unfreeze the display, select **Log** > **Freeze Display** again or click the box icon. The box icon in the left corner is removed.

Using filters

Filters enable you to control the contents of your console, view, or individual summaries. You apply a filter to notification attributes, any class, or instance, or both. For example, you may want to monitor only critical notifications with high impact on your business operations. There is one filter per view or summary. Filter criteria are saved if you save your consoles.

This section describes how to filter notifications with the Filter Builder dialog box. Filtering summaries includes information on applying a topological filter to a summary using the Filter Builder.

Filtering topology contains additional information about filtering a topology tree. *â€œFiltering mapsâ€ on page 99* includes information about filtering class instances in a map.

Filtering notifications

You can apply a filter to your Notification Log view. The filter can consist of one or more criteria. Only notifications that match all of your criteria are displayed. Filter criteria are saved if you save your console.

Use one of the following methods to open the Filter Builder dialog box:

- Click a Notification Log view and select **Log** > **Filter**.
- Right-click in the title area of the view and select **Filter** in the shortcut menu.

Layout of the Filter Builder

Initially, the Filter Builder dialog box opens with a blank Sheet1 tab. At the top, the Edit menu enables you to add, copy, or delete a Sheet tab.

On the left, the green plus sign button enables you to add one filter criterion at a time. Menus for each filter criterion enable you to select a notification attribute and one of the following conditions, if applicable:

- A match condition such as a specific value or expression. You can also specify wildcard characters in a match condition. Values are case-sensitive.
- The *is child of* condition (the IsA filter option) for notification attributes that have a class name for their value. IsA (“is child class of”) filter option includes additional information.

  If you want to treat a wildcard character as a text character, insert a backslash (\) before the wildcard character. For example, to filter on all event names that include a bracket, specify “*\]*”. (Do not include the quotation marks in the expression.)

  The **Helper** button is displayed depending on the selected notification attribute. This button:

- Provides a list of acceptable values.
- Prompts you for a range of values.
- Enables you to define an expression.

  If you add a wildcard character to an expression, the **Helper** button is disabled.

  The red X button deletes a specific filter criterion.

  At the bottom of the dialog box are the following buttons: OK, Cancel, and Refresh. To apply your filter and exit the dialog box, click OK. Click Cancel to exit without applying your changes. Refresh resets the Filter Builder dialog box to its original or previously applied filter criteria.

  Notification Log columns includes descriptions of notification attributes. Chapter 12 Wildcard Patterns includes a list of wildcards.

Pattern matching

When you create a filter, you can specify as many attribute-value pairs as you want. Each pair is a filter criterion. There is one filter per view. See Pattern matching for an example.

To pass a filter, notifications must satisfy all conditions in at least one Sheet tab:

- In a Sheet tab, criteria are related to one another with a logical operator AND. To satisfy a given tab, notifications must satisfy all conditions specified in the tab.
- Individual Sheet tabs are related to one another with a logical operator OR. Notifications must satisfy the conditions in at least one tab.

IsA (“is child class of”) filter option

The IsA filter option, displayed as is child of, only appears for notification attributes that have a class name for their value, including: Class, ClassName, and ElementClass.

To create an IsA filter for one of these notification attributes, select the class and the is child of option from the menus. To apply your filter and exit the dialog box, click **OK**.

The Notification Log Console then displays only the notifications for instances of the specified class and all of its subclasses.

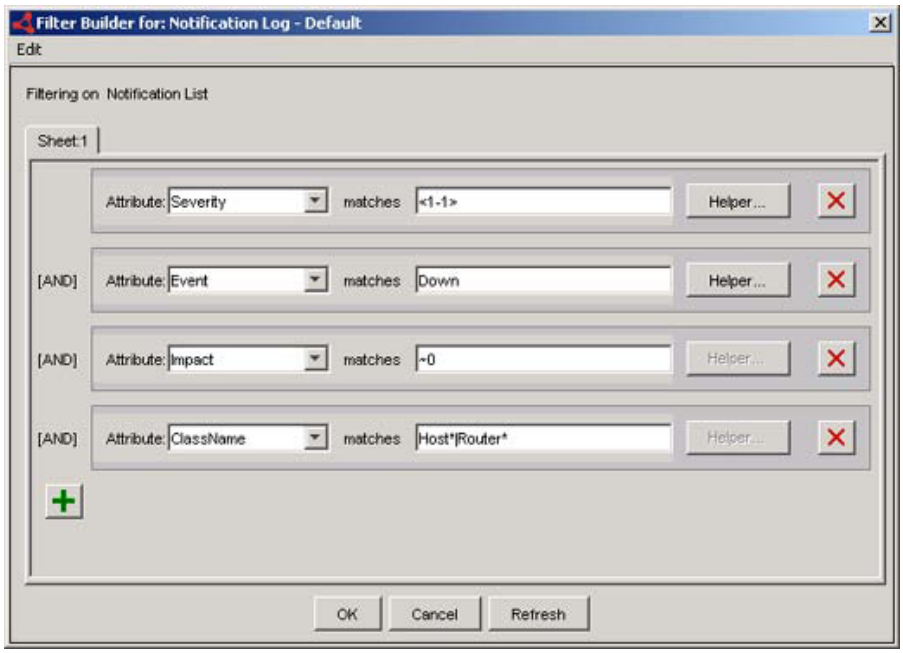
Note Only a single class name, without any wildcard characters of any kind, may be specified for an IsA filter.

Example of a filter

To display only critical notifications for Down events for a router or a host that impact your business operations, specify:

- A value of 1 for Severity, Down for Event
- A value of "~0" (not zero) for Impact, and any router or host

Figure 4-4. Filter Builder dialog box



Examining Topology

5

Service Assurance abstracts topological information from Managers and third-party applications. As you monitor your managed domain, you might need to examine your topology. The Topology Browser Console displays the topology of any attached Manager.

This chapter includes the following topics:

- Accessing topology
- Available topological information and its representation
- Topology Browser Console or view
- Finding an instance or device
- Using the Containment dialog box

Accessing topology

This section describes alternative methods for accessing topological information.

Once any console is opened, there are alternative methods for accessing topological information:

- Add a Topology Browser view to any existing console. Chapter 10 Customizing Your Console includes information about views and adding views.

  Note The Topology Browser is not available as a dashboard viewlet. However, topology can be examined in the Business Dashboard, for example, by right-clicking a notification or map node, and selecting Browse or Browse Detail, or by clicking the Browse button in a Notification Properties or Containment view. These actions open an additional topology browsing window.

- Browse opens the Topology Browser view in a secondary window to access topological information. Browse is available as a button in most secondary window and dialog boxes or as an Event option in the menu for selected notifications. For example, the Browse button appears in the Notification Properties dialog box and the Find Instance dialog box. (The button is activated when you select a row in the table.)
- The **Browse Detail** option under **Event** menu opens the Topology Browser view with topology from an underlying Manager in a secondary window.
- The Containment dialog box displays information and components for a selected element. *"Using the Containment dialog box" on page 81* includes additional information.

Available topological information and its representation

For most situations, the Topology Browser Console and Map Console provide the most complete representations of your topology.

There are different kinds of topological information. For example:

- Devices, logical groups such as IP networks and VLANs, and other infrastructure elements (such as network connections) that compose the domains managed by underlying Managers.
- User-defined groups of elements (configured by your administrator).
- Business elements such as application services, service offerings (such as Web hosting contracts), and service subscribers (such as customers, business units, or corporations). Service information and service classes may not be available for your site.

  Topology is represented in a tree format as in the map tree and the Topology Browser Console or by map icons in a map.

  Chapter 6 Examining Maps includes information about the Map Console, including how maps represent topological information and map color-coding.

Topology Browser Console or view

The Topology Browser (console, view, or secondary window) presents the topology of any Manager as a topology tree. Operators can view the topology of any attached Manager by selecting it from the Manager list box.

Displaying topology

To display an expanded topology tree in the left panel, you need to select a Manager from the Manager menu above the left panel.

Note A plus (+) sign indicates unexpanded objects. (On some systems, an open circle appears instead of a plus sign.)

If you already used the Browse option, the Manager icon is already expanded beginning with the class of your selection.

To navigate the topology tree:

1. Click the plus sign next to a class to view its elements (instances).
2. Click an element in the topology tree to display tabs of information in the right panel.
3. Click the plus sign next to an element to display its relationships.
4. Click the plus sign next to a relationship to display classes of related elements.

5 Click the plus sign next to a related class to display the related instances.

To refresh the contents of a topology tree, right-click in the background area and select **Refresh Tree** from the shortcut menu. Then, expand the tree.

For each object you select, a corresponding property sheet with one or more tabs is also displayed:

- For an Manager, the Modules and Threads tabs provide information about models, programs, and process threads. For a Domain Manager, the Correlation tab also displays and provides correlation information such as the correlation interval.
- For classes, the Description and Attributes tabs describe the class and its attributes.
- For elements (instances):
  - Attributes tab lists the attribute names, data types, values, and descriptions of the attributes.
  - Groups tab displays groups if the instances belong to any groups.
  - (Global Manager only) The Events tab displays notifications if they are generated. The Events tab does not display for a selected element of a Domain Manager.

Note If your user ID has the required authorization, for elements of a selected Domain Manager, you can modify attribute values. Double-click in the Value column, modify the value, and select Apply.

In the Topology Browser, an individual object with a plus (+) sign does not open or expand if a class exceeds 1,000 instances. Instead, a node displays, reporting that there are more than 1,000 instances. This limit can be changed by specifying the com.smarts.maxTopoInstances property during console startup. Chapter 10 Customizing Your Console provides detailed information on tailoring console properties.

Select **Edit** > **Find Instances** to find an individual instance and display related topology. (*"Finding an instance or device" on page 80* includes additional information.)

Also, the tool tip displays the correct number of instances. To activate the tool tip, hold the cursor over the object you wish to expand.

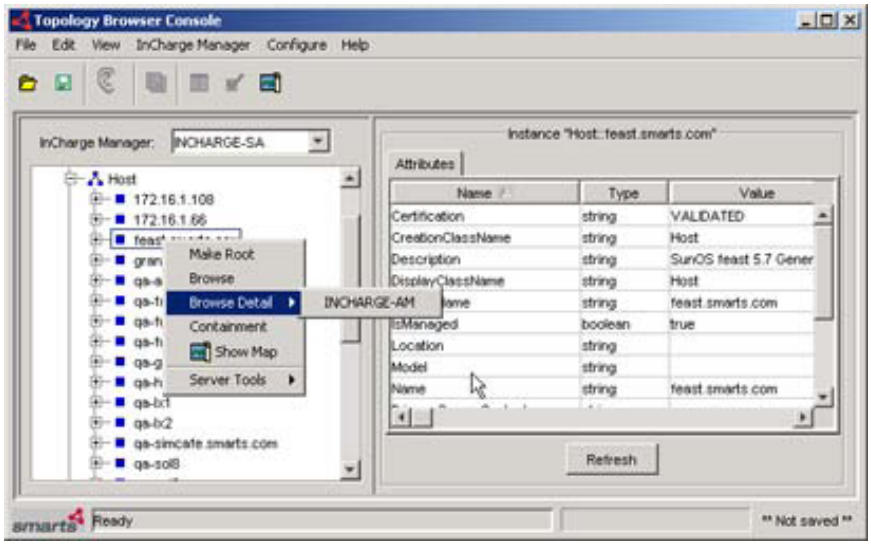
Browse Detail

The **Browse Detail** menu option is available:

- In the shortcut menu of the Topology Browser Console. Right-click a selected element in the tree and select **Browse Detail** in the menu.
- In the **Event** menu or the shortcut menu of the Notification Log Console. Right-click a selected notification and select **Browse Detail** in the menu.
- In a map. Right-click a node or an edge and select **Browse Detail** in the shortcut menu.

  Browse Detail provides a submenu that lists all of the underlying Managers that contain the selected element in their topology. You can select one of the underlying sources and display it in a Topology Browser view. Browse Detail example shows an example.

Figure 5-1. Browse Detail example



If the underlying Manager is not attached to the console, the console establishes a connection automatically with your login ID. If this is not possible, you might be prompted to supply another VMware Smart Assurance username and password.

If the selected element does not have any underlying sources, Browse Detail is disabled. Also, Browse Detail is not available for notifications generated by non-VMware Smart Assurance sources such as third-party adapters.

For hierarchical Service Assurance deployments, you can select Browse Detail as many times as necessary to navigate to the desired Manager.

Filtering topology

The topology filter enables you to control which classes and specific instances appear in the Topology Browser. You can specify a filter for each attached Manager and create a general filter for attached Managers that are not assigned filters. Filter criteria are saved if you save your consoles.

To specify filtering criteria:

1 Right-click in the topology tree panel.

2 In the shortcut menu, select **Select** to display the **Select tree content** dialog box.

3 In the **Select tree content** dialog box, you can:

- Select **All attached domains** to apply the filter to all attached Managers.
  - Select **Current domain** to apply the filter to the selected Manager.
  - Display all the classes including classes without instances. Select the **Show classes with no instances** checkbox.
  - Display one or more specific classes. Select the class. To select multiple classes, press the **Ctrl** key while making your selections.
  - If you select classes that have instances, you can also select specific instances.

4 To make your changes take effect, you must click **OK**.

To undo filter changes:

5 Display the **Select tree content** dialog box.

6 Clear the **Include only selected classes** checkbox.

7 Click **OK**.

Note To make additional changes, right-click and choose **Select** again. When the tree is expanded, you can select and right-click an instance and select the Make Root menu option. This will refresh the tree to list the selected instance as root. To return the display to the entire tree, right-click in the tree's background and choose **Select** again.

Finding an instance or device

If you need to locate an element by name, class, or IP address, use one of the following search tools. For example, if the class exceeds 1,000 elements and the Topology Browser does not expand, you can select the class in the Find Instance search tool to list all of its instances. After you receive search results, you can open the Topology Browser for topological information about the element, examine components of the element with the Containment dialog box, or display a map of it using Show Map.

In the consoles, the **Edit** menu lists the options, Find Instance and Find System:

- Use Find Instance to locate any topological element including application services, service offerings, service subscribers, and systems.
- Use Find System to locate systems or devices like routers and switches.

Finding an instance

To search for an instance:

1 Select **Edit** > **Find Instance** in your console. The **Find Instance** dialog box displays.

2 Fill in the fields, as described below. The fields are:

- **Manager** lists the Managers to search. Select one.
  - **Classes** is a list of classes to search. You must select one or more classes. (To select multiple classes, press the **Ctrl** or **Shift** key while making your selections.)
  - **Instance name** is the instance you want to find. You can specify a complete name, a partial name with wildcard characters, or the asterisk (*) wildcard if the name is unknown and you wish to search for all instances. Chapter 12 Wildcard Patterns includes a list of wildcards.

3 Click **Find** to start the search. The results display in a table.

The Find Instance dialog box limits the number of "matches" that display. If more than the limit number of matches is returned, a message displays asking you to refine your search.

The maximum number of instances that can display defaults to 1000 unless you configure the -Dcom.smarts.maxTopoInstances parameter to display more than 1000. The -Dcom.smarts.maxTopoInstances parameter limits the number of instances that are displayed in a topology tree. A new parameter, -Dcom.smarts.maxFindInstances, when configured, can override the -Dcom.smarts.maxTopoInstances parameter, for example, you can configure the value of the maxTopoInstances parameter to be a value of 3000 and the value for the maxFindInstances parameter to be a value of 500.

Note The value for the FindInstances parameter is not the number of instances searched, but the number of matches to be displayed. If the maxTopoInstances parameter is configured with a value of 100, the FindInstances parameter can still return matches for a class with 150,000 instances, provided there are less than 100 "matches" for the search string among the 150,000 instances.

Finding a system

To search for a system:

1 Select **Edit** > **Find System** in your console. The **Find System** dialog box displays.

2 Fill in the fields, as described below. The fields are:

- **Manager** lists the Managers to search. Select one.
  - **System name or IP Address** to find lists the device or IP address you want to find. Specify the device name (for example, moto-gw), a complete name (for example, moto-gw.smarts.com), or an IP address.

    Note Wildcard characters are not permitted.

3 Click **Find** to start the search.

If the server takes a significant amount of time searching for the specified system, the **Find** button is disabled until the server returns the search results. During this time you can perform additional console operations.

Search results

After the search results display in the table, you can sort them by clicking one of the column headings. You can also select one of the table rows and click one of the buttons located at the bottom of the dialog box. The available buttons are:

- **Browse** – Click this button to display the Topology Browser for the instance.
- **Containment** – Click this button to display a Containment dialog box of the instance.
- **Show Map** – Click this button to display the instance in the Map Console.
- **Close** – Click this button to exit the dialog box.

Using the Containment dialog box

The Containment dialog box displays information about an element's containment in tabular format. It provides information and components for a selected element. For example, for a selected port or interface, the Network Adapters tab displays its status, mode, current utilization, and the name of a peer network adapter.

Note Containment is not available for user-defined groups and services.

Several methods exist to display a Containment dialog box. For example, you can display containment information in either a dialog box or a view. To do so, you can:

- From the map tree, select an instance in the map tree, right-click and select **Containment** in the shortcut menu.
- In a map, right-click a node and select **Containment** in the shortcut menu. For a normal (status color green) node, double-click it to display the dialog box.
- From **Find Instance** or **Find System** dialog boxes, click **Containment**.
- In the **Event** menu or the shortcut menu, right-click a selected notification and select **Containment** in the menu.
- In the shortcut menu of the **Topology Browser Console**, right-click a selected element in the tree and select **Containment** in the menu.
- Add a Containment view using **View** > **Add View**. This view is context-sensitive, and can show containment information for the currently selected element in a different view in the same console, for example, if you select a notification in a Notification View in the same console.

  Note If the server takes a significant amount of time to respond to a containment request, the Containment window displays the Getting data from ... message until the server returns the data. During this time, you can perform additional console operations.

  In the Containment dialog box, information is organized using tabs. Each tab consists of a table. Depending upon the type of element and the type of analysis being performed by the underlying domain, different information is available.

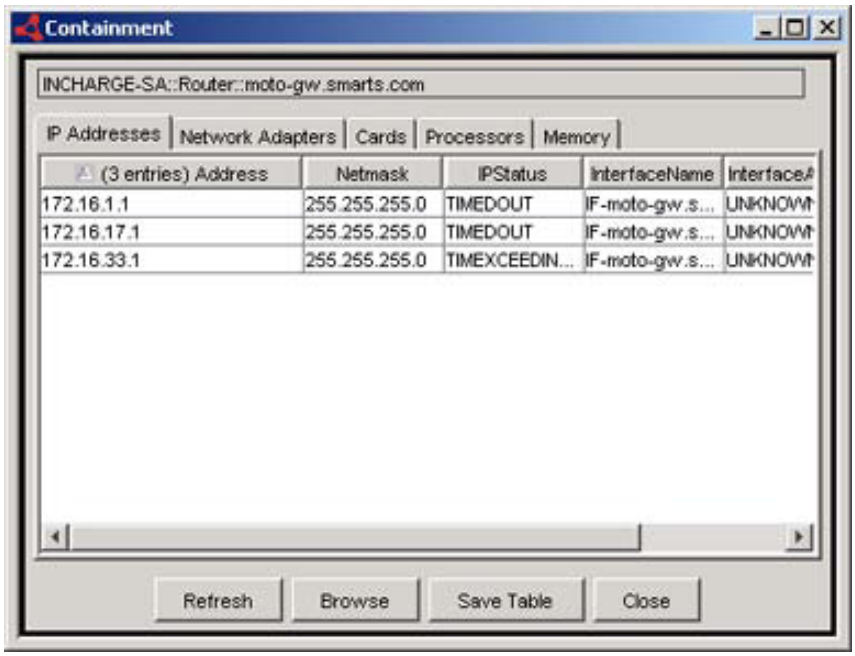
  For example, if VMware Smart Assurance IP Performance Manager is enabled on the underlying Domain Manager, then tabs for memory, processor, and environment display. If IP Performance Manager is not enabled, the tabs do not display or specific columns such as CurrentUtilization appear blank.

  The following buttons are available: Refresh, Browse, Save Table, and Close. The **Save Table** button saves the contents of a selected tab locally as a text file. (Saving audit log and containment information includes additional information.)

Containment dialog box example

Containment dialog box shows an example of a Containment dialog box for router moto-gw.

Figure 5-2. Containment dialog box



Examining Maps

6

A map provides a graphical representation of your topology and, by default, is updated continuously. As you monitor your managed domain, you might need to examine the elements of your maps and investigate the active events that affect them.

This chapter includes the following topics:

- Accessing maps
- Available topological information and its representation
- Representing notifications in maps
- Types of maps
- Adjusting the appearance of a map
- Customizing map backgrounds
- Viewing large maps: Overview window
- Filtering maps

Accessing maps

This section describes alternative methods for accessing individual maps and how to navigate among maps.

In addition to the different methods for opening available consoles (Chapter 3 Starting a Session), you can access a map using the **Show Map** option from any existing console. Show Map functionality opens the Map Console and displays the default map for the selected element. Show Map is available as a button in some secondary window and dialog boxes or as a menu option for selected notifications. For example:

- The **Show Map** button appears in the **Find Instance** and **Find System** dialog boxes. (The button is activated when you select a row in the table.)
- The Show Map option appears in the **Event** menu or the shortcut menu if you right-click on a selected notification.

- Use the **Show Map** button on the toolbar to display a default type of map for a selected summary. Show Map is enabled if a topological filter is specified for the summary. Filtering summaries contains additional information.

  Note If the Map Console is open, these options display the selected map in the currently open Map Console. A second Map Console does not open.

Opening a map

When you open a Map Console, you need to select a Global Manager from the **Manager** menu to display an expanded map tree in the **Topology** tab of the left panel. In a tree, a plus (+) sign indicates that the object or class can be expanded. (On some systems, an open circle appears instead of a plus sign.)

The Groups tab in the left panel displays a tree of user-defined groups for topological elements if groups exist.

Different types of maps are available for the instances in each tab.

If relevant topological information is not available for a selected instance, a message appears, stating that a map is not available.

To open a map in either tab:

1. Select a Global Manager from the **Manager** menu to display an expanded map tree in the **Topology** tab.

   Or, click the plus sign next to a group in the **Groups** tab:

   - For a class in the **Topology** tab, you can view its elements (instances).
     - For a group in the **Groups** tab, you can view its subgroups.

2. For the default type of map, you can click an instance in the map tree. Or, right-click an instance and select the type of map you want to display from the shortcut menu. The map appears in the right panel.

   Also, you can right-click an icon in the existing map and select another type of map from the shortcut menu.

   Note If a saved map of a given map type exists for the selected element, it is displayed. Saving a map includes additional information.

   To display more than one map concurrently, right-click a node in an existing map. Then, select **Map Window** from the shortcut menu. Select a map type in the submenu. A secondary window displays the additional map.

Navigating among maps

To navigate between multiple maps, the Map Console provides several navigation methods:

- The map tree — Select an element in the map tree to display the default type of map. Or, you can select an element in the tree, right-click, and select another type of map from the shortcut menu.

- A node in a map — Right-click a node in an existing map and select another map type from the submenu.
- A history field list box — Lists the current map (instance and map type) and other recently viewed maps. To re-display a map, select it from the history field list box located in the top border of the Map Console.
- Previous and Next toolbar buttons — Enables you to move quickly between maps.
- Multiple window of maps — Opens additional window to concurrently display maps of your selected node. To do so, right-click a selected node in a map, select Map Window, and choose a map type.

Available topological information and its representation

The Map Console is designed especially to display information about a managed topology using a variety of map types. For example, the VLAN Connectivity map reveals the connections to a VLAN and the VLAN Membership map reveals the members of a VLAN.

You can broaden the scope of the map by expanding nodes and incrementing map hops to reveal additional relationships.

Map scope

For most maps, a map is centered around a selected node (for example, a device, IP network, VLAN, or service) and shows connections to the selected entity (one hop away). You can change the scope of the elements displayed in the map to see additional connected elements by incrementing the number of hops. You can expand an entire map, one or more individual devices, or a service one increment at a time. A hop is the distance between two nodes that are either physically or logically connected.

- For an entire map, the scope of a map is defined by the number of hops from the focal object (boxed icon). Each time you select the **Increment Hops** option, a map expands by adding all nodes (and their edges) that are one hop away from any existing, expandable node.
- For individual devices, when you select a device and use the **Expand Map Element** option, a map expands by adding all nodes (and their edges) that are one hop away from the selected device. (You can select more than one individual device by pressing the Ctrl key while you use the Expand Map Element option.)

- For Storage Insight NAS and SAN Connectivity maps, when you select an edge with a plus sign (+) and use the Expand Map Element option, the edge expands by one hop.

  Using the Expand Map Element option and the Increment Hops or Decrement Hops options together may result in unexpected behavior. To avoid this, use the **Reset Map** option after the **Expand Map Element** option but before you use the **Increment Hops** or **Decrement Hops** option.

  Note The options Increment Hops, Decrement Hops, and Expand Map Element are not available for IP Network Membership, VLAN Membership, IP Network Physical Connectivity, VLAN Physical Connectivity, and any type of Group map. The scope of these maps always includes the set of devices in the selected IP network, VLAN, or group.

  Applications and Business Services maps support the Expand Map Element option, but not Increment Hops.

Common map attributes

The following attributes, classified by entity, are common to all maps:

- Nodes — A node represents a device, IP network, VLAN instance, service subscriber, service offering, an application, or a user-defined group. The icon used to depict a node depends on the class of the instance. A severity icon bar underneath a node is colored to indicate that its state is normal, affected by one or more abnormal conditions, or unknown. A plus sign (+) next to a node indicates that it is connected to additional nodes not currently shown in the map. A box outlining a node indicates that the node is a map focal node. One or more nodes compose a map. You can incrementally expand the scope of the map to show the additional nodes connected to devices.

  The com.smarts.map.showNormalBanner property determines whether normal map nodes display a green banner. The default value for this property is false, no banner is shown under normal nodes. If the node can be expanded, a small green + displays at the right side of the node. Setting the com.smarts.map.showNormalBanner property to true displays a full-width green banner below each normal map node. Chapter 10 Customizing Your Console provides detailed console-property information.

- Edges — An edge represents a relationship or connection between nodes (for example, a physical connection such as a cable on a Physical Connectivity map), or participation in a logical group (for example, routers participating in a VLAN for a VLAN Connectivity map). The representation depends on the type of map. An edge that represents a topological instance is colored to indicate its status (for example, green for Normal). If an edge represents a relationship, it is colored black.

Tool tips in maps

To activate a tool tip, hold the cursor over the object. A tool tip provides the following information for the following map icons:

- A device (node). Tool tip lists the device's name, model, location, contact, and description.
- An IP network (node). Tool tip lists the number of devices, by type, that are member systems of the IP network.

- A VLAN (node). Tool tip lists the number of devices, by type, that are member systems of the VLAN.
- A group (node). Tool tip lists the group's name, number of individual members, and number of subgroups.
- A service (node):
  - Software service. Tool tip lists the software service's name, the device that hosts it, and a description.
  - Software service redundancy group. Tool tip lists the class and name of the object.
  - Service subscriber. Tool tip lists the service subscriber's name and number of service offerings.
  - Service offering. Tool tip lists the service offering's name and number of service subscribers.
- Edges:
  - Physical connectivity or network connection. Tool tip lists interface and port endpoint information.
  - All other map edges. Tool tip lists the object's name at each endpoint.

    Note Tool tip information for edges in Group maps is not available.

    For example, a Physical Connectivity map containing routers, switches, and their physical connections, the tool tip displays:

  - For each router and switch, the device's name, model, location, contact, and description.
  - For the physical connections, the interface or port number at each end of the connection.

Representing notifications in maps

In a map, the icons (nodes and edges) reflect the collective state of active events on an object.

Understanding color coding and icons

Similar to notifications in the Notification Log Console, the map uses color to indicate that elements are affected by one or more abnormal conditions. A color-coded severity bar indicates the state of the node.

The color-coded severity bar is not displayed for nodes whose state is normal, unless the com.smarts.map.showNormalBanner property is set to true.

Note The notification list configured by your administrator determines which notifications are reflected in your Map Console. If the notification list does not include an event, notifications for the event will not be reflected in the map icons. For example, if a notification list excludes all events from a specific router, the router always appears with a normal state in the map. If your Map Console does not accurately reflect observed conditions, contact your administrator.

Colors and meanings summarizes the colors that display in a map.

Table 6-1. Colors and meanings

Condition	Severity icon (nodes only)	Color (nodes and edges)
Critical event		Red
Major event		Orange
Minor event		Yellow
Unknown		Light blue
Normal/okay		Green

Note The severity icon does not display for edges. However, the color of an edge is meaningful, as follows:

- Edges that represent topology instances are color-coded to reflect status.
- Edges that represent relationships such as VLAN Membership and IP Network Membership are colored black.

Note In an IP Network map, the node for an IP network is always normal, even if the network is inaccessible.

By default, the Normal status indicator is not displayed. However, you can change the setting that controls this display by setting the com.smarts.map.showNormalBanner to true. Command syntax for the -D option contains additional information.

To view the icons and other visual indicators used in maps, select **Map** > **Map Legend**.

Your administrator can configure custom map icons to represent map elements. The *VMware Smart Assurance Service Assurance Manager Configuration Guide* contains additional information.

Displaying notification and topological information

To display detailed diagnostic information, you can:

- Double-click a node or group icon with a severity bar to display the **Notification Properties** dialog box. Or, right-click and select **Notification Properties** in the shortcut menu. *"Displaying notification properties" on page 62* includes information about the **Notification Properties** dialog box.

  If more than one notification affects the icon, you are prompted to select one. A map consideration contains additional information.

  Note Double-clicking a normal node (severity bar not displayed or green) displays the **Containment** dialog box if component information is available. *"Using the Containment dialog box" on page 81* contains additional information.

- Right-click a selected edge (solid line or jagged line) in a Physical Connectivity, IP Network Connectivity, or VLAN Connectivity map. The shortcut menu lists NotificationProperties and the Browse option for the Topology Browser.
- Right-click a selected node, select the **Browse** option, and view the colored events in the **Events** tab.

Types of maps

The types of maps that are available depend on your license(s) and user profile. The Group maps need to be configured by your administrator and may not be available for your session.

Network topology maps

The network topology maps and related classes are available for the IP Availability Manager or IP Performance Manager.

Network topology maps contain elements such as IP networks, VLANs, routers, switches, and hosts, and various types of connections such as cables and trunk cables. The maps typically depict connectivity between elements or device membership. The *VMware Smart Assurance IP Availability Manager User's Guide* and the *VMware Smart Assurance IP Performance Manager and Server Performance Manager User's Guide* describe network topology maps in greater detail.

Types of network topology maps are:

- Physical Connectivity Map
- IP Network Connectivity Map
- IP Network Membership Map
- VLAN Connectivity Map
- VLAN Membership Map

Business Services maps

The Business Services map and related classes are available for the Business Impact Manager.

Business Services maps display service subscribers (organizations, business units, lines of business (LOBs), departments, and customers), business processes, service offerings (for example, order capture, Router Services, Domain Name Service), software services (for example, InCharge services), redundancy groups, and related elements. The Business Services maps are available for infrastructure elements in the Topology tab and groups in the Groups tab.

The VMware Smart Assurance Business Impact Manager User Guide describes Business Services maps.

Applications map

The Applications map and related classes are available for the Application Insight Domain Manager and Application Connectivity Monitor Domain Manager.

An Applications map displays the topological elements related to the delivery of application services. Such elements may include the systems that host software services, redundancy groups, and checks.

Applications maps are described more completely in VMware Smart Assurance Application Insight documentation and VMware Smart Assurance Application Connectivity Monitor documentation.

Network Protocol Manager Connectivity maps

Network Protocol Manager (NPM) maps depict BGP and OSPF topologies and connectivity between topological elements.

Types of NPM maps are:

- An OSPF topology map contains elements such as OSPF areas, services, networks, neighbor relationships, and virtual links; and relationships and connections.
- A BGP topology map contains elements such as autonomous systems, BGP services, and BGP sessions; and relationships and connections.
- An EIGRP topology map contains EIGRP elements along with their relationships and connections.
- An IS-IS topology map shows the status of the IS-IS and transport network elements and their many relationships.

  These maps are described more completely in VMware Smart Assurance Network Protocol Manager documentation.

Multiprotocol Label Switching maps

Multiprotocol Label Switching (MPLS) maps depict MPLS topology. The maps might contain router, LSP, LSP hop, VPN, VRF, Forwarder, and PseudoWire elements, along with their relationships and connections.

Types of MPLS maps are:

- LSP map
- LSP Hops map
- VPN map
- PseudoWire map

  These maps are described more completely in VMware Smart Assurance MPLS Manager documentation.

Storage Insight maps

Storage Insight maps depict storage network topology. The maps might contain storage network elements such as HostSystem and connections such as Powerpath_DataPath and PowerPathRedundancyGroup.

Types of Storage Insight maps are:

- Storage Insight NAS Connectivity Map
- Storage Insight SAN Connectivity Map

  These maps are described more completely in VMware Smart Assurance Storage Insight Manager documentation.

Multicast map

The Multicast map depicts multicast topology, such as instances of the MulticastService, MulticastGroup, MulticastTree, MulticastSource, and MulticastRedundancyGroup classes, and connectivity between topological elements. The maps in the Global Console show labels for devices with special roles within Multicast.

The type of Multicast map is Multicast Connectivity (distribution tree).

The Multicast map is described more completely in VMware Smart Assurance Multicast Manager documentation.

VoIP map

For Voice Over IP (VoIP), the Applications map displays the topological elements related to the delivery of application services. Such elements may include the systems that host software services, redundancy groups, and checks.

Group maps

A group consists of one or more infrastructure devices, IP networks, VLANs, subgroups, and services. Groups are created by your administrator and may not be available for your session. The VMware Smart Assurance Service Assurance Manager Configuration Guide includes additional information on creating groups and importing data for groups.

A member can be an infrastructure device, IP network, VLAN, software service, service subscriber, or service offering. A member cannot be a subgroup.

A group map can display other groups (subgroups/child groups). To display the elements belonging to a group, double-click a selected group node. If the elements exceed 100, you are prompted to confirm whether to display them.

For a high-level group, individual members not assigned to any subgroups do not display in a map. Members are only displayed for groups that do not have subgroups.

The group node is colored to indicate that its state is normal, affected by one or more abnormal conditions, or unknown. The color is determined by the highest severity condition affecting the elements of the group. For example, if an element is experiencing a critical failure, the status bar is colored red. Edges for groups do not change colors.

In a Connectivity group map, one solid line edge represents aggregated relationships. Elements of one group have one or more connections with elements of another group.

Types of group maps are:

- Group Physical Connectivity map. This map displays physical connectivity between group elements. The solid line edges between groups represent one or more physical connections between elements of different groups. The edges do not change colors to reflect their state. The number of hops cannot be changed.

- Group IP Network Connectivity map. In this map, an edge between two groups indicates that there are one or more IP networks common to the two groups. The group icon containing the IP network is displayed; an IP network icon is not displayed. The number of hops cannot be changed.
- Group VLAN Connectivity map. In this map, an edge between two groups indicates that there are one or more VLANs common to the two groups. The group icon containing the VLAN is displayed; the VLAN icon is not displayed. The number of hops cannot be changed.
- Group Membership map. This map displays all of the elements of a selected group or a subgroup. The edges do not display. The concept of a hop is not applicable.

Group IPNetwork Connectivity map example

To display a Group IPNetwork Connectivity map:

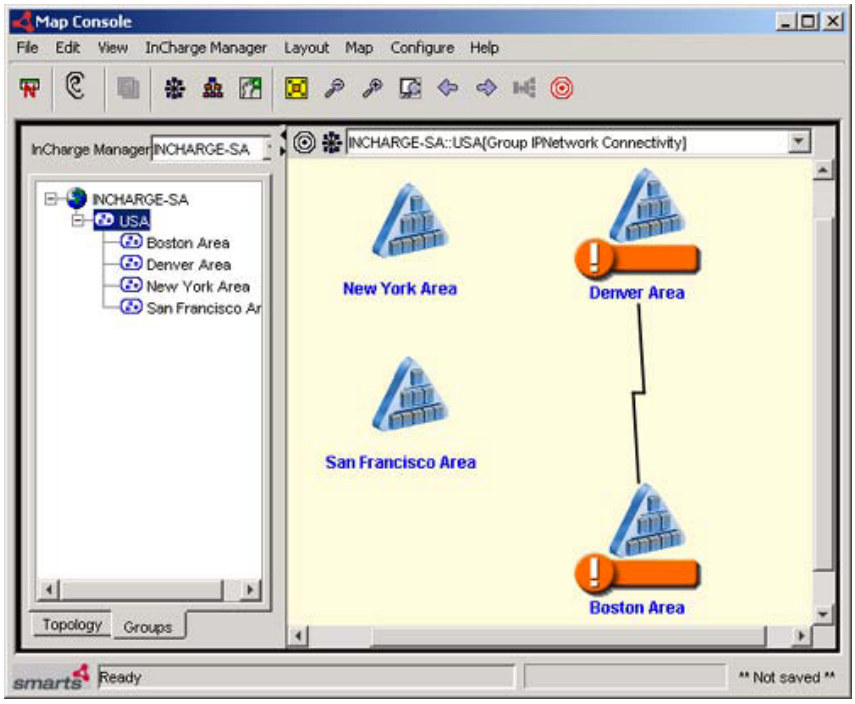
1 Open the Map Console.

2 Select a group in the **Groups** tab.

3 Right-click and select **Group IPNetwork Connectivity** in the shortcut menu. The map displays.

Group IP Network Connectivity map shows a Group IPNetwork Connectivity map for the group USA. Within the USA group, the subgroups have devices that share common IP networks. Notice that two subgroups, Denver and Boston, are orange, indicating serious (major) conditions.

Figure 6-1. Group IP Network Connectivity map



Adjusting the appearance of a map

Several methods exist to adjust or fine-tune the appearance of your map. You can:

- Change the layout from circular to hierarchical. Right-click in the map and select **Hierarchical Layout** from the shortcut menu. Objects in your map are rearranged and the layout indicator changes accordingly.
- Change the layout from circular to orthogonal. Right-click in the map and select **Orthogonal Layout** from the shortcut menu. Objects in your map are rearranged and the layout indicator changes accordingly.
- Change the layout to manual. Right-click in the map and select **Manual Layout** from the shortcut menu. The initial positions of existing nodes are retained. (This option is especially useful for large, complex maps.)

  In manual layout, any new nodes or edges that appear later due to topology changes, the Expand Map Element option, or Increment Hops, display in the lower-left area of the map. You can drag them from the center to new positions that will be maintained as long as the layout type is manual.

  When elements on a map are removed from the topology, their corresponding representation on the map is also removed. When you view the map in Manual Layout, the remaining map elements are not repositioned.

  If you change the manual layout to circular or hierarchical, all manual positions are lost. If you save a map with manual layout, the positions are saved. To return to the map's default layout or to its layout when last saved, select **Map** > **Reset Map** (this resets all map attributes). A layout indicator at the top of the right panel identifies the layout of a selected map.
- For a MPLS VPN map, change the layout based on internal logic. Right-click in the map and select **Organize** from the shortcut menu.
- For NPM maps, enable the display of labels for routers. Right-click in the map and select **Node Labels** from the shortcut menu.
- Move or reposition individual nodes in the map by dragging them.

  Note To select multiple nodes, press **Ctrl** while making your selections.

- Enlarge the right panel and hide the map tree. To do so, click the leftarrowhead on the panel divider. To display the map tree again, click the rightarrowhead.
- Scale the entire map to fit the right panel of the Map Console.
- Right-click in the map and select **Fit to Window** from the shortcut menu.
- Magnify or shrink a map with Zoom or Overview toolbar buttons.
- Increase or decrease the scope of your map by one increment at a time. This adds new nodes to or subtracts nodes from an existing map.

  Right-click in the map and select **Increment Hops** or **Decrement Hops** from the shortcut menu.

- Expand a selected node with the plus sign to increase the scope for it. Right-click the node and select **Expand Map Element** from the shortcut menu. This adds new nodes connected to the selected node.

  Note To select multiple nodes, press **Ctrl** while making your selections and continue to press the **Ctrl** key when you select **Expand Map Element**.

  Using the Expand Map Element option and the Increment Hops or Decrement Hops options together may result in unexpected behavior. To avoid this, use the Reset Map option after the Expand Map Element option but before you use the Increment Hops or Decrement Hops option.

- Add and remove classes using a filter. *"Filtering maps" on page 99* contains additional information.
- Color only map objects experiencing root-cause events (IsRoot = Yes). Click the **Color-by-Root-Cause** toolbar button (tool tip labeled Toggle Root Cause Coloring). Map objects without root-cause events turn gray. Map objects with root-cause events are colored based only on the severity of the root-cause events.

  The Color-by-Root-Cause indicator, at the top of the right panel, indicates when this option is enabled. This option remains enabled for allmaps until you click the toolbar button again.

  For example, a router with two events—a non-root event (IsRoot = No) with severity 1 and a root-cause event (IsRoot = Yes) with severity 2—is colored red. It is colored to reflect the collective state of the active events and, in this case, the most critical severity is 1 (red). If you click the Color-by-Root-Causetoolbar button, the router changes from red to orange, because the lone root-cause event has a severity 2.

- Specify a user-defined background. *"Customizing map backgrounds" on page 96* contains additional information.

  To undo your adjustments, including those made by a filter, and reset the map back to its original layout, select **Map** > **Reset Map**.

  Saving a map contains additional information.

  Navigating among maps describes several navigation methods.

  Chapter 10 Customizing Your Console contains additional information on creating a customized console.

Customizing map backgrounds

You can change the map background color and use custom background images.

Map background colors

By default, different kinds of maps are displayed with different color backgrounds. Default map background colors shows the default map background colors.

Background color	Type of map
Light blue background	Physical Connectivity and Group Physical Connectivity maps

Light yellow background	IP Connectivity and Group IP Connectivity maps
Light green background	VLAN Connectivity and Group VLAN Connectivity maps
Beige background	IP Membership, VLAN Membership, and Group Membership maps
Yellow background	Business Services maps
Purple background	Applications maps

Note You can set a parameter, com.smarts.mapBackgroundColor, to customize the background color. When the com.smarts.mapBackgroundColor property is specified, all maps display the specified background color. When a map is saved, the background color is not included in the saved information. Command syntax for the -D option contains additional information.

Creating custom backgrounds

You can create and install custom map backgrounds using your own images. Examples may include geographic maps, where map nodes are placed over the regions they serve, or organizational charts, where map nodes are placed over the organizational departments they serve.

Custom background requirements

Ensure that the map background file meets the following requirements:

- Required file format— Must be .gif format.

  Note The map background filename must be saved with the .gif extension. The .gif extension must be in lowercase. If the filename for your map background file is .GIF, save the file as .gif. To save the map background file with the .jpg extension, set the smarts.allowBGjpegs property to true. Command syntax for the -D option provides additional information.

- Image size — Must be no larger than 1500 pixels high or 2000 pixels wide.
- Image file location — Store the graphic file in the *BASEDIR/smarts/local/images/<background directory>* where, *<background directory>* is the host where the Global Manager is running.

Adding a custom background

To add a custom map background, do the following:

1. Set the Map Console to Manual Layout (as opposed to Hierarchical, Circular, or Orthogonal Layout): Right-click the map and select **Manual Layout** from the shortcut menu.

   Setting the map to Manual Layout ensures that the position of map elements will not change in regard to one another or to their position on the map background. In addition, with Manual Layout, the Global Console automatically centers the map background within the map window.

2 Right-click the map and select **Set Background** from the shortcut menu.

   The **Set Map Background** dialog box displays that shows thumbnails of the map background images available in the *BASEDIR/smarts/local/images/<background directory>* where, *<background directory>* is the host where the Global Manager is running.

3 In the **Set Map Background** dialog box, select an image, adjust the image size using the controls at the bottom of the dialog box, and then click **OK**. You can also click **Apply** to preview the map.

   The Global Console loads the image so that it is centered over the minimum rectangular bounding box that includes all of the map nodes.

4 After the map is loaded, you can move the map nodes to the appropriate locations on the background image.

   If you repositioned the nodes, right-click the map and select **Fit in Window** from the shortcut menu.

5 Save the map. When a saved map is opened, map nodes retain their position. Saving a map contains additional information.

Removing a custom background

To remove a custom background and return to the default background:

1 Open the **Set Map Background** dialog box.

2 Select **No background image** from the **Map Background File** list box.

3 Click **OK**.

Viewing large maps: Overview window

The **Overview** window displays the entire contents of the map currently being viewed in the right panel as in Map Console with Overview window. This feature is useful for viewing precise areas of a large map.

To magnify areas in your map:

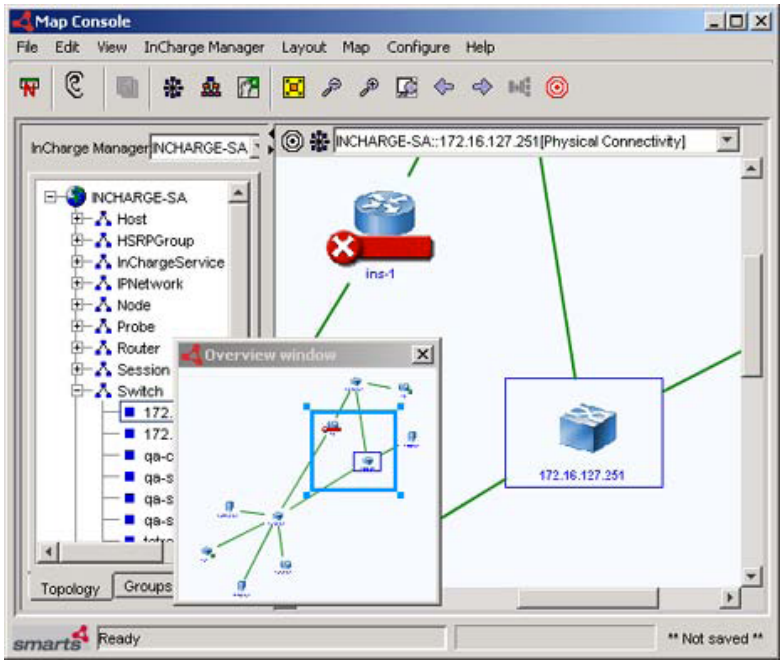
1 Click the **Overview** toolbar button or select **Map** > **Overview**.

2 Click and drag the pointer to outline a small rectangular area. This area is then magnified and displayed in the right panel.

   To resize the rectangle, click and drag its borders in the Overview window. The smaller you make the rectangle, the more magnified the view becomes in the right panel.

   You can also move the rectangle to a new area as well, by clicking and dragging it. As the rectangle is moved, the view in the right panel changes accordingly.

Figure 6-2. Map Console with Overview window



Filtering maps

The map filter enables you to control which classes of instances appear in a specific map. You can remove classes of devices (systems) and logical groups and add them back again. Filter criteria are saved if you save your maps. Saving a map includes additional information.

You can also filter a map by root cause. *"Adjusting the appearance of a map" on page 94* includes additional information.

Removing a class

To remove one or more classes:

1 Select **Map** > **Edit Map Filter** in the Map Console. The **Map Filter** dialog box displays.

2 Select a class from the **Included Classes** list.

3 Click **Remove**. The class is moved to the **Filtered Classes** list.

Note To remove another class, repeat step 2.

4 After the last selection, click **OK**.

Adding a class

To add one or more classes:

1 Select **Map** > **Edit Map Filter** in the Map Console.

2 Select a class from the **Filtered Classes** list.

3 Click **Add**. The class is moved to the **Included Classes** list.

Note To add another class, repeat step 2.

4 After the last selection, click **OK**.

Examining Summaries

7

The Summary View Console provides a graphical overview of notifications, alarmed elements, and business impact instances. By default, a summary is updated continuously. As you monitor your managed domain, you might need more information about a specific summary or to investigate the attributes that compose it. You may also need to add new summaries or modify existing ones.

This chapter includes the following topics:

- Accessing summary information
- About summaries
- Adjusting the contents of a Summary view

Accessing summary information

This section describes another method to access summary information and how to navigate between a summary and its notifications or its default map.

In addition to the different methods for opening available consoles (Chapter 3 Starting a Session), you can add a Summary view to any existing console to access summary information. (Chapter 10 Customizing Your Console includes information about views and adding views.)

To navigate between an individual summary and its corresponding Notification Log view:

1 Right-click the summary and select **Show Notifications** in the shortcut menu. Or, for the selected summary, click **Summary** > **Show Notifications** or the **Show Notifications** toolbar button.

   The Notification Log view for the selected summary displays in a secondary window.

2 To return to the Summary view, click **Close** in the Notification Log view.

   To navigate between an individual summary and its corresponding default map:

3 Right-click the summary and select **Show Map** in the shortcut menu. The default type of map for the selected summary displays in a secondary window.

4 To return to the Summary view, click **Close**.

Note Show Map is enabled if a topological filter is specified for the summary. Topology Filter dialog box includes additional information.

About summaries

A summary provides a graphical overview (bar chart or pie chart) of notifications from one source, a Global Manager. A Summary view can contain several summaries attached to either the same Global Manager or to different Global Managers.

Summaries can represent notifications for infrastructure elements and collection objects (ServiceOffering, ServiceSubscriber, or any group created by your administrator), organized in some meaningful way. The content is determined by summary parameters and, optionally, a filter. *"Adjusting the contents of a Summary view" on page 104*includes information on summary parameters. Filtering summariesincludes additional information on filters.

When you are interpreting summaries, you should be aware of the different components of a summary and the information they represent.

Summary components

A summary view is a graphical display of information in either a horizontal bar chart or a pie chart. The chart represents the number (horizontal bar chart) or percentage (pie chart) of counted items (notifications, alarmed elements, or impacts). For example, a chart might show the number of Notifications categorized by severity level, or the number of Notifications that have been acknowledged. Displaying all elements by severity includes additional information on displaying elements by severity levels.

A summary includes the summary title, which is the user-configurable display name of the summary. The default title of a summary is the name of the group, service offering, subscriber, or Notification Log. In addition, the summary identifies the Global Manager that is the source of the summary information.

The summary represents the counts by numeric values (labels) and visually by horizontal bars or sections of a pie.

Note If the criterion is Severity, the colors of the horizontal bars correspond to those in the Notification Log legend; otherwise, the colors are not significant.

In a horizontal-bar chart, the labels are displayed as a vertical list along the left side of the bars, while the counts for each category are displayed horizontally across the bottom. In a pie chart, the sections represent the percentage of each category, with a legend indicating the category criteria.

To display the count or the percentage information in a tool tip, hold your cursor over a horizontal bar or pie section.

Modifying a new summary or an existing one includes instructions about changing the contents of a summary (for example, its title, counted elements, or criterion).

Unavailable (gray) content

Sometimes, the contents of a summary turn gray. This occurs if:

- The Global Console disconnects from the Global Manager. When the connection is re-established, the affected summaries in the Summary view are automatically recounted and displayed.
- A collection object specified for a summary's topological filter is removed from the topology.

Calculation notes

Depending on the summary, when a counted item (an affected element, an event, or impact value) matches more than one value of the criterion, the sum of the detailed counts might exceed the totals. For example, if affected devices are counted by instance name such as RouterCore*, Router*, and Switch*, the detailed counts might exceed the number of affected devices in the total count because, for example, any instance name that matches RouterCore will also match Router, and will therefore be counted twice.

How percentages are calculated

To display percentages or total count, use a tool tip. Hold your cursor over a horizontal bar or pie section.

Percentages are calculated as follows:

- For counted elements, the percentage is the number of elements experiencing events for a given value of the criterion, divided by the total number of elements in the summary.

  For example, for elements counted by the criterion severity, 12 (14 percent) for the value Critical indicates that 12 elements have critical events. This represents 14 percent of 83 elements in a summary.
- For counted notifications, the percentage is the number of events for a given value of the criterion, divided by the total number of events in the summary.
- For counted impact, the percentage is the sum of the impacts for all events for a given value of the criterion, divided by the sum of the impacts for all events in the summary.

Adjusting the contents of a Summary view

Several methods exist to adjust the appearance of your Summary view. You can:

- Modify a new or an existing summary in a Summary view.
- Rename a summary.
- Specify a display update interval for a summary.
- Add a new summary to a Summary view.
- Delete a summary from a Summary view.
- Rearrange summaries within a Summary view.

- Apply a filter to a summary.

  You can also change the name of a Summary View Console, add different views to it, and save the console with customizations. Chapter 10 Customizing Your Console contains additional information.

Modifying a new summary or an existing one

When you initially open a Summary View Console (**File** > **New**) or add a Summary view (**View** > **Add View**) to a console, it contains one default summary for each attached Global Manager.

To modify a specific summary, edit its parameters and apply or change its filter, as illustrated in Edit Summary Parameters dialog box. Changes to a summary are saved when you save the console.

Note Filtering summaries includes information on filters.

To edit summary parameters:

1 Click a summary.

2 Select **Summary** > **Edit Summary Params** . Or, right-click in the area near the summary title and select **Edit Summary Params** in the shortcut menu. The **Edit Summary Parameters** dialog box displays.

Figure 7-1. Edit Summary Parameters dialog box

3 In the **General** tab, you can change the following:

- **Manager** — Select the Manager from the Manager menu.
  - **Chart Type** — Select Horizontal Bar or Pie in the Chart Type menu.
  - **All elements by severity** — Select this option to display all elements by severity in a summary.
  - **Title** — Select the button for the empty Title field and type the new name. To return to the Default title, select the Use Default option.
  - **Update Interval** — Select the Update Continuously checkbox, or clear the checkbox and specify the time in the Update Every field.

4 Click **Apply** to see the results in the selected summary, then click **OK** when you are finished. Or, you can click the **Attributes** tab.

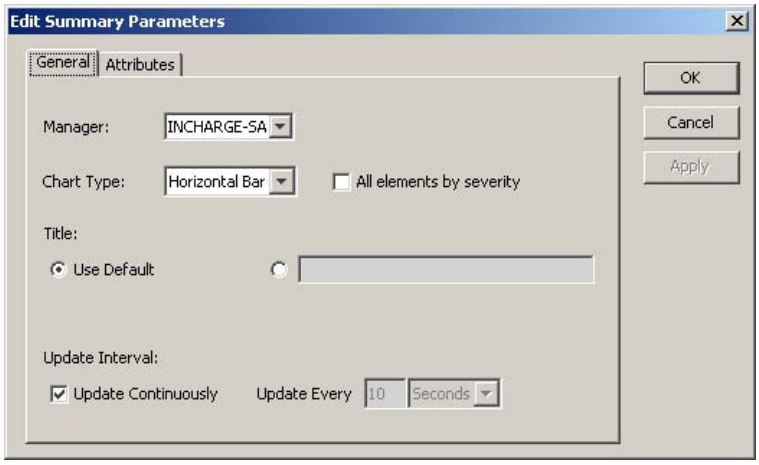
5 In the **Attributes** tab, you can change the summary parameters, as follows:

- Change the criterion used to organize the counts by selecting a category in the **Count** menu and an attribute in the **categorized by** menu. For example, you can choose to count notifications categorized by Class, or Alarmed Elements categorized by Acknowledged. Notification Log columns includes attribute descriptions.
  - Specify values for the criterion. For some attributes like Severity, the values are predefined. For other attributes like InstanceName, you can specify exact names or names with wildcard characters for pattern matching. Values are case-sensitive. (Chapter 12 Wildcard Patterns includes a list of wildcards.)

For some attributes like Event, there is an **Enable Top 5 Occurrences** checkbox, which is selected by default, and which sets the criteria to the five most frequently occurring values. You can clear the checkbox to specify your own criteria instead of the default “top 5”.

Use the **Other** checkbox to count events that do not match any of the values.

6 Click **Apply** to see the results in the selected summary, then click **OK** when you are finished.



Displaying all elements by severity

To display all elements by severity in a Summary view, click the All elements by severity checkbox. When this option is selected, additional summary parameters are not required and the Attributes tab does not display. The resulting summary lists the number of alarmed elements as a fraction of the total number of elements.

If an element has multiple severity notifications, the element is listed only once, at the highest severity notification level. For example, if a Global Manager has two elements, one element listed as normal and one element listed as having one Critical, one Major, and three Unknown notifications, the summary will list:

- One element as normal
- One element as Critical

Note When the All elements by severity option is selected, you cannot modify or set filter options for the summary. You can change the topological filer allowing you to select a group as the basis for the summary.

Modifying a summary’s title

In the **Edit Summary Parameter** dialog box, you can also rename a summary. To rename a summary, specify a new name in the **Title** field of the **Edit Summary Parameter** dialog box and click **OK**.

Specifying a display update interval for a summary

In the **Edit Summary Parameter** dialog box, you can also specify an interval for scheduled updates. Summaries are constantly being updated in your console by default. If you want to control how often summaries are updated, you can specify time intervals for scheduled updates.

To specify an interval for scheduled updates:

1 Clear the **Update Continuously** checkbox and specify the time in the **Update Every** field.

2 Click **OK .**

Adding a new summary to a Summary view

To add a summary to a Summary view:

1 Click on the view to activate it. The active view has a dark gray border.

2 Select **Summary** > **Add Summary**. An additional summary appears in the Summary View Console.

Deleting a summary from a Summary view

To delete a summary from a Summary view:

1 Click on the summary you want to delete.

2 Select **Summary** > **Delete Summary**.

Rearranging summaries in a Summary view

You can reposition summaries with the arrow toolbar buttons. Click the toolbar button to move a summary one cell to the left or right. If another summary is next to the selected summary, click the toolbar button to change the order of the summaries.

To specify how many summaries appear per row in a Summary view:

1 Click the view.

2 Select **Summary** > **Layout**.The default value is four. Specify a number.

3 Click **OK**.

Filtering summaries

The Summary view uses the same filtering mechanism as the Notification Log view except that there is an additional topological filter and a default filter criterion for active events. The default filter criterion for active events ensures that the summary represents only active events. There is one filter per summary. Filter criteria are saved if you save your console.

To customize a summary's filter criteria, use the Filter Builder dialog box, which is accessed by right-clicking the area near the summary title and selecting Filter in the shortcut menu.

A topological filter enables you to limit the display of notifications for all of the members of a specified collection object. A collection object can be a service offering, service subscriber, or any group created by your administrator.

If a topological filter is not specified, the total count indicates the number of affected elements for the entire topology and disables the Show Map toolbar button for a given summary.

In addition, you can apply filters from the Filter Builder dialog box that control which notifications might appear in the summaries. Filtering notifications includes additional information.

Use one of the following methods to open the Filter Builder dialog box:

- In the Summary View Console, click a summary and select **Summary** > **Filter**.
- Right-click in the area near the summary title and select **Filter** in the shortcut menu.

Topology Filter dialog box

The Topology Filter button appears in the Filter Builder dialog box when a summary is selected. To specify a topological filter:

1. In the **Filter Builder** dialog box, click **Topology Filter**. The **Topology Filter** dialog box appears.
2. In the **Class Name** menu, select a collection object (ServiceOffering, ServiceSubscriber, or group).

   The value None allows all of notifications to display in a summary unless you specify other filter criteria.
3. Select a class instance from the **Select instance** list.

   If instances do not display in the **Select instance** list, click **Get instances** to retrieve a list. Depending upon your network configuration and if the collection object has thousands of instances, it might take a few minutes to retrieve a list.

   Instances appear, by default, in the **Select instance** list if the collection object has fewer than 50 instances. *"Adjusting Java properties" on page 151* includes information on the com.smarts.maxFilterInstances property.

   The instance's name displays as a summary title unless you specified a title using the **Edit Summary Parameter** dialog box. Modifying a summary's title includes additional information.
4. Click **OK** after your last selection. This immediately applies the topological filter to the selected summary and closes the **Topology Filter** dialog box.

   If you want, you can continue to create or modify filter criteria in the Filter Builder dialog box. Filter criteria specified in the Filter Builder affect notifications that might affect summaries.

   Note If you click Cancel in the Filter Builder dialog box after applying a topological filter, the newly created topological filter is not cancelled.

Examining Status Tables

8

A Status Table Console provides a high-level graphical overview of the status of underlying infrastructure elements as they affect the collection objects (ServiceOffering, ServiceSubscriber, or any group created by your administrator) specified in the Status Table. For example, in a Status Table view, you can determine at a glance which services or applications used by corresponding business elements are affected by the health of managed infrastructure elements.

A Status Table view is dynamically updated as the state of elements and notifications within the Global Manager's topology is updated. In addition, the Status Table view is updated as elements are added or removed from the topology.

The ability to view and configure a Status Table is associated with your user profile. Your administrator can configure Status Table views and then associate them with your user profile. As a result, your console may or may not display Status Table information.

This chapter includes the following topics:

- Accessing Status Table information
- About Status Table information
- Configuring a Status Table view

Accessing Status Table information

To open a new Status Table Console from an existing console, select **File** > **New** > **Status Table Console** . The **Status Table Console** displays in a secondary window.

To refresh the information in a row or column, click the name of an element in the row or column.

Another method to access Status Table information is to add the Status Table view to your console. Select **View** > **Add View**. *"Tailoring your console with views" on page 158* includes additional information.

About Status Table information

The Status Table Console displays a grid comprised of the following:

- Primary Class (y-axis) — Selection from a group of collection objects (ServiceOffering, ServiceSubscriber, or any group created by your administrator).

- Secondary Class (x-axis) — Selection from the group of corresponding instances of the Primary Class.

  For example, if primary class, Customer, and secondary class, ServiceOffering is selected the Status Table view can show the instances and notification status of the various service offerings available to each customer.

  For each point on the grid where an instance of the Secondary Class is located on a Primary Class row, the table displays the severity icon for the corresponding infrastructure element with the highest severity status, including the status, Normal. If there is no severity icon, there is no instance of that element for that class.

  From the Status Table, you can obtain detailed information about the element by right-clicking its icon.

  Note Client and server tools can be invoked from an instance node displayed in the Status Table.

Examining element details

To see detailed information about an element, right-click the severity icon for the element, and then select one of the options, listed in Status Table shortcut menus, from the shortcut menu.

Table 8-1. Status Table shortcut menus

Selection criteria	Option	Description
Right-click the severity icon for an instance	Browse	Opens the Topology Browser view for the current Global Manager that contains the selected element in a secondary window
	Containment	Displays an element's components
	Notification Properties	Displays notification properties for that element
	Show Map	Opens a map with that element as focus
	Server Tools	Displays a list of server tools if enabled
	Client Tools	Displays a list of client tools if enabled

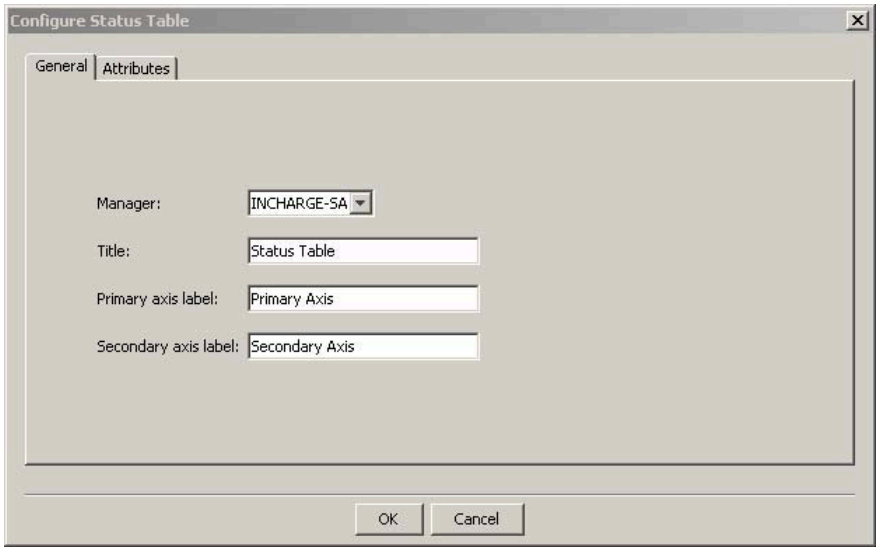
Configuring a Status Table view

To configure a status table view:

1 Click the status table view to activate it. The active view has a black border.

2 Select **Status Table**> **Configure Status Table**. The **Configure Status Table**dialog box displays as illustrated in Configure Status Table dialog box

Figure 8-1. Configure Status Table dialog box



The Configure Status Table dialog box contains two tabs:

- General — Options allow you to select a manager and to add a title and axis labels to the status table.
- Attributes — Functionality allows you to select multiple classes and class instances.

Adding a title and axis labels to the Status Table view

To add a title and axis labels:

1 Display the **Configure Status Table** dialog box.

2 From the **General** tab:

- Select the manager from the **Manager** list box.
  - Type a title for the Status Table in the **Title** field.
  - Type a label for the Primary axis in the **Primary axis label** field.
  - Type a label for the Secondary axis in the **Secondary axis label** field.

3 Click **OK**.

Configuring the Status Table primary and secondary axes

To configure the status table view's primary and secondary axes:

1 Display the **Configure Status Table** dialog box.

2 Click the **Attributes** tab.

3 Select the classes for the Primary Class (y-axis) and the Secondary Class (x-axis).

4 Click **OK**.

The **Status Table Console** displays using the parameters you typed.

Using Save includes information on saving your Status Table console.

The *VMware Smart Assurance Service Assurance Manager Dashboard Configuration Guide* includes additional information about the Status Table as a dashboard viewlet.

Responding to Notifications

9

Operators can perform a variety of tasks in response to notifications or to changed states of map icons. Operators usually address the notifications based upon their severity and perform exploratory or corrective actions. This chapter provides step-by-step instructions for acting upon notifications and for saving and recording information.

Note Depending upon their user profiles defined by the VMware Smart Assuranceadministrator, operators might have access to different types of consoles and console operations.

Instructions apply to the following consoles: Notification Log, Map, Topology Browser, and Summary View, unless noted otherwise.

This chapter includes the following topics:

- The notification life cycle
- Taking action
- Saving and recording information
- HyperNotif Statistics

The notification life cycle

A notification can be in one of five states. If the Event State column in your Notification Log view is displayed, you can view the event state. The five event states are:

- UNINITIALIZED — The original event state of a notification.

  The UNINITIALIZED state is not visible in the console because, like any client, the console does not receive uninitialized notifications.

- ACTIVE — The event state of a notification when an event occurs and the notification informs (notifies) a client of the event.

  When a notification is notified, the event state changes from the current value to ACTIVE. The notification displays in the Global Console unless an administrator sets a notification list filter that prevents it from displaying.

- SUSPENDED — The event state of a notification when the Global Manager can no longer receive information about an active notification (for example, an agent is not responding).

  In this case, the notification remains active although its event state changes to SUSPENDED and its severity level changes to Unknown (severity=4).

  Note The SUSPENDED attribute is not applicable when the Broadcast Event State on Restart parameter system default is configured to FALSE. The “Defining System Defaults” section of the VMware Smart Assurance Service Assurance Manager Configuration Guide provides detailed information.

- WAS_ACTIVE — The event state of a notification when an underlying Manager disconnects from a Global Manager (due to a network outage, for example) or a Global Manager is restarted.

  In this case, the notification remains active although its event state changes to WAS_ACTIVE. If the session connection cannot be re-established, the severity level also changes to Unknown (severity=4).

  Once the session connection is re-established and the notification is re-notified, the WAS_ACTIVE state changes back to ACTIVE. If an underlying Manager fails to re-notify an active notification, the system clears the event and state of the notification changes from WAS_ACTIVE to INACTIVE.

  Note The WAS_ACTIVE attribute is not applicable when the Broadcast Event State on Restart parameter system default is configured to FALSE. The “Defining System Defaults” section of the VMware Smart Assurance Service Assurance Manager Configuration Guide provides detailed information.

- INACTIVE — The event state of a notification when a notification has stopped occurring. When a notification is in the INACTIVE state, it is said to be *cleared*.

  Summary of event states summarizes possible event states of a notification and columns that might appear in your console.

Table 9-1. Summary of event states

Event State column	Active column	Severity column
ACTIVE	True	Can be severity levels 1–5
SUSPENDED	True	Severity level 4
WAS_ACTIVE	True	Severity level 4
INACTIVE	False	Severity level from when notification was active

Note The UNINITIALIZED event state is not visible in the console.

Notification severity includes a description of icons that correspond to severity levels.

Acknowledgement

Operators usually address the notifications based upon their severity and perform exploratory or corrective actions. *"Taking action" on page 122* includes a list of actions.

One of the actions that an operator can take is acknowledgement. After an operator completes corrective actions or determines that notifications do not require attention, an operator can acknowledge active and inactive notifications. Acknowledgement informs fellow operators that they can ignore the specific notification. When an operator acknowledges a notification, the notification ownership (Owner field) is changed to the operator who acknowledged the notification and the value Yes displays in the Acknowledged field.

Inactive notifications can also be automatically acknowledged by the Global Manager. When the Global Manager acknowledges an inactive notification, the notification ownership is changed to SYSTEM.

Note Acknowledgement does not change a notification's state unless the notification attribute ClearOnAcknowledge is set to True for a specific notification. Methods to clear active notifications includes information about the ClearOnAcknowledge attribute.

Methods to clear active notifications

Active notifications may become inactive (cleared) in the following ways:

- When an underlying Manager determines that an event is no longer occurring, the state of its notification is changed to inactive and the changed state is recorded in the audit log. The Manager, the source of the notification, clears the event.
- If the source of the notification is not capable of clearing an event, the event can be cleared after an expiration interval provided by the source.
- When the notification attribute ClearOnAcknowledge is set to True for a specific notification, the notification becomes inactive when an operator acknowledges it.
- When an underlying Manager fails to re-notify an active notification after a disconnect condition is restored, the state of the notification changes from WAS_ACTIVE to INACTIVE. The system clears the event.

Notification archival

The system archives inactive notifications if:

- They have been acknowledged.
- The time interval set for the InactiveAutoArchiveIntervalArchival parameter has passed. The parameter is specified in the Service Assurance configuration file, ics-default.xml file.

  Related audit logs are also archived. Unacknowledged notifications cannot be archived. Configuration parameters related to notifications includes information about archival parameters.

Archived notifications are removed from the Global Manager's memory-resident database and are written to an archive file. The notification archive file is named global_manager.archive and located in the BASEDIR/smarts/local/logs directory.

After a notification is archived, the Global Manager treats a recurrence of that notification as though it were a first occurrence. The values of notification attributes start all over again: new First Notify time, Count starts at 1, and so on.

Removal from display

Notifications, active or inactive, are removed from the console display if they are:

- Filtered out by notification list filter criteria
- Filtered out by console filter option
- Archived

Example of a notification's life cycle

Each notification has a unique name. A notification's name consists of the class name and instance name where the event occurred, and the event name. The notification naming convention is:

```
NOTIFICATION-ClassName_InstanceName_EventName
```

For example, the notification NOTIFICATION-Router_R1_Down identifies the event Down, which occurred in instance R1 of the Router class.

The Notification Log Console will not list more than one notification with this name. If the event clears and occurs again before it is archived, the Count field is increased accordingly.

The following notification attributes are related to a notification's state:

- First Notify — Is the first time a notification occurs.
- Last Notify — Is the last time a notification occurs.
- Last Clear — Is the last time a notification cleared.
- Last Change — Is the last time a notification changed.
- Count — Is the number of occurrences of an event starting from First Notify until Last Notify.

  For the First Notify and Last Notify attributes, the timestamp value is provided by the underlying domain that diagnosed the event.

  Notification Log columns includes additional notification attributes information.

States of NOTIFICATION-Router_R1_Down illustrates the states of the notification NOTIFICATION-Router_R1_Down. For the First Notify and Last Notify attributes, the timestamp value is provided by the underlying domain that diagnosed the event. Values for Last Change, Count, and Last Clear (not shown) are provided by the Global Manager.

Note When a Global Manager disconnects from an underlying Domain Manager, all notifications identified as ACTIVE are marked as WAS_ACTIVE. When the Global Manager reconnects to the underlying Domain Manager, the Global Manager refreshes its subscriptions and starts receiving currently active events from the Domain Manager. Existing WAS_ACTIVE notifications are interpreted as resubscription messages, not as re-occurrences of notifications. The notification is updated to a state of ACTIVE, the Last Change attribute is assigned the current time, and the Last Notify attribute value remains unchanged.

Table 9-2. States of NOTIFICATION-Router_R1_Down

Time	User/system actions	Notification status	Time of first notify	Time of last notify	Time of last change	Count
2:00		Notify	1:00	1:00	2:00	1
2:15		Clear	1:00	1:00	2:15	1
2:25		Notify	1:00	2:25	2:25	2
2:35		Clear	1:00	2:25	2:35	2
3:00	Acknowledge		1:00	2:25	3:00	2
3:05	Archived		1:00	2:25	3:00	2
3:55		Notify	3:55	3:55	3:55	1
4:00	Disconnect		3:55	3:55	4:00	1
4:05		Notify	3:55	3:55	4:05	1

In this example, an Availability Manager generated a Down event at 1:00.

At 2:00, the Global Manager connected to the Availability Manager and the Global Manager created the notification NOTIFICATION-Router_R1_Down for the Down event. The Global Manager retains the original timestamp of the event and stores it in the notification—First Notify and Last Notify are assigned the values of 1:00. The notification's EventState is ACTIVE.

At 2:15, the notification is cleared.

At 2:25, the Availability Manager generated the same Down event again, the Availability Manager was already connected to the Global Manager, and the Global Manager reactivates the notification. The First Notify remains 1:00 and the Last Notify reads 2:25. The notification's EventState changes to ACTIVE.

At 2:35, the notification is cleared. The notification's EventState changes to INACTIVE.

At 3:00, the operator acknowledged the notification. The notification's EventState changes to INACTIVE.

Notice at 3:05, the notification is archived and the archive action records the most recent values for First Notify, Last Notify, and Last Change. A notification cannot be archived until it has been acknowledged. Acknowledgement does not change a notification's state unless the notification attribute ClearOnAcknowledge is set to True for a specific notification. The notification is removed from the notification view.

At 3:55, the Availability Manager generated a Down event again and the Global Manager created the notification again. After a notification is archived, the Global Manager treats a recurrence of that notification as though it were a first occurrence. The notification's EventState is ACTIVE. The value of notification attributes start all over again: new First Notify time, Count starts at 1, and so on.

At 4:00, the Availability Manager disconnects from the Global Manager. The Global Manager marks the notification as WAS_ACTIVE. Last Change value is updated as whenever a change is applied to a notification.

At 4:05, the Availability Manager is restarted and reconnects to the Global Manager. Since a reconnection causes a client to re-subscribe to remote server's events, all currently active alarms in the Availability Manager that the Global Manager subscribed are re-sent to the Global Manager. The Global Manager uses these event messages to update the event state of existing notifications. Notifications that did not previously exist or were INACTIVE before the disconnect, are notified with their Last Notify and Last Change times initialized or updated appropriately, and the notifications' EventState is ACTIVE. For existing WAS_ACTIVE notifications, the event message is interpreted as a re-subscription message, in other words not as a re-occurrence of the notification. The notification's Last Notify does not change. Its EventState is updated to ACTIVE and Last Change time is assigned the current time since changes were applied to it. In short, Last Notify attribute value is not updated when a notification transitions from WAS_ACTIVE to ACTIVE.

Configuration parameters related to notifications

Inactive acknowledged notifications can be archived after a time interval specified by the System Administrator in the Global Manager Administration Console. The System Administrator can also specify an interval for INACTIVE unowned notifications to be automatically acknowledged. Related audit logs are also archived. Unacknowledged notifications cannot be archived.

Durable, momentary, and stale notifications

Some notifications are caused by durable events. A durable event has a measurable duration; it is active for a period of time (for example, a link failure). Durable events are sent from underlying Managers.

Other notifications are caused by momentary events. A momentary event occurs and is significant for only a specific point in time (for example, an authentication failure event for a device).

Whether an event is durable or momentary is indicated in the Event Type column of your Notification Log Console. (*“About notifications” on page 56* includes column descriptions and also severities.)

Note Sometimes, notifications become outdated (or "stale"). Due to network outages, it is possible that the underlying Managers disconnect from the Global Manager. At this point, a Session Disconnected notification displays to inform the operator that disconnected sources are detected. The notifications from the unavailable sources are not updated in the console. Responding to disconnected Managers includes additional information.

Taking action

When an event occurs and Service Assurance generates a notification and displays a severity icon, you can respond and perform corrective procedures.

You can:

- Acknowledge notifications.
- Take and release ownership of notifications while you are working on them.
- Invoke tools such as Telnet, Ping, email, or pager messages, or open and close trouble tickets if they have been configured by your administrator.

Acknowledging notifications

To inform your fellow operators that they can ignore a notification, you can acknowledge the notification if you have completed some corrective action for it or determined that it can be disregarded. You can acknowledge active and inactive notifications.

To acknowledge one or more notifications:

1. In the **Notification Log Console**, select a notification. (To select multiple notifications, press the **Ctrl** key while making your selections.)
2. Select **Event** > **Acknowledge** in the Notification Console’s Event menu. (Alternatively, right-click the notification and select the **Acknowledge** option from the shortcut menu.)

   The value Yes displays in the **Acknowledged** field.

   When a notification is acknowledged, an entry is added to its audit log. Acknowledged notifications may be archived after some period of time, depending on your Service Assurance configuration. By acknowledging a notification, you automatically take ownership of it.

Unacknowledging notifications

If you decide that certain acknowledged notifications do require additional attention, you can reset acknowledgement to unacknowledgement.

To unacknowledge notifications:

1 In the **Notification Log Console**, select a notification.

Note To select multiple notifications, press the **Ctrl** key while making your selections.

2 Select **Event** > **Unacknowledge** in the Notification Console's Event menu. Alternatively, right-click the notification and select the **Unacknowledge** option from the shortcut menu.

The value No displays in the **Acknowledged** field.

When notifications are unacknowledged, entries are added to their audit logs. Unacknowledged notifications are not archived. Unacknowledging a notification does not change its ownership.

Taking ownership

To inform your fellow operators that you are working on a notification, you can insert your username in the notification's Owner field. To do so:

1 In the **Notification Log Console**, select the notification.

2 Select **Event** > **Take Ownership** or right-click and select **Take Ownership** from the shortcut menu.

Your username is added to the **Owner** field and it is also recorded as an entry in the audit log.

The Owner field is informative; no additional rights are granted to the owner. Also, if there is an existing owner listed, you can overwrite it when you take ownership.

Releasing ownership

To inform your fellow operators that you are no longer working on a notification, you can remove your username from the Owner field. To do so:

1 In the **Notification Log Console**, select the notification.

2 Select **Event** > **Release Ownership** or right-click and select **Release Ownership** from the shortcut menu.

Your username is deleted from the **Owner** field and the deletion is also recorded as an entry in the audit log.

Scheduling maintenance

To inform your fellow operators that a specific managed element is entering its scheduled maintenance period, you can set the In Maintenance option in a notification. When a managed element enters its scheduled maintenance period, all active, existing, and newly generated notifications for the scheduled element or related managed entity display the In Maintenance option.

You can schedule maintenance by:

- Interactively using the console

- In bulk using the command line

Note By default, the Schedule Maintenance functionality is only enabled for administrators. If this functionality is not available to you, contact your administrator to have this functionality enabled for you. The VMware Smart Assurance Service Assurance Manager Configuration Guide provides additional information on removing console operations.

The Schedule Maintenance functionality is available only for classes which belong to the following categories:

- UnitaryComputerSystem
- ICIMServiceConnection
- SoftwareService
- NetworkConnection

To schedule maintenance:

a Ensure that the Business Impact Manager server is running and that the MBIM domain has been defined and enabled.

Note The VMware Smart Assurance Service Assurance Manager Configuration Guide provides detailed information on defining and enabling domains.

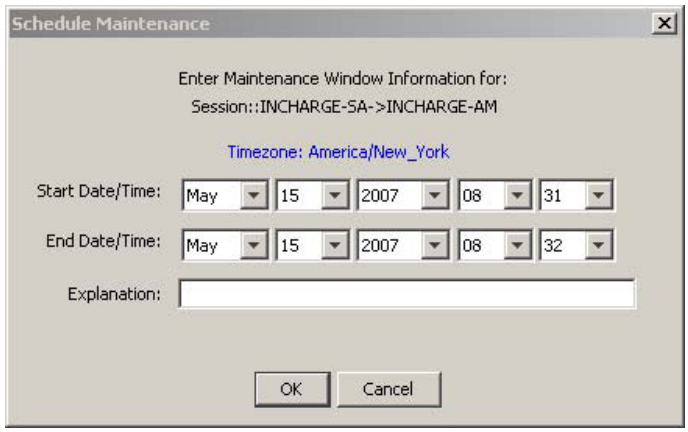
b In the **Notification Log Console**, right-click a notification.

The submenu appears.

c Select **Schedule Maintenance**.

The **Schedule Maintenance** dialog box appears, as illustrated in Schedule Maintenance dialog box.

Figure 9-1. Schedule Maintenance dialog box



d Type the starting date and time for the maintenance period in the **Start Date/Time** fields.

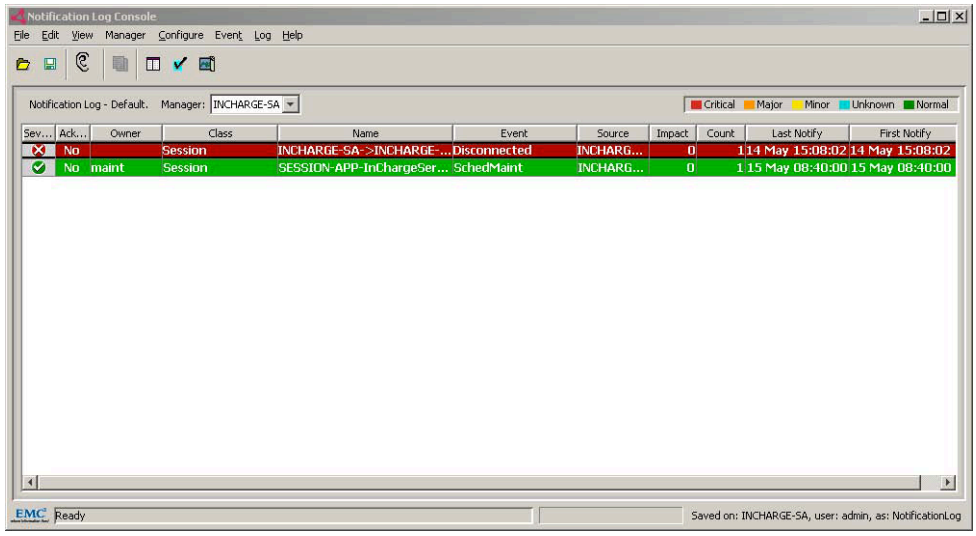
e Type the ending date and time for the maintenance period in the **End Date/Time** fields.

f Type a reason for the maintenance period in the **Explanation** field.

g Click **OK**.

The notification for the managed element displays SchedMaint in the Event column, as illustrated in Notification displaying SchedMaint.

Figure 9-2. Notification displaying SchedMaint



Double-clicking the SchedMaint notification displays the Notification Properties dialog box.

Scheduled maintenance fields defines scheduled maintenance fields available in the General tab.

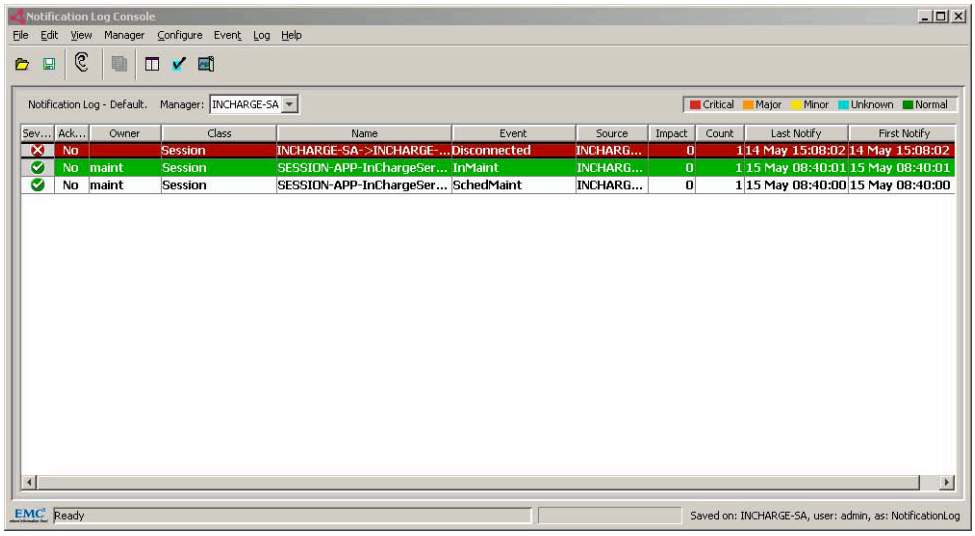
Table 9-3. Scheduled maintenance fields

Field	Definition
UserDefined1	Defines the duration of the maintenance interval in seconds. **Note** If the user specifies a maintenance interval beginning before the current time, this duration will only be the time remaining until the end of the maintenance interval, not the length of the whole interval. Example: If user specifies interval from 9:00 to 10:00, and it is 9:30 when the Schedule Maintenance request is submitted, UserDefined1 will have the value of 30 minutes, not 60 minutes.
UserDefined2	Defines the end of the maintenance period.
EventText	Defines the following scheduled maintenance information: ■ Start time ■ End time ■ User ID (identifies the user scheduling the maintenance) ■ Explanation text (text entered in the Scheduled Maintenance dialog box's Explanation field, see Schedule Maintenance dialog box)

Note When you schedule maintenance to begin in the future, a SchedMaint notification is created. When the maintenance period begins, the Service Assurance Manager server generates an InMaint notification. This notification lists only the maintenance period end time.

When the date and time of the scheduled maintenance period has arrived, the notification displays InMaint in the Event column, as illustrated in Notification displaying InMaint.

Figure 9-3. Notification displaying InMaint



The notification is cleared when the maintenance date and time have ended.

Clearing a scheduled maintenance period

To clear a scheduled maintenance notification:

1 In the **Notification Log Console**, right-click an InMaint notification.

2 Select **Acknowledge**.

The scheduled maintenance notification is cleared.

Deleting a scheduled maintenance period

Note You can only delete a scheduled maintenance notification if it has not entered the scheduled maintenance period.

To delete a scheduled maintenance notification:

1 Log in to the console without user maint privileges.

2 In the **Notification Log Console**, right-click a SchedMaint notification.

3 Select **Acknowledge**.

The scheduled maintenance notification is removed.

Forcing a scheduled maintenance period

If you have scheduled a maintenance period for the future, you can force a scheduled maintenance to take place immediately.

To force a scheduled maintenance:

1 Log in to the console with user maint privileges.

2 In the **Notification Log Console**, right-click a SchedMaint notification.

3 Select **Acknowledge**.

4 Right-click the notification and select **Schedule Maintenance**.

The **Schedule Maintenance** dialog box appears.

5 Type the starting date and time for the maintenance period in the **Start Date/Time** fields.

6 Type the ending date and time for the maintenance period in the **End Date/Time** fields.

7 Type a reason for the maintenance period in the **Explanation** field.

8 Click **OK**.

Enabling maintenance tracking

To enable maintenance tracking:

1 Log in to the console.

2 Define and enable the MBIM domain.

Note The VMware Smart Assurance Service Assurance Manager Configuration Guide provides detailed information on defining and enabling domains.

3 In the **Domain Manager Administration Console**, select **INCHARGE-MBIM** from the **Manager** list box, and select **Topology** > **Add Source** to launch the **Add Source** dialog box.

4 In the dialog box, select **SA** from the **Element Type** list box, type the name of the Service Assurance Manager server (for example, **INCHARGE-SA**) in the **Element Name** field, and then click **OK** to add the Service Assurance Manager server as a topology source.

5 In the **Topology Browser Console**, right-click the instance of the local Service Assurance Manager server in the InChargeDomain class.

A submenu appears.

6 Select **Enable Maintenance**.

Disabling maintenance tracking

To disable maintenance tracking:

1 Log in to the console.

2 In the **Topology Browser Console**, right-click the instance of the local Service Assurance Manager server in the InChargeDomain class.

A submenu appears.

3 Click **Disable Maintenance**.

Scheduling bulk maintenance

At times, you might want to schedule multiple devices and groups for maintenance. You can schedule multiple devices and groups for maintenance using a text file (for use with the bulk maintenance adapter) or an XML file (to be used with the sm_config functionality). When a group is scheduled for maintenance, a schedMaint notification for the group is created, resulting in all the members of the group being scheduled for maintenance.

Scheduling bulk maintenance using a text file

To schedule bulk maintenance using a text file:

1 Open a text editor.

2 Create a file with the format:

```
ClassName InstanceName startDate startTime endDate endTime
# This is the input file for bulk maintenance
# Hosts to be scheduled for maintence are
Host    MAJOR-WIN2K-VM  06-23-2009  16:00   06-23-2009  18:59
Host    USENSMAJORL2E   06-23-2009  16:00   06-23-2009  18:59
# The following group is scheduled for maintence
SelectiveGroup HGRP-TL/G1 07-09-2009  11:58   07-15-2009  16:57
```

3 Save and exit the file.

4 Upload the file to the server.

Loading the bulk maintenance text tile provides detailed information for uploading the text file to the server.

Loading the bulk maintenance text tile

To load the bulk maintenance text tile:

1 Open a **Command Prompt** window.

2 Change directory to the smarts/bin directory.

3 Type the following command:

```
t Sm_adapter -s samserver --file=fileName --output=outputfileName ../rules/ics/ics-bulk-maint.asls
“In maint, based on group HGRP-TL/G1, until 7-15-2009 16:57”
```

Scheduling bulk maintenance using an XML file

To schedule bulk maintenance using an XML file:

1 Open an XML editor.

Note An XML template file, bulk-maint-sample.xml, is located in the conf/ics directory.

2 Create a file with the format:

```
<?xml version="1.0" encoding="iso-8859-1"?>
<!DOCTYPE ics_config SYSTEM "ics-config.dtd">
<ics_config version="2">
   <maintconfig className = "Host" instanceName = "hostb"
      startYear = "2009"
      startMonth = "7"
      startDay = "11"
      startHour= "10"
      startMinute= "20"
      endYear = "2009"
      endMonth = "7"
      endDay = "11"
      endHour= "12"
      endMinute = "20"/>
</ics_config>
```

3 Save and close the file.

Note Save the file in the local/conf/ics directory.

4 Upload the file to the server.

Loading the bulk maintenance XML file provides detailed information on uploading the XML file to the server.

Loading the bulk maintenance XML file

To load the bulk maintenance XML file:

From a **Command Prompt** window, type the following command:

```
sm_config -s <SAMserverName> import -force <xmlfileName>
```

The output from running the command is added to the SAM server log file.

Scheduling bulk maintenance for port and interface components

You schedule bulk maintenance for port and interface components by specifying the component's SystemName, the device instance name, in either a text file or an XML file.

Scheduling bulk maintenance for port and interface components using a text file

To schedule bulk maintenance for port and interface components using a text file:

1 Open a text editor.

2 Create a file with the format:

```
ClassName InstanceName startdate startTime enddate endTime SystemName
# This is the input file for bulk maintenance for ports and interfaces
# Ports to be scheduled for maintence are
Port abc 08-05-2009 16:00 08-05-2009 19:00 router1
```

3 Save and exit the file.

4 Upload the file into the server.

Loading the bulk maintenance text tile provides detailed information for uploading the text file to the server.

Scheduling bulk maintenance for port and interface components using an XML file

To schedule bulk maintenance for port and interface components using an XML file:

1 Open an XML editor.

2 Create a file with the format:

```
<?xml version="1.0" encoding="iso-8859-1"?>
<!DOCTYPE ics_config SYSTEM "ics-config.dtd">
<ics_config version="2">
 <maintconfig className = "Port" instanceName = "abc"
      startYear = "2009"
      startMonth = "7"
      startDay = "26"
      startHour= "10"
      startMinute= "00"
      endYear = "2009"
      endMonth = "7"
      endDay = "28"
      endHour= "16"
      endMinute = "00"
      systemName = "router1"/>
</ics_config>
```

3 Save and close the file.

4 Upload the XML file to the server.

Loading the bulk maintenance XML file provides detailed information on uploading the XML file to the server.

Unscheduling bulk maintenance

If errors exist in the maintenance schedule, you might want to unschedule the devices from maintenance. If the devices to be unscheduled from maintenance have not entered their maintenance period, their corresponding schedMaint notification is archived. If the devices to be unscheduled from maintenance have entered their maintenance period, unscheduling the devices clears their corresponding InMaint notification and all the related notification's InMaintenance attributes are set to false. If maintenance period for the devices to be unscheduled from maintenance has passed, unscheduling the devices from maintenance has not effect on their corresponding notifications.

Unscheduling bulk maintenance using a text file

Use the text file containing the original maintenance entries you want to remove from maintenance when removing devices from maintenance. Define the variable, removeSchedMaint, using the -D sm_adapter option.

To unschedule bulk maintenance using a text file:

From a **Command Prompt** window, type the following command:

```
t Sm_adapter -s SAMServer -DremoveSchedMaint=true --file=fileName ../rules/ics/ics-bulk-maint.asl s
```

Unscheduling bulk maintenance using an XML file

To unschedule bulk maintenance using an XML file:

1 Open the original XML file containing the device entries you want to remove from maintenance in an XML editor.

2 Type the following line in the first device entry:

```
removeSchedMaint = “TRUE”
<?xml version="1.0" encoding="iso-8859-1"?>
<!DOCTYPE ics_config SYSTEM "ics-config.dtd">
<ics_config version="2">
   <maintconfig className = "Host" instanceName = "hostb"
      startYear = "2009"
      startMonth = "8"
      startDay = "11"
      startHour= "10"
      startMinute= "20"
      endYear = "2009"
      endMonth = "8"
      endDay = "11"
      endHour= "12"
      endMinute = "20"
      removeSchedMaint = “TRUE”/>
     <maintconfig className = "Router" instanceName = "10.9.131.17"
      startYear = "2009"
      startMonth = "8"
      startDay = "16"
      startHour= "13"
      startMinute= "00"
      endYear = "2009"
      endMonth = "8"
      endDay = "16"
      endHour= "14"
      endMinute = "20"/>
</ics_config>
```

3 Save and close the file.

Note Save the file in the local/conf/ics directory. An example XML file, bulk-maint-sample.xml, is located in the conf/ics directory.

4 Reload the XML file into the server.

Loading the bulk maintenance XML file provides detailed information for loading the XML file into the server.

Scheduling repair time

The Repair Time dialog box is accessed from a root-cause notification. The Repair Time dialog box allows you to type an estimated repair time and have it display in a notification field. Any notifications that are caused by the selected notification also get the specified repair time.

The console does not support Repair Time as one of the standard default Notification Console columns. However, you can configure one of the User Defined columns to include this information.

To access the Repair Time functionality, your administrator should configure one of the User Defined Notification Log Console columns to display the heading "Repair Time". Your administrator must enable the Schedule Maintenance Administration console operation for each user profile permitted to display the Repair Time dialog box. The “Modifying a notification list” section of the VMware Smart Assurance Service Assurance Manager Configuration Guide provides detailed information.

Note Repair time data is for informational purposes only.

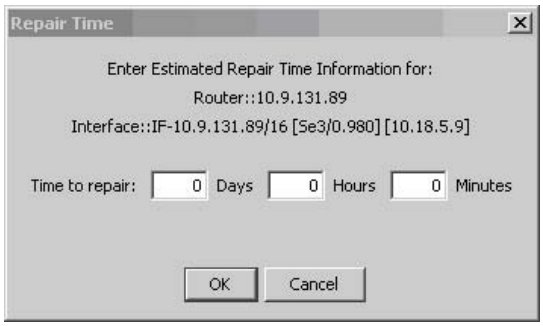
To schedule repair time for a managed element:

1 In the **Notification Log Console**, right-click a notification.

2 Select **Repair Time**.

The **Repair Time** dialog box appears, as illustrated in Repair Time dialog box.

Figure 9-4. Repair Time dialog box



3 Type the amount of time the repair will take to be complete.

4 Click **OK**.

The Repair Time notification field displays the time when the repair is expected to be completed.

About tools

A tool is a program that you can invoke in response to a notification or for a topology element. Such an action might be to ping or to Telnet to the affected system, or to open a trouble ticket for a specific notification.

The Global Console supports these types of tools:

- Server tools are executed by the Global Manager and are available to any console that attaches to the Global Manager.

  In console shortcut menus, the server tools are listed in the Server Tools submenu.

  Server actions are also recorded as entries in the server's audit log.

- Client tools are executed by the Global Console and are available to locally installed consoles.

  In console shortcut menus, the client tools are listed in the Client Tools submenu.

  Note Some tools prompt for runtime user-specified parameter values. If multiple instances are selected when you launch these tools, the Specify Options for get properties tool dialog box includes an option allowing you to specify values once and apply the specified values to all selected objects. With this option selected, you only need to type the runtime parameters once for all selected objects.

  Your administrator can configure tools for server or client execution. For example, some available tools include:

- Ping
- Telnet
- Trouble tickets, opening and closing (server only)
- Email
- Pager message
- LSP Ping
- Launch ADM Web Console
- Get SCM Alert Details
- Get SCM Server Details

  Note The Get SCM Alert Details and the Get SCM Server Details tools are only available from Global Consoles accessed through Internet Explorer.

  In addition, your administrator can modify these sample tool programs, provided by VMware, Inc., and rename the menu options that appear in your consoles:

- Sample—Ping, Ping Interface, Ping Device, Ping All
- Sample—Telnet

- Sample—Open Trouble Ticket
- Sample—Close Trouble Ticket

The following sections describe how to use Ping and Telnet, open and close trouble tickets, display the Tool Output window, and use Email, pager message, and their recipients dialog box.

Using ping and telnet

The tools ping and telnet are available from the Global Console. To invoke either tool:

1 Right-click one of the following selections:
   - A notification in the **Notification Log Console**
   - A map icon in the **Map Console**
   - A managed element in the topology tree of the **Topology Browser Console**

2 Select a tool from the shortcut menu.

   Server tools are listed under the Server Tools submenu.

   Client tools are listed under the Client Tools submenu.

   Note These submenus only display if the tools are configured and are relevant for the selected entity.

   Menu option names for these tools may have been modified by your administrator.

Opening and closing trouble tickets

Trouble tickets are sometimes used to track notifications while the operators are working on them. If the trouble ticket tools (Open and Close programs) are configured by your administrator, you can open a trouble ticket (insert a Ticket ID number) for a notification or close a trouble ticket.

To open and close a trouble ticket for a notification, use the tools Open Trouble Ticket and Close Trouble Ticket, respectively.

Note Menu option names for these tools may have been modified by your administrator.

Opening a trouble ticket

To open a trouble ticket:

1 Right-click a selected notification in the **Notification Log Console**.

2 In the shortcut menu, select **Server Tools** > **Open Trouble Ticket**.

Closing a trouble ticket

To close a trouble ticket for a notification:

1 Right-click a selection.

2 In the shortcut menu, select **Server Tools** > **Close Trouble Ticket**.

Using the Tool Output window

Viewing tool output depends on the tool's configuration. Typically, the output displays in the Tool Output shortcut window, which opens when the tool is invoked.

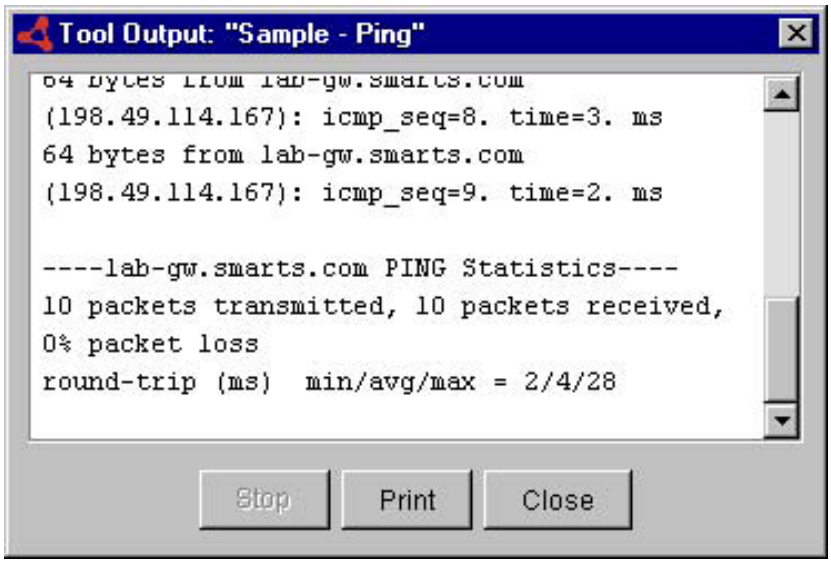
In the Tool Output shortcut window, the buttons are:

- Stop — Stops the tool program while it is running.
- Print — Prints the output to your default printer.
- Close — Closes the window after the tool program completes processing or is stopped; you cannot close the window while the tool is running.

  If the tool produces an error, a message is displayed in the window. (For Server tools, an error message is displayed in the window on the host where the console is running.)

  For example, Example of a Tool Output window displays the result for the Ping tool when it is invoked for a router notification.

Figure 9-5. Example of a Tool Output window



Email, Pager Message, and their recipients dialog box

The tools Mail and Pager are available in the Notification Log Console.

To invoke either tool:

1 Right-click a selected notification in the **Notification Log Console**. (To include multiple notifications in your message, press the **Ctrl** key while making your selections.)

  You can right-click the selection regardless of its state (active or inactive): A cleared problem can be as important as a problem that has occurred.

2 Select **Mail** or **Page** in the shortcut menu.

   This displays the **Mail Action** or **Pager Action** dialog box.

3 In the dialog box, fill in the fields. The **Mail Action** *and* **Pager Action** dialog boxes are the same, except for the **Mail Subject** field and the resulting action.

   The dialog box fields are:

   - **Manager** — Is the Manager for the recipients listed in the To field. If you are attached to multiple Managers, select one.
     - **To** — Designates a recipient for the action. You must select a recipient. If you need to send an action to someone who is not listed, click **Configuration** to display the **Recipients Editor** dialog box and add the person to the list.
     - **Subject** — Identifies the subject of the email message. You can change it if you wish.
     - **Message** — Is the body of the email or pager message. The message text includes the event and related notification attributes. This is not always enough information, however, for the person receiving the message. You may wish to add a brief note that provides more information about the event.

4 Select the recipient.

   If you open a Mail or Pager Action dialog box and the To section does not initially list recipients, you need to create a distribution list of recipients. Preparing a distribution list includes instructions.

5 Click **OK** to apply your changes and send the email or pager message.

Note The mail action uses the industry-standard SMTP for email. In the Recipients Editor dialog box, you need to verify the values in the Mail server and Sender email address section that define the values for the mail services running at your site.The pager action requires a shell script, provided by your systems administrator, to access the pager software. Your administrator needs to create a script named pager.sh in the BASEDIR/smarts/local/actions directory.

Preparing a distribution list

The Recipients Editor dialog box enables you to create a list of people to receive email or pager actions.

To open the Recipients Editor dialog box, select **Edit** > **Recipients** or click **Configuration** in an open **Mail Action** or **Pager Action** dialog box.

The Recipients Editor dialog box is divided into four sections:

- Manager section lists the Manager for the recipients. If you are attached to multiple Managers, select one.
- Current Recipients section lists the recipients for a selected Manager. To delete an entry from the list, select it and click **Delete**. (To select multiple entries, press **Ctrl** while making your selections.) Click **OK** to apply your changes.
- The Recipient Information section is where you add new recipients to the list or change existing information.

- Mail server and Sender e-mail address section. The information in this section must be correct in order to successfully send email. You can change the mail server name and email address:
  - The Mail server field must be set to the hostname where the mail services are running and should match the value specified by your system administrator in the Service Assurance Manager's configuration. The default value is localhost.

    If you specify a mail server name in the Recipients Editor dialog box that is different from the configuration value, the value in the dialog box temporarily overrides the configuration value. To change the name permanently, contact your administrator.
  - The Sender email address field identifies the operator who is sending the email. By default, it displays your email information.

Adding a recipient

To add a recipient in Recipients Editor dialog box:

1. From the **Manager** list, select the manager where you want to save the recipient.
2. Provide the recipient's name.
3. Add the recipient's email address or pager number. When you choose an action, the appropriate phone number or email address is sent to the pager or email software.
4. Supply a password if it is required to send a pager message. The password value is passed as a parameter to the pager script.
5. (Optional) Add a description for your records.
6. Click **Apply** or **Create**. The new recipient appears in the list of **Current Recipients**.
7. Click **OK** to apply your changes.

Launching an ADM web console

Use the Launch in Context functionality to open an Application Discovery Manager (ADM) Console in context. The ADM Console includes functionality to display detailed information about selected objects populated into the Service Assurance Manager as a result of the integration with ADM. The Launch ADM Web Console tool is available from the Map Console.

Note The *VMware Smart Assurance Application Discovery Manager Integration Guide* provides detailed information.

To launch an ADM web console:

1. From the **Map Console**, right-click an object.

   The shortcut menu displays.
2. Select **Client Tools**.
3. Select **Launch ADM Web Console**.

   The ADM web console appears.

Viewing SCM alert and server details

When the Service Assurance Manager is integrated with the Server Configuration Manager (SCM), the Global Manager can receive alerts from SCM, allowing you access to SCM reports listing the Change and Compliance alerts collected by the SCM for machines monitored by the Service Assurance Manager.

Note The *VMware SCM Integration with VMware Smart Assurance Configuration and User Guide* provides detailed information on configuring the integration between the Service Assurance Manager and SCM and viewing detail reports.

To view SCM alert and server details:

1 Right-click a Change or Compliance alert in the **Notification Log Console**.

2 In the shortcut menu, select **Client Tools**.

3 Select one of the following:

- **Display SCM Alert Details** — To display Alert Details Reports.
  - **Display SCM Server Details** — To display the Server Details Reports.

    The report displays in a Report Viewer.

    Note The Display SCM Alert Details and the Display SCM Server Details tools are only available from Global Consoles accessed through Internet Explorer.

Saving and recording information

In addition to acting upon notifications or the state of icons in maps, you may need to add comments to audit logs, save notification information and maps, and print tool output and maps.

Adding comments to a notification's audit log

Sometimes for documentation purposes, you may need to add comments to an audit log for a specific notification. For example, you may want to log a summary of actions taken to solve a problem or list pending issues for the operators on the next shift. The inserted entries cannot be edited or deleted and they are archived as part of the audit log. Append new item to Audit Log dialog box shows an example.

To add comments:

1 In the Notification Log Console, right-click a notification.

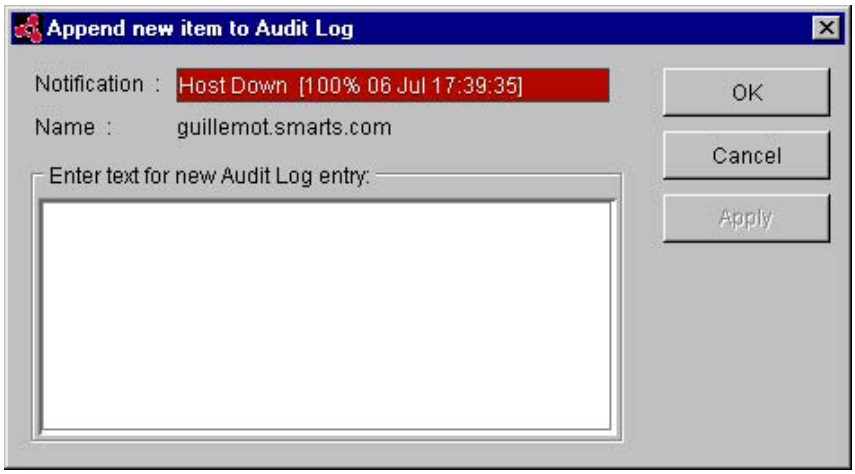
The notification shortcut menu appears.

2 Click **Add to Audit Log**.

Note Alternatively, select **Event** > **Add to Audit Log** from the console's menu bar.

The **Append new item to Audit Log** dialog box displays.

Figure 9-6. Append new item to Audit Log dialog box



3 Type your comments for one entry and click **OK**. For more than one entry, click **Apply** after each entry, then click **OK** when you are finished.

An alternate method for opening the Append new item to Audit Log dialog box is to open the Notification Properties dialog box.

To open the Notification Properties dialog box:

4 In the Notification Log Console, right-click a notification.

The notification shortcut menu appears.

5 Click **Properties**.

Note Alternatively, select **Event** > **Properties** from the console's menu bar.

6 Select the **Audit Log** tab.

7 Click **Add to Audit Log**.

â€œDisplaying notification propertiesâ€• on page 62 includes additional information about the Notification Properties dialog box.

Saving Notification Log information

You can save the contents of a Notification Log view. The information is stored locally as an ASCII file. Each row of information is saved as a separate line of text in the file. The resulting file can be imported into other applications such as a spreadsheet program or printed.

To save notification information, in a Notification Log Console, select **Log** > **Save log** contents to file or right-click the view title and select Save Log Contents to File from the shortcut menu.

In the Save log contents to file dialog box, you can choose format settings and a location for the file.

The Save log contents to file dialog box is divided into four sections and a Save location field:

- Field delimiter — Separates each field within a line using a tab character or a user-specified character such as vertical bar (|). To specify a custom delimiter, click the Use custom delimiter option and specify the character; tab is the default.
- Column headers — Includes column headers as the first line. To exclude the headers, clear the Include column headers checkbox.
- Columns to include — Includes columns that are visible, which is the default, or all columns.
- Notifications to include — Includes all notification rows, which is the default, or only selected rows.
- Save location — Specify a directory path and filename, including the file extension (.txt). If you do not specify a path, the file is saved locally to the *BASEDIR/smarts/local/logs* directory by default. Or, you can click Browse and choose a location in the Select filename dialog box.

  Click **OK** or **Apply** to create the text file. If the file already exists, its contents are overwritten.

Saving audit log and containment information

You can save the contents of an audit log and a selected table of the Containment dialog box. The information is stored locally as an ASCII file. Each row of information is saved as a separate line of text in the file. The resulting file can be imported into other applications such as a spreadsheet program or printed.

To save the information, you can:

- In the **Audit Log** tab of the **Notification Properties** dialog box, click **Save table to file**.
- For a selected tab in the **Containment** dialog box, click **Save Table**.

  In the Save table to file dialog box, you can choose format settings and a location for the file.

  The Save table to file dialog box is divided into two sections and a Save location field:

- Field Delimiter — Separates each field within a line using a tab character or a user-specified character such as vertical bar (|). To specify a custom delimiter, click the Use custom delimiter option and specify the character; tab is the default.
- Column Headers — Includes column headers as the first line. To exclude the headers, clear the Include column headers checkbox.
- Save location — Specify a directory path and filename, including the file extension (.txt). If you do not specify a path, the file is saved locally to the *BASEDIR/smarts/local/logs* directory by default. Or, you can click Browse and choose a location in the Select filename dialog box.

  Click **OK** or **Apply** to create the text file. If the file already exists, its contents are overwritten.

Saving a map

You can save a map of each map type for each instance in the map tree. The purpose of saving a map is to override the default map of the selected type (for example, Group Membership or VLAN Connection) for a specific device, IP network, VLAN, group, service, or application.

To save a map, in the Map Console, select **Map** > **Save Map**. Click **OK** to acknowledge the informational message that displays the location of the saved map. The map is saved in the *BASEDIR/smarts/consoles/<userid>* directory on the host where the Global Manager is running.

Some changes you make to the map before saving are also saved. These changes can include:

- Adjusted scope (for example, expanded nodes)
- Node positions
- Layout type (circular, hierarchical, or manual)
- Filtered classes
- User-defined backgrounds
- Zoom level

  If you use the Color-by-Root-cause toolbar button (tool tip labeled Toggle Root Cause Coloring) to color a map, the map coloring is not saved.

  If the topology changes after a map is saved, the changes are applied to the information displayed in the map view when the map is redisplayed. (The saved map is updated only when the updated map is saved.)

  If you save a map that already exists in your userid directory for a specific element and map type, it is replaced.

  When you click a managed element in the map tree, the Global Console queries the Global Manager for a saved map in the following order:

  a The Global Manager checks your remote directory, the *BASEDIR/smarts/local/consoles/<userid>* directory, for any saved maps for that element. If a saved map exists, it displays.

  b If there is no saved map in your user directory, it then checks for a shared, saved map in the *BASEDIR/smarts/local/consoles* directory on the host where the Global Manager is running.

  c If a saved map exists in the /consoles directory for the selected element, it displays. If no map exists, then the Global Console uses the default map for the selected element.

Sharing a saved map

To share a map saved in your directory with other users, in a UNIX shell, copy the saved map file from your *BASEDIR/smarts/local/consoles/<userid>* directory to the *BASEDIR/smarts/local/consoles* directory on the host where the Global Manager is running. Once the saved map has been copied to this directory, all users of the Domain Manager have access to view the saved map. The map file naming convention is described below.

Note Write permission to the remote host directory is required for the copy operation.

To share a saved map with only selected users, copy the saved map file to the *BASEDIR/smarts/local/consoles/<userid>* directory of each user who is to share the map.

Map file naming convention

Maps are automatically assigned filenames by the Global Manager when they are saved. The filename given is a combination of the Global Manager name, the instance name, and the map type represented by a number. The suffix of the filename is icsvm. *Table 22 on page 144* lists the numeric representation for each map.

For example, an INCHARGE-SA Global Manager Physical Connectivity map of router moto-gw is assigned the filename:

```
INCHARGE-SAmoto-gw1.icsvm
```

Printing a map

To print a map, in the Map Console, select **Map** > **Print Map**. In the window, you can select the following buttons:

- Print — Prints your map. The Print dialog box for your default printer displays. Check your settings for paper orientation and resolution if necessary. Click **OK**.
- Print Setup — Enables you to format your map as follows:
  - To print the whole map with all nodes, select the **Print Entire Graph** option.
  - To print the portion of the map that appears in the Map window, select the **Print Current Window** option.
  - To print selected elements that you have selected in the map, select the **Print Current Selected** option.
  - To title the print, type the name in the **Caption** box, ensure that the **Print Caption** checkbox is selected. You can format the title using the **Font** button and the **Position** list box.

    Also, you can format the print using the Margins, Multipage Printing and Other options.

    Click **OK**.
- Zoom In and Zoom Out — To scale the map view.
- Fit In Window — Fits the map to the size of the panel.
- Close — Closes the window.

Printing Tool Output

When you invoke a tool such as Ping or Open Trouble Ticket from the Global Console, the output usually displays in the Tool Output shortcut window.

To print the output:

1. Click **Print** . The **Print** dialog box for your default printer displays.
2. Check your settings for paper orientation and resolution if necessary.

3 Click **OK** .

Using the Tool Output window *i*ncludes additional information about tool output.

HyperNotif Statistics

HyperNotif Statistics is a debug tool that reports two specific kind of notification data, namely Client Statistics and Server Statistics.

- Client Statistics — With respect to a Service Assurance Manager server, Client Statistics provides the notification data statistics for notifications received from the underlying Service Assurance Manager server.

  Note If the underlying Domain Manager is not a Service Assurance Manager 8.0 or later, then the data will not be available as there are no HyperNotif transactions. In such cases, use the debug tool **dmdebug ---queues**.

- Server Statistics — With respect to a Service Assurance Manager server, Server Statistics provides notification data statistics for notifications sent to each of the HyperNotif client connected to the Service Assurance Manager server. The HyperNotif Client can be:
  - Service Assurance Manager Console
  - Service Assurance Manager (Presentation server), under which lies this Service Assurance Manager (Aggregate server).

Command

The command to run the HyperNotifStatistics tool:

```
#dmctl  -s <server name> invoke ICS_NLManager::ICS-NLManager reportHyperNotifStats
```

Sample output

```
SA-9.0_NL-Driver-HyperNotif     [1 worker(s)]
Current Size 0 , max 0; processed entries 0
SM_ProtocolEngine-1 19527 SA    [1 worker(s)]
Current Size 0 , max 27; processed entries 32
SM_ProtocolEngine-4 3340 IC Console - V9.1.0.0  [0 worker(s)]
Current Size 0 , max 26; processed entries 29
```

In the output:

- *SA-9.0_NL-Driver-HyperNotif* — Indicates the name of the thread along with the number of workers, which is the number of threads in the process.
- *Current size* — Indicates the current size of the queue.
- *Max* — Indicates the maximum size of the queue, at any point in time. This is a historical data.

- *Processed entries* — Indicates the total number of entries processed.

  Note The HyperNotif Connections are cleaned up only after 45 minutes of inactivity. Therefore, the stale connections will be reported for that duration. For example, if a Service Assurance Manager Console is detached, or if a Console is closed, and the command is run, then the output will still show the stale connections.

Customizing Your Console

10

The Global Console can be customized according to an operator's preferences. This chapter describes how to change the appearance of your console, customize it with views, and save the customized console. Two examples of consoles illustrate these customization options.

This chapter includes the following topics:

- Changing the console appearance
- Adjusting Java properties
- Tailoring your console with views
- Saving a console

Changing the console appearance

This section describes how to control the display of the toolbar buttons and status bar, the layout of multiple views, and how to revise the text in a console title bar.

Hiding the toolbar and status bar

In a Global Console, toolbar buttons are located below the menus and the status bar is located at the bottom of the console. You can control the display of the toolbar and status bar. For example, if you prefer to work without toolbar buttons, you can hide them:

- To hide the toolbar, select **View** > **Toolbar** to clear the Toolbar option.
- To hide the status bar, select **View** > **Status** to clear the Status option.

  To re-display the hidden bar, reselect the appropriate option in the View menu.

Changing the console layout of views

If your console consists of multiple views, you can change the console layout by rearranging the views. To change the layout of a console:

1 Select **File** > **Layout** to display the **Console Layout** dialog box. In the Console Panel Layout section of the dialog box, two list boxes appear:

- **Panel** determines which panel the Tile operation affects.
  - **Tile** controls how multiple views in a panel are displayed. Right To Left places the views in a row. Top To Bottom stacks them one on top of the next.

2 Click **OK .**

Note You can also change the console layout while you are adding or copying views to a current console. In the Add View or Copy View dialog boxes, use the Console Panel list box. Adding a view or Copying a view in a current console provides additional information.

Changing the title of a console

If you want, you can revise or replace the console title. To change the text in the title bar of a console:

1 Select **File** > **Layout** to display the **Console Layout** dialog box.

2 In the **Title** field, type the new console name.

3 Click **OK .**

Adjusting Java properties

The -D option for the sm_gui command enables you to adjust specific Java properties that affect the Global Console. For example, you can control the display of text for toolbar buttons, maps, and the font that displays throughout the console. You can also redefine the Java log file location and specify the connection timeout for the console.

Command syntax for the -D option

You can specify the sm_gui command with -D parameter options from UNIX command line. You can also use sm_edit to add properties in the BASEDIR/smarts/conf/console/properties.conf file. When properties are added to the properties.conf file, the -D parameter options are not used. The tutorial information included in the properties.conf file provides additional information.

The -D option for the sm_gui command is:

```
tsm_gui –Dproperty1=value1 –Dproperty2=value2–D ...
–Dpropertyn=valuen s
```

Specify the -D option for each property/value pair. For example, to change the font to Arial and set the font to 20 points, specify:

```
sm_gui -Dcom.smarts.font=Arial -Dcom.smarts.fontSize=20
```

Properties and their acceptable values are listed in Properties and their values.

Table 10-1. Properties and their values

Property	Acceptable value	Description
com.smarts.securityMessage	string	Defines the name of the ASCII file containing the security warning message. **Note** The file must be located in the directory where the HTML and properties files are located.
com.smarts.server.logMessages	true or false	True — Causes the server to write messages to the server log file. False — Does not cause the server to write messages to the server log file. **Note** The ServerMesg_<*userid*>.log is created when the com.somarts.server.logMessages parameter is set to true. This log contains all sever events associated with a specific user. For example, if UserA is logged onto the system and the com.smarts.server.logMessages parameter is configured to true, messages would be written to SeverMesg_UserA.log.
com.smarts.mapNodeText.font	string	Allows the user to define the map icon font. **Default value**: Helvetica
com.smarts.mapNodeText.fontSize	integer	Allows the user to define the map icon font size. **Default value**: 12 point
com.smarts.connectionTimeout	integer (in seconds)	This property indicates the maximum amount of time that the console will wait for the Manager pulse check (the upTime attribute) to respond. If there is no response within the specified time, the console disconnects from the Manager. The default is 300 seconds (5 minutes). Any integer between 1 - 89 is changed to a minimum value of 90. Zero (0) or any integer below disables the timeout.
com.smarts.font	string	Enables a user-specified font to display throughout the Global Console. The font must be a Java-supported font appropriate for the operating system or it is ignored. The font should reside in the directory location as described by Java documentation.
com.smarts.fontSize	integer	Enables a user-specified font size to display throughout the Global Console. The font size must be compatible with the com.smarts.font property or it is ignored.

Table 10-1. Properties and their values (Continued)

Property	Acceptable value	Description
com.smarts.java.log	fully qualified filename	If specified, the Java log contents are saved to the specified file. (The default is no file specified.)
com.smarts.informs	user-defined field	If specified, this property controls which underlying Managers are accessible by using Browse Detail from the Notification Log view. A user-defined field must be configured to contain the names of the underlying Managers. The VMware Smart Assurance Service Assurance Manager Configuration Guide includes information about customizing user-defined notification attributes.
com.smarts.map.showAllBusiness	true or false	True — Shows all nodes and edges in a Business Services map, including those that are not part of paths that originate from or terminate at the map central node. (This is the default.) False — Shows the nodes and edges in a Business Services map that either originate from or terminate at the map central node.
com.smarts.map.showNormalBanner	true or false	True — Shows map nodes with the status of Normal with a green color bar underneath the icon. False — Shows map nodes with the status of Normal without a green color bar underneath the icon. (This is the default.)
com.smarts.mapBackgroundColor	string	Enables you to specify a single background color for all maps. This parameter overrides the default color for all map types. Note that if the setting you enter is invalid, the background color for all maps will be white. Use a six-character string, RRGGBB, where RR is a hexadecimal value between 00 and ff (= 0 to 255), specifying the red component; GG specifies the green component; and BB specifies the blue component. For example, to specify the beige color called “antique white” in Netscape, the string is: com.smarts.mapBackgroundColor=FAEBD7 Map background colors includes information on default background colors.
com.smarts.maxFilterInstances	integer	Enables you to change the maximum number of instances that will automatically display in the Topological Filter tab. 50 is the default. If a class has more instances than the maximum number, you need to click Get instances to retrieve a list.
smarts.maps.maxGroupMembers	a positive integer	A positive integer. This is the maximum number of members of a leaf group that will display for a Group Membership map *without* a prompt dialog box. The dialog box prompts the operator when there is a large number of members to display. 100 is the default.

Table 10-1. Properties and their values (Continued)

Property	Acceptable value	Description
com.smarts.maxTopoInstances	integer	Enables you to change the maximum number of instances that display for a class or relationship in the Topology Browser. The default is 1000. VMware, Inc. recommends not changing the default unless it is necessary because it affects performance and usability.
com.smarts.viewer.hideToolbarText	true or false	True — Hides the display text for the toolbar buttons. (This is the default.) False — Shows the text for the toolbar buttons.
com.smarts.viewer.map.disableMaps	true or false	True — Disables the display of maps. False — Does not disable maps. (This is the default.)
smarts.allowBGjpegs	true or false	True — Allows map background files to be saved in jpeg (.jpg) format. False — Does not allow map background files to be saved in jpeg format.
com.smarts.disable_keepalives	integer	Enables you to disable KeepAlive messages for the Global Console. Specify a non-zero number to disable KeepAlive messages. Zero (0) enables KeepAlive messages.
com.smarts.log.level	option	Defines the level of messages written to the console java log. Options include: ■ FATAL ■ SEVERE ■ SERIOUS ■ DEFAULT (default option) ■ WARNING ■ INFO ■ CONFIG ■ DEBUG ■ TRACE **Note** Options are listed in order from display least information to display most information.
com.smarts.securityEnabled	true or false	True — Enables security. (This is the default when the sm_gui.exe is executed.) False — Disables security. **Note** This property must be specifically declared and set to true in the Web Console and in the viewlets.
smarts.remote.broker	host:port	Defines the default broker for domain attach dialog boxes.
com.smarts.writeable	path string	Defines the location of console logs.

Table 10-1. Properties and their values (Continued)

Property	Acceptable value	Description
com.smarts.debugConnection	true or false	True — Causes the server to write all console operation invocations received from the console to the server log file. False — Does not cause the server to write console operation invocations received from the console to the server log file.
com.smarts.highLatency	true or false	True — Reduces the number of calls to the server to obtain property values. Returns larger packets of data containing bundled property values. False — Smaller multiple calls are sent to the server to obtain multiple property values. The highLatency parameter can be added to any Service Assurance Manager related dxa configuration file used to import data from an underlying server that is part of a high latency network environment. Examples of applicable dxa configuration files include dxa-conn.conf, dxa-sam.conf, and dxa-oi.conf. For the majority of configurations, the highLatency parameter will apply to the presentation Service Assurance Manager server (dxa-sam.conf) when the underlying aggregation Service Assurance Manager server is remotely located. **Note** Before updating the dxa-conn.conf file, back up the file.
com.smarts.user.timezone	timezone name	Causes the console to format all times and timestamps according to the specified time zone. Examples of acceptable values are: PST for U.S. Pacific Standard Time and GMT for Greenwich Mean Time. The default is the time zone where the console is running. Class TimeZone at the Java website includes additional information. **Note** Older versions of the console used the Java user.timezone parameter to change the time zone, but the user.timezone parameter does not work with the Web Console or Java Web Start.

Table 10-1. Properties and their values (Continued)

Property	Acceptable value	Description
com.smarts.timestampFormat	pattern-format string	Overrides the default formatting of timestamps in the console, for example, the First Notify, Last Notify, and Last Change fields in the notification view. An example of the default format is 28 Mar 17:08:09. Using the new parameter, you can change this to a different format. The following examples illustrate different configurations of the com.smarts.timestampFormat parameter: ■ 03.28 17:08:09-0500 — Displays the local time zone offset from GMT. ■ 28 Mar 17:08:09 EDT — Displays the local time zone as text. ■ 07.03.28 17:08:09 — Displays the year. To configure the com.smarts.timestampFormat parameter, enter a Java SimpleDataFormat pattern-format string as the value of the parameter. The format language for constructing the pattern string is specified in the Java J2SE 5.0 documentation, available from the Sun website, in the description of the java.text.SimpleDateFormat class. For example, the console's default timestamp format is: dd MMM HH:mm:ss. The alternative formats illustrated above have the following pattern strings: ■ "03.28 17:08:09-0500" "MM.dd HH:mm:ssZ" (to display the local time zone offset from GMT) ■ "28 Mar 17:08:09 EDT" "dd MMM HH:mm:ss z" (to display the local time zone as text) ■ "07.03.28 17:08:09" "YY.MM.dd HH:mm:ss" (to display the year) **Note** Characters in the format string are case sensitive: "Z" means something different and will produce different strings than "z".
com.smarts.oldGetMap	true or false	Defines whether the console retrieves map data as a string or as formatted data. If set to true, the console retrieves map data as formatted data. **Default value**: False
com.smarts.getMap.timeout	integer	Defines the time, in seconds, that the Get Map function tries to retrieve map data before the function times out. Once the Get Map function times out, the Get map timed out message appears. **Default value**: 120

Table 10-1. Properties and their values (Continued)

Property	Acceptable value	Description
com.smarts.clientTool.setEnv	true or false	Defines the method of passing parameters to client scripts. If configured to true, the console directly loads parameters passed to the client script into the environment. If configured to false (or when a value is not specified), the console passes parameters to the client scripts as command line arguments and requires the client script to parse the parameters to load them into the environment. **Note** Setting this property to false is backward compatible for existing scripts that parse the command line parameters and create environment variables. When this property is set to true, the script does not receive any command line parameters to parse, because the properties already exist as variables in the environment, *as if* the script had parsed and set them but without the script actually having to do so.
com.smarts.fasttopologybrowse	option	Defines whether the topology browser performance is enhanced for displaying related instance information. Options include: ■ Off — Default value ■ On — Speed up enhancement is activated with instance information sorted ■ Nosort — Speed up enhancement is activated with instance information not sorted **Note** When configuring this property to nosort, relation information displays more quickly in the topology tree in high latency environments because instance names are not sorted. When many related instances for a class are displayed, specific instances may be difficult to locate because instance names beginning with identical characters may not be grouped together. For example, when this property is configured to nosort, not all router instances beginning with the characters Chicago may be displayed together.
com.smarts.showDomainConsistsOf	true or false	Defines whether the InChargeDomainConsistsOf relationship displays in the topology view. If configured to false, the InChargeDomainConsistsOf relationship does not display in the topology view reducing the possibility of the console not responding. If configured to true, all the information for the ConsistsOf relationship displays in the topology view. **Default value**: False

Increasing the Java heap space size

If the console runs out of memory, the maximum amount of heap space available to the console must be adjusted by specifying the -H (or --heapsize=) parameter to the sm_gui command.

The default heap allocation is 350 megabytes, which may not be sufficient for large or complex deployments. (The previous default heap space size was 256 megabytes.) As heap space becomes close to being fully allocated, the console tries to enter warning messages in the console's Java Message Log. But often, the memory is allocated in a single uninterrupted operation, resulting in no message being written to the console's Java Message Log. For example, during the initial loading of notifications at startup time, if there are more than 60,000 notifications to be loaded and the available heap space is less than 270 megabytes, the console may close down without any warning message. However, in this example if just enough space is available, the console may become unresponsive due to Java's attempts to find space in a garbage collection.

To increase the Java heap space size, allocate additional heap space. For example, to allocate 800 megabytes of heap space, type the following from the command line:

```
sm_gui -H800M <
other -D parameters ...
>
```

Tailoring your console with views

The Global Console is usually defined by one default view, console-specific toolbar buttons, and menus. However, the Global Console can consist of multiple views. The following console views are available: Notification Log, Map, Topology Browser, Summary, Status Table, Notification Properties, and Containment.

You can customize a console to display multiple views. For example, you can add a Topology Browser view to your Notification Log Console. Or, you can add three Notification Log views to a console; each view using a filter for specific notifications. Or, you can customize a Notification Log view and copy it in order to provide a consistent display and minimize your customization effort.

Note The following types of views, Notification Log, Topology Browser, Summary, Status Table, Notification Properties, and Containment, can be added, copied, or deleted in consoles. In the Map Console, the default Map view cannot be added, copied, or deleted. Also, a Map view cannot be added to a console. Unlike other types of consoles, there can only be one Map Console.

Availability of Dashboard viewlets includes additional information about which views are available through the Global Console, Web Console, Business Dashboard, and third-party Web Portal products.

Adding a view

To add a view:

1 Select **View** > **Add View**.

The **Add View** dialog box appears.

2 Click the **View Type** menu to list the available views. Select the view you want to add to the console. (A custom view is one that has been developed by a programmer to work with the Notification Log Console.)

3 Use the **Console Panel** list boxes to arrange views within the console:

- The **Panel** list box determines where the view appears within the console.
  - The **Tile** list box determines how multiple views within the same panel are arranged. Views that are oriented horizontally, such as Notification Log, usually display better when they are tiled Top To Bottom.

4 Click **OK .**

Note To add multiple views, reopen the **Add View** dialog box for each view you want to add.

Adding a custom view containing a Java component

To add a custom view containing a Java component in the console or in the Web console or dashboard:

1 Create a class derived from the component.

The component must be in a Java package that does not match any of the existing Java packages, for example, com.<*customercompanyname*>.

2 Create a jar file containing compiled class file(s).

The jar file is specified in the SM_CLASSPATH variable of the runcmd_env.sh. This variable can also be set in the individual command window. The fully qualified path of the jar file must be specified.

Example:

```
SM_CLASSPATH=C:\SAM-NEC4\SAM\smarts\local\classes\foreign.jar
```

3 From the console, select **View** > **Add View** > **Custom View.**

4 Type the full class path of the component in the **Custom View** field.

For example, if the component is compiled into the jar file as com.<*customercompanyname*>.Ourview.class, type com.<*customercompanyname*>.Ourview.

The component appears in a new view in the console.

Note To add a view containing a Java component for Java Web Start, you must have your private jar file signed with the VMware certificate. Java Web Start requires all jar files to be signed with the same certificate.

Copying a view in a current console

To copy a view in the current console:

1 Click the view you want to copy to activate it. The active view has a black border.

2 Select **View** > **Copy View** > **Copy View**. This displays the **Copy View** dialog box.

3 Use the **Console Panel** list boxes to arrange views within the console:

- The **Panel** list box determines where the view appears within the console.
  - The **Tile** list box determines how multiple views within the same panel are arranged. Views that are oriented horizontally, such as Notification Log, usually display better when they are tiled Top To Bottom.

4 Click **OK .**

Note This option is not available for the Map view.

Copying a view to a new console

You can copy the following views to a new console: Notification Log, Topology Browser, and Summary.

To copy a view to a new console:

1 Click the view you want to copy to activate it. The active view has a black border.

2 Select **View** > **Copy View** > **Copy View as new console**.

The new console displays over the existing console.

Note This option is not available for Status Table, Notification Properties, Containment, or Map.

Deleting a view

To delete a view from the console:

1 Click the view you want to delete to activate it. The active view has a dark gray border.

2 Select **View** > **Delete View**.

Saving a view as a dashboard viewlet

To save a view as a dashboard viewlet:

1 Select **View** > **Save View As dashboard viewlet**. The **Configure Save View as dashboard viewlet** dialog box displays.

2 Select the manager from the list.

3 Click either **Save for User** or **Save for Profile**, and then select a user or user-profile from the list.

4 Select or type a name in the **View Name** field.

5 Click **OK** after your last selection. This immediately applies the parameters to the view and closes the dialog box.

The VMware Smart Assurance Service Assurance Manager Dashboard Configuration Guide includes additional information on deploying dashboard viewlets.

Changing the title of a Notification Log view

To change the title of a Notification Log view:

1 Select **Log** > **Log Properties** to display the **Log Properties** dialog box.

2 In the **Title** field, type the new view name.

3 Click **OK .**

This is useful when you have multiple Notification Log views with different filtering criteria.

Context sharing concepts

You can set up context sharing so that a selected entity in one view determines the content that is displayed in one or more other views. For example, you can set up context sharing so that each time you select a notification in a Notification Log, a Map view displays a map for that notification. In this example, the Notification Log acts as a source, while the Map view acts as a listener. Without context sharing, you have to select a notification in the Notification Log, right-click, and select Show Map to display a map for each notification.

Views can participate in context sharing as sources, listeners, or both. To enable context sharing, you need to configure listening views as described in Setting up context sharing. Source and listening views can also exist in separate consoles.

Source views and elements for context sharing shows the views that can act as sources and indicates which entities you can select to change the content in listening views.

Table 10-2. Source views and elements for context sharing

Views that can act as sources	Entity to select
Notification Log view	Notification
Summary view	Summary **Note** When you select a summary as a source, the Notification Log configured as a listener displays the set of notifications associated with that summary.
Map view	Node or edge
Status Table view (source only)	One of the following classes on the y-axis: ■ ServiceOffering and subclasses ■ ServiceSubscriber and subclasses ■ HierarchicalGroup ■ SelectiveGroup ■ ApplicationGroup Any instance on the x-axis.
Topology view (source only)	Topology instance

The following views can act as listeners:

- Notification Properties (listen only)

- Notification Log
- Summary
- Map
- Containment (listen only).

  Context sharing roles and icons describes the context sharing roles, and shows the icons that display when context sharing is implemented.

Table 10-3. Context sharing roles and icons

Role	Description	Icon
Source	User selection in a source view changes the content in a listening view.	--
Listener	The content changes based upon user selection in a source view. Any filters set for the listening view will continue to control the display.	--
	In the title area, this icon indicates that a view is configured as a listener. The tool tip for the icon indicates which entities the view is configured to listen to.	
	In the title area, this icon indicates that a view is actively listening (a user selection in a source view is affecting the view). When a Notification Log is configured as a listener, you can click this icon to display the original notifications again. In the Notification and Map view, the tool tip for the icon indicates the entity the view is currently listening to.	

Context sharing is disabled for a Notification Log view if the Freeze Display option is enabled. To enable context sharing, first unfreeze the display by clicking the box icon in the title area. Freezing your display includes additional information.

Setting up context sharing

To configure a view as a listener:

1. Select the view to make it active, and then select **View** > **Listen to Context** or click the **Listen to Context** toolbar button. The **Select Context To Listen To** dialog box displays with the options that are appropriate for that view.
2. Select one of the following options:
   - **Listen to ALL** — Select all options that this view can listen to
     - **Collection Entity**
     - **Instance**
     - **Summary**
     - **Notification**
3. Click **OK** after your last selection. This immediately applies the parameter to the view and closes the dialog box.

Removing context sharing

To remove context sharing from a view:

1 Select the view to make it active, then select **View** > **Listen to Context** or click the **Listen to Context** toolbar button. The **Select Context(s) To Listen To** dialog box displays.

2 Select **Listen to NONE** or any one of the available options that you do not want to listen to.

3 Click **OK**. The **Listening to Context** icons are removed from the listener view (if the view is no longer listening to any option).

Saving a console

After you customize your console, you can save your console locally on the host where the Global Console is running or remotely on the host where the Global Manager is running. Summary of saved customizations summarizes the customizations and information that is saved for your console.

Table 10-4. Summary of saved customizations

What's saved	What's not saved
Console customizations (hidden bars, layout, titles, views)	Topology
Content customizations (filters and selections in the Column Sort Order dialog box, except for Click Sort)	Click Sort selections
The names of the Global Managers you attached to	The actual notifications or maps

Note To save maps, you must save them separately (*"Saving a map" on page 143* includes additional information.)

Console file naming conventions

In order for a console to be saved, you must follow these file naming conventions:

- Filenames must consist of letters, numbers, underscores, dashes, or any combination thereof.
- Filenames must not contain spaces.

  Examples of recommended filenames are: Console_SA, SA-Map, or Notification-Log3Views.

Using Save

To save a console:

1 Select **File** > **Save** or click the **Save** toolbar button. The Specify save destination dialog box appears if you are saving the console for the first time.

2 Click the **Local** button or the **Remote** button in the dialog box and perform the steps described in Saving a console locally, starting with step 2.

   If you have previously saved the console, your customizations are saved accordingly and the Specify save destination dialog box does not appear.

Saving a console locally

To save a console locally:

1 Select **File** > **Save As** > **Save Local As**. This displays the **Save Console** dialog box.

2 Type a name for the console in the **Object name** field. For a previously saved console, the name displays in the field. You can also specify another name with the extension .iccon.

3 Choose where you want to save the console or note the default location, *BASEDIR/smarts/local/consoles*.

4 Click **Save**.

5 In the **Select Domains to Reattach** dialog box, select one or more Manager that the saved console will automatically attach to when the console is opened. (To select multiple managers, press the **Ctrl** or **Shift** key while making your selections.)

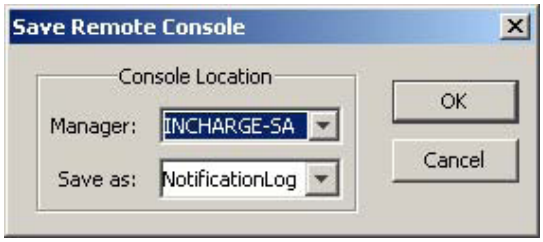
   This command saves the console settings to a local file. Whenever you start a session, to use the local console, you must open it from a running console (**File** > **Open** > **Open Local**).

Saving a console remotely

To save a console remotely:

1 Select **File** > **Save As** > **Save Remote As**. This displays the **Save Remote Console** dialog box, as shown in Save Remote Console dialog box.

   Figure 10-1. Save Remote Console dialog box



2 Select a location to save the console. Choose a Manager.

3 The Save as field lists the names of existing remote consoles. For a previously saved console, the name displays in the field. You can also specify another name without the extension .iccon.

   If a remote console name appears in the field, the existing console might be part of your user profile. Contact your administrator to see if you should overwrite the existing console.

4 In the **Select Domains to Reattach** dialog box, select one or more Managers that the saved console will automatically attach to when the console is opened. (To select multiple managers, press the **Ctrl** or **Shift** key while making your selections.)

5 Click **OK**. To use the customized console, you must open it from a running console (**File** > **Open** > **Open Remote**).

6 (Optional) To share the console with other users, in a UNIX shell, copy the console file from the *BASEDIR/smarts/local/consoles/<userid>* directory or the *BASEDIR/smarts/local/consoles/<user_profile>* directory to the *BASEDIR/smarts/local/consoles* directory on the remote host.

Note Write permission to the remote host directory is required for the copy operation.

Troubleshooting

11

This chapter includes the following topics:

- Common issues and resolutions
- Common issues for Companion UI

Common issues and resolutions

The following topics are included in this section:

- Checking Manager status
- Identifying a port number
- Refreshing the console
- Reattaching to a Manager
- Responding to disconnected Managers
- Accessing console message logs

Checking Manager status

If you do not know the operational status of your Manager, use the brcontrol command or the Browse button in the Attach Manager dialog box to list the Managers and their status. The status listed for your Manager should be Running. If your Manager is not running, contact your administrator, consult the VMware Smart Assurance System Administration Guide, or refer to your specific product's Installation Guide for instructions on starting the Manager.

For the brcontrolcommand, type one of the command lines shown in The brcontrol command.

Table 11-1. The brcontrol command

Operating system	Example
UNIX	BASEDIR/smarts/bin/brcontrol

Identifying a port number

If you do not know the port number of a Manager, use the brcontrolcommand or the Browse button in the Attach Manager dialog box to display the port number.

Refreshing the console

If your console does not display properly, you can force the console to redisplay. For example, if fragments of menus or fields from dialog boxes linger after the menus or dialog boxes close, you can redisplay the console.

To refresh a console, select **View** > **Refresh**.

Reattaching to a Manager

Initially, when you log in to start a session, you specify the Manager to which you want to attach. Ordinarily, you do not have to attach again during your session.

If the machine running Service Assurance becomes unavailable, the Global Console polls the broker every 30 seconds and reattaches when the Manager is operational. Attaching to a Manager includes instructions on manually attaching or reattaching to an VMware Smart Assurance Manager.

Note If an VMware Smart Assurance Manager disconnects, a Domain Disconnected message appears informing you that the manager disconnected and that the console will reconnect when the domain becomes available.

Responding to disconnected Manager s

When underlying Managers disconnect from the Global Manager (for example, due to a network outage), the notifications from the unavailable sources are not updated in the console. The affected notifications, maps, and summaries no longer reflect the current conditions.

If a disconnect situation occurs, a Session Disconnected notification informs you that a specific Manager is disconnected and a similar entry is added to the audit log.

When the Manager reconnects, the Session Disconnected notification clears, and it is recorded in the audit log.

If you receive a Session Disconnected notification, your administrator should investigate it for a network connection failure or an operational problem. The Manager may need to be restarted.

Accessing console message logs

The Global Console has two logs which are useful for troubleshooting:

- The Java console is the first tool to use for console debugging. It shows store exceptions, errors reading attributes, and stack traces.

  To collect the most information about potential console problems, specify the -Dcom.smarts.log.level=TRACE property.

  Java console information can automatically be saved to a file on your local workstation by specifying the -Dcom.smarts.java.log=<*filename*> property. When specifying this property, the file is written in the <*SM_WRITEABLE*>/logs directory.

SM_WRITEABLE is an environment variable whose default value can be changed in the runcmd_env.sh. Use this console information to assist with debugging issues.

Note Before starting the console with the -Dcom.smarts.java.log=<*filename*> property, verify that the <*SM_WRITEABLE*>/logs directory exists under BASEDIR/smarts/local.

- The message log shows everything the Manager sends to the console while the log window is activated (opened or minimized).

  This information can automatically be saved to a file on your local workstation by specifying the -Dcom.smarts.server.logMessages=true property. When specifying this property, the file is written to the <*SM_WRITEABLE*>/logs directory. Use this information to assist with debugging issues when the console stops responding.

  Note Before starting the console with the -Dcom.smarts.server.logMessages=true property, verify that the <*SM_WRITEABLE*>/logs directory exists.

  To access the log views, select **View** > **Java Console** or **View** > **Message Log**.

  In the Java console, the following warning is benign:

```
Warning: Could not get the full set of system properties
```

Common issues for Companion UI

The following topics are included in this section:

- HTTP error page
- Domain Manager not configured
- Internal error in the Global Manager, Global Console, or Smarts CUI

  When you launch Companion UI from a selected notification in the Notification Log Console or view, the following types of errors may appear as a web page in your browser.

HTTP error page

During launching if Companion UI encounters an error whereby it fails to access a service, an HTTP error page appears in your browser.

For example, if the Tomcat service is not running, the following error appears:

```
404 Page Not Found
```

Domain Manager not configured

If your Domain Manager is not configured as a data source in Companion UI , this error appears in your browser:

```
Launch Companion UI: <domain name> not configured. Please contact your System Administrator.
```

Contact your Smarts CUI administrator for assistance. Also, the VMware Smart Assurance SolutionPack Installation and Configuration Guide provides information about adding data sources to Smarts CUI.

Internal error in the Global Manager , Global Console , or Smarts CUI

If an internal error occurs in the top-level Global Manager, Global Console, or Companion UI, this error appears in your browser:

```
Launch Companion UI: â€¦

In a Smarts CUI deployment, the top-level Global Manager is configured as the SAM Presentation Server.
```

Wildcard Patterns

12

Types of wildcard patterns

A wildcard pattern is a series of characters that are matched against incoming character strings. You can use these patterns when you define pattern matching criteria.

Matching is done strictly from left to right, one character or basic wildcard pattern at a time. Basic wildcard patterns are defined in Basic wildcard patterns. Characters that are not part of match constructs match themselves. The pattern and the incoming string must match completely. For example, the pattern abcd does not match the input abcde or abc.

A compound wildcard pattern consists of one or more basic wildcard patterns separated by ampersand (&) or tilde (~) characters. A compound wildcard pattern is matched by attempting to match each of its component basic wildcard patterns against the entire input string. Compound wildcard patterns are listed in Compound wildcard patterns.

If the first character of a compound wildcard pattern is an ampersand (&) or tilde (~) character, the compound is interpreted as if an asterisk (*) appeared at the beginning of the pattern. For example, the pattern ~*[0-9]* matches any string not containing any digits. A trailing instance of an ampersand character (&) can only match the empty string. A trailing instance of a tilde character (~) can be read as “except for the empty string.”

Note Spaces are interpreted as characters and are subject to matching even if they are adjacent to operators like “&”.

Table 12-1. Basic wildcard patterns

Character	Description
?	Matches any single character. For example, server?.example.com matches server3.example.com and serverB.example.com, but not server10.example.com.
*	Matches an arbitrary string of characters. The string can be empty. For example, server*.example.com matches server-ny.example.com and server.example.com (an empty match).

Table 12-1. Basic wildcard patterns (Continued)

Character	Description
[set]	Matches any single character that appears within [set]; or, if the first character of [set] is (^), any single character that is *not* in the set. A hyphen (-) within [set] indicates a range, so that [a-d] is equivalent to [abcd]. The character before the hyphen (-) must precede the character after it or the range will be empty. The character (^) in any position except the first, or a hyphen (-) at the first or last position, has no special meaning. For example, server[789-].example.com matches server7.example.com through server9.example.com, but not server6.example.com. It also matches server-.example.com. For example, server[^12].example.com does not match server1.example.com or server2.example.com, but will match server8.example.com.
<n1-n2>	Matches numbers in a given range. Both *n1* and *n2* must be strings of digits, which represent nonnegative integer values. The matching characters are a non-empty string of digits whose value, as a nonnegative integer, is greater than or equal to *n1* and less than or equal to *n2*. If either end of the range is omitted, no limitation is placed on the accepted number. For example, 98.49.<1-100>.10 matches a range of IPv4 addresses from 98.49.1.10 through 98.49.100.10. Example of an omitted high end of the range: <50-> matches any string of digits with a value greater than or equal to 50. Example of an omitted low end of the range: <-150> matches any value between zero and 150. For a more subtle example: The pattern <1-10>* matches 1, 2, up through 10, with * matching no characters. Similarly, it matches strings like 9x, with * matching the trailing x. However, it does not match 11, because <1-10> always extracts the longest possible string of digits (11) and then matches only if the number it represents is in range.
|	Matches alternatives. For example, ”ab|bc|cd” without spaces matches exactly the three following strings: “ab”, “bc”, and “cd”. A | as the first or last character of a pattern accepts an empty string as a match. Example with spaces “ab | bc” matches the strings “ab” and “ bc”.
\	Removes the special status, if any, of the following character. Backslash (\) has no special meaning within a set ([set]) or range (<n1-n2>) construct.

Special characters for compound wildcard patterns are summarized in Compound wildcard patterns.

Character	Description
&	“And Also” for a compound wildcard pattern. If a component basic wildcard pattern is preceded by & (or is the first basic wildcard pattern in the compound wildcard pattern), it *must* successfully match. Example: *NY*&*Router* matches all strings which contain NY and also contain Router. Example: <1-100>&*[02468] matches even numbers between 1 and 100 inclusive. The <1-100> component only passes numbers in the correct range and the *[02468] component only passes numbers that end in an even digit. Example: *A*|*B*&*C* matches strings that contain either an A or a B, and also contain a C.
~	“Except” for a compound wildcard pattern (opposite function of &).If a component basic wildcard pattern is preceded by ~, it *must not* match. Example: 10.20.30.*~10.20.30.50 matches all devices on network 10.20.30 except 10.20.30.50. Example: *Router*~*Cisco*&*10.20.30.*~10.20.30.<10-20>* matches a Router, except a Cisco router, with an address on network 10.20.30, except not 10.20.30.10 through 10.20.30.20.