

# Neuron Event Manager

USER'S GUIDE

Product Version: 1.16.0

Document Revision: 1.0.0



## Copyright

Copyright © 1995-2011 Halcyon Monitoring Solutions, Inc.  
All rights reserved. This product and related documentation is protected by copyright and distributed under licenses restricting its use, copying, distribution and decompilation. No part of this product or related documentation may be reproduced in any form by any means without prior written authorization of Halcyon Monitoring Solutions, Inc. and its licensors.

Corporate Headquarters  
Halcyon Monitoring Solutions  
800 Bellevue Way NE,  
Suite 400  
Bellevue, WA 98004, USA

Tel: 416-932-4600  
Fax: 416-932-4711  
Email: [info@HalcyonInc.com](mailto:info@HalcyonInc.com)  
URL: [www.HalcyonInc.com](http://www.HalcyonInc.com)

## License Agreement

Downloading Halcyon software constitutes acceptance of the End User Binary Code License agreement, which can be found here: <http://www.halcyoninc.com/products/license.php>

Without purchasing a license, the Halcyon Software will only operate for a trial period of 14 days from installation. If you wish to purchase a license to use the Halcyon Software, please contact us at:

Web: <http://www.HalcyonInc.com>  
Email: [info@HalcyonInc.com](mailto:info@HalcyonInc.com)  
Tel: 416-932-4647  
Fax: 416-932-4711

## Technical Support

For assistance with any Halcyon products, contact Technical Support:

Tel: 1-877-932-4666 (Toll Free in North America)  
Tel: 1-416-932-4666 (International)  
Email: [support@HalcyonInc.com](mailto:support@HalcyonInc.com)

### Halcyon Forums:

Halcyon experts actively participate in the online Halcyon Forums. The experts are constantly monitoring the forums, answering questions and posting useful tips, tricks, and general knowledge base information. Whether you have a technical question or just wish to expand our knowledge base, this is the place for you. <http://forums.HalcyonInc.com>

## About Halcyon

Halcyon delivers Infrastructure Management solutions that provide operational visibility, availability, and reliability for business critical services and their underlying infrastructure. Since 1994, numerous Fortune 100 and SMEs, spanning every major geography and sector, have adopted Halcyon solutions.

At Halcyon, we believe the health of the IT infrastructure is integral to the success of a business. Our clients rely on us for complete end-to-end monitoring solutions that are straightforward, easy to deploy and use, and cost-effective, coupled with a history of client service excellence.

### **Your Infrastructure is Our Business**

# Contents

---

|          |  |           |
|----------|--|-----------|
| <b>1</b> | <b>PREFACE</b>                         | <b>7</b>  |
| 1.1      | PURPOSE OF THE DOCUMENT                | 7         |
| 1.2      | INTENDED AUDIENCE                      | 7         |
| 1.3      | RELATED DOCUMENTS                      | 7         |
| <b>2</b> | <b>GENERAL OVERVIEW</b>                | <b>9</b>  |
| 2.1      | PRODUCT OVERVIEW                       | 9         |
| 2.2      | GETTING STARTED                        | 9         |
| <b>3</b> | <b>VIEWING EVENTS (EVENT VIEWER)</b>   | <b>10</b> |
| 3.1      | TOPOLOGY PANEL                         | 11        |
| 3.1.1    | TOPOLOGIES                             | 11        |
| 3.1.2    | TOPOLOGY ASSET DISPLAY FORMAT          | 13        |
| 3.1.3    | VIEWING VIRTUALIZATION                 | 14        |
| 3.1.4    | FILTERING EVENTS USING THE TOPOLOGY    | 14        |
| 3.2      | STATUS PANEL                           | 15        |
| 3.3      | ACTIONS PANEL                          | 15        |
| 3.3.1    | EVENT DETAILS                          | 15        |
| 3.3.2    | EVENT TAGS                             | 16        |
| 3.3.3    | ALL EVENT TAGS                         | 17        |
| 3.3.4    | VIEW NEURON AGENT                      | 19        |
| 3.3.5    | EDIT NEURON AGENT                      | 20        |
| 3.3.6    | MANAGE EVENTS                          | 20        |
| 3.4      | FILTERS PANEL                          | 20        |
| 3.4.1    | TYPES OF EVENT VIEWER FILTERING        | 20        |
| 3.4.2    | FILTER BY SEVERITY                     | 21        |
| 3.4.3    | FILTER BY TIME RECEIVED                | 22        |
| 3.4.4    | FILTER BY STATE                        | 22        |
| 3.4.5    | FILTER PANEL CONTROLS                  | 23        |
| 3.5      | SEARCH PANEL                           | 24        |
| 3.5.1    | DOING A SIMPLE SEARCH                  | 24        |
| 3.5.2    | REFINING A SEARCH                      | 25        |
| 3.6      | EVENT VIEWER SETTINGS                  | 25        |
| 3.6.1    | DISPLAY SETTINGS                       | 26        |
| 3.6.2    | HIGHLIGHT SETTINGS                     | 26        |
| 3.6.3    | MAXIMUM NUMBER OF EVENTS               | 26        |
| 3.6.4    | VISIBLE COLUMNS                        | 26        |
| <b>4</b> | <b>MANAGING EVENTS (EVENT MANAGER)</b> | <b>27</b> |
| 4.1      | STATUS PANEL                           | 28        |
| 4.2      | CREATING AND EDITING RESPONSE RULES    | 29        |
| 4.2.1    | OVERVIEW                               | 29        |
| 4.2.2    | FILTERS                                | 30        |
| 4.2.3    | ACTIONS                                | 33        |

|            |   |           |
|------------|---|-----------|
| 4.2.4      | SCHEDULES                                 | 36        |
| 4.2.5      | POLICY                                    | 39        |
| <b>4.3</b> | <b>CREATING AND EDITING INBOUND RULES</b> | <b>40</b> |
| 4.3.1      | OVERVIEW                                  | 40        |
| 4.3.2      | OPS CENTER STREAM FILTERS                 | 40        |
| 4.3.3      | SNMP STREAM FILTERS                       | 42        |
| 4.3.4      | SNMP STREAM TRANSFORMATION                | 44        |
| <b>4.4</b> | <b>ACTIONS PANEL</b>                      | <b>46</b> |
| 4.4.1      | IMPORT RULES                              | 46        |
| 4.4.2      | VIEW RULE DETAILS                         | 47        |
| 4.4.3      | RUN PENDING ACTIONS                       | 47        |
| 4.4.4      | CLEAR PENDING ACTIONS                     | 48        |
| 4.4.5      | TEST ACTIONS                              | 48        |
| 4.4.6      | COPY RULES                                | 49        |
| 4.4.7      | ENABLE/DISABLE RULES                      | 49        |
| 4.4.8      | DELETE RULES                              | 49        |
| 4.4.9      | VIEW EVENTS                               | 50        |
| <b>4.5</b> | <b>FILTERS PANEL</b>                      | <b>50</b> |

# Figures

|  |    |
|--|----|
| FIGURE 3-1: EVENTS TAB EVENT VIEWER .....                      | 10 |
| FIGURE 3-2: SELECT TOPOLOGY TO VIEW .....                      | 11 |
| FIGURE 3-3: OS TOPOLOGY .....                                  | 12 |
| FIGURE 3-4: SYSTEMS TOPOLOGY .....                             | 13 |
| FIGURE 3-5: TOPOLOGY ASSET DISPLAY .....                       | 13 |
| FIGURE 3-6: SEVERITY TOPOLOGY ASSET DISPLAY .....              | 13 |
| FIGURE 3-7: VIEWING SOLARIS ZONES IN SYSTEMS TOPOLOGY .....    | 14 |
| FIGURE 3-8: EVENT VIEWER STATUS .....                          | 15 |
| FIGURE 3-9: EVENT VIEWER ACTIONS .....                         | 15 |
| FIGURE 3-10: EVENT DETAILS PANEL.....                          | 16 |
| FIGURE 3-11: EVENT TAGS PANEL.....                             | 16 |
| FIGURE 3-12: ALL EVENT TAGS PANEL .....                        | 17 |
| FIGURE 3-13: EVENT TAG EDITOR .....                            | 17 |
| FIGURE 3-14: VIEW NEURON AGENT.....                            | 19 |
| FIGURE 3-15: EDIT NEURON AGENT WINDOW .....                    | 20 |
| FIGURE 3-16: SEVERITY FILTER.....                              | 22 |
| FIGURE 3-17: TIME RECEIVED FILTER .....                        | 22 |
| FIGURE 3-18: STATE FILTER.....                                 | 23 |
| FIGURE 3-19: SEARCH PANEL.....                                 | 24 |
| FIGURE 3-20: EVENT VIEWER SETTINGS .....                       | 25 |
| FIGURE 4-1: EVENTS TAB EVENT MANAGER.....                      | 27 |
| FIGURE 4-2: EVENT MANAGER STATUS .....                         | 28 |
| FIGURE 4-3: RESPONSE RULE FILTERS TAB .....                    | 30 |
| FIGURE 4-4: RESPONSE RULE ACTIONS TAB .....                    | 33 |
| FIGURE 4-5: RESPONSE RULE ADDITIONAL ACTIONS .....             | 34 |
| FIGURE 4-6: RESPONSE RULE SCHEDULES TAB .....                  | 37 |
| FIGURE 4-7: CREATE A BETWEEN TIME WINDOW .....                 | 38 |
| FIGURE 4-8: RESPONSE RULE POLICY TAB .....                     | 39 |
| FIGURE 4-9: OPS CENTER STREAM INBOUND RULE FILTERS TAB .....   | 41 |
| FIGURE 4-10: SNMP STREAM INBOUND RULE FILTERS TAB.....         | 42 |
| FIGURE 4-11: SNMP STREAM INBOUND RULE TRANSFORMATION TAB ..... | 44 |
| FIGURE 4-12: VIEW RULE DETAILS PANEL.....                      | 47 |

# Tables

|   |    |
|---|----|
| TABLE 1-1: INTENDED AUDIENCE .....                              | 7  |
| TABLE 1-2: RELATED DOCUMENTS .....                              | 7  |
| TABLE 4-1: RULES TABLE .....                                    | 28 |
| TABLE 4-2: RESPONSE RULE OVERVIEW TAB FIELDS .....              | 29 |
| TABLE 4-3: RESPONSE RULE FILTER TYPES .....                     | 30 |
| TABLE 4-4: RESPONSE RULE DEFAULT ACTIONS .....                  | 33 |
| TABLE 4-5: RESPONSE RULE ADDITIONAL ACTIONS FROM ADAPTERS ..... | 35 |
| TABLE 4-6: RESPONSE RULE EVENT DATA PARAMETERS .....            | 36 |
| TABLE 4-7: RESPONSE RULE SCHEDULE TYPES .....                   | 37 |
| TABLE 4-8: INBOUND RULE OVERVIEW TAB FIELDS .....               | 40 |
| TABLE 4-9: OPS CENTER STREAM INBOUND RULE FILTER TYPES .....    | 41 |
| TABLE 4-10: SNMP STREAM INBOUND RULE FILTER TYPES .....         | 43 |

|   |    |
|---|----|
| TABLE 4-11: SNMP STREAM INBOUND RULE FILTER TYPES | 44 |
| TABLE 4-12: TEST ACTION EVENT DETAILS             | 48 |

# 1 Preface

## 1.1 Purpose of the Document

The purpose of this document is to describe the *Neuron Event Manager* and how end-users, managers, and administrators will use it.

## 1.2 Intended Audience

This guide is written for the following type of audience:

**Table 1-1: Intended Audience**

| Role                     | Usage   |
|--------------------------|---|
| End User                 | The User's Guide is intended for end users who use the product on a daily basis. This guide provides information on how to use the product for tasks such as viewing and filtering events.                                    |
| Manager<br>Administrator | The User's Guide provides information for managers who are responsible for preparing the product for use by end users. Their tasks include setting event management rules that dictate the actions taken for incoming events. |

## 1.3 Related Documents

This solution is composed of a series of underlying products. For further information regarding the configuration, usage and administration of the products, please refer to the following documents.

These documents may be located in the doc folder of the solution distribution or on the website ([www.halcyoninc.com/docs](http://www.halcyoninc.com/docs)).

**Table 1-2: Related Documents**

| Component Name           | Related Documents   |
|--------------------------|---|
| Neuron Management Suite  | <ul style="list-style-type: none"> <li>▪ Neuron Management Suite Installation Guide</li> </ul>  |
| Neuron Management Server | <ul style="list-style-type: none"> <li>▪ Neuron Management Server Release Notes</li> <li>▪ Neuron Management Server User's Guide</li> </ul> |
| Neuron Event Manager     | <ul style="list-style-type: none"> <li>▪ Neuron Event Manager Release Notes</li> </ul>  |
| Neuron Inventory Manager | <ul style="list-style-type: none"> <li>▪ Neuron Inventory Manager Release Notes</li> <li>▪ Neuron Inventory Manager User's Guide</li> </ul> |

|                              |  |
|------------------------------|--|
| Neuron Configuration Manager | <ul style="list-style-type: none"><li>▪ Neuron Configuration Manager Release Notes</li><li>▪ Neuron Configuration Manager User's Guide</li></ul> |
| Neuron Health Manager        | <ul style="list-style-type: none"><li>▪ Neuron Health Manager Release Notes</li><li>▪ Neuron Health Manager User's Guide</li></ul>               |
| Neuron Utilities             | <ul style="list-style-type: none"><li>▪ Neuron Utilities User's Guide</li></ul>  |
| Neuron Integration Solutions | <ul style="list-style-type: none"><li>▪ README.Solutions</li></ul>   |
| Neuron Server Configuration  | <ul style="list-style-type: none"><li>▪ README.config</li></ul>  |

## 2 General Overview

---

### 2.1 Product Overview

The Events Tab within the *Neuron Management Portal* UI (please refer to the *Neuron Management Server User's Guide* for details about the *Portal*, including logging in), allows users to view as well as manage Neuron Events. Events in Neuron may have been generated by Neuron's own Configuration and Health monitoring (refer to the *Neuron Configuration Manager* and *Neuron Health Manager User's Guides*), from agents reporting to Neuron or from other third party products that have been integrated with Neuron, such as Oracle Enterprise Manager Ops Center.

By default, the Events Tab starts in View Mode (showing the Event Viewer). You can switch to Manage Mode (and show the Event Manger) by clicking the Manage Events button in the Actions Panel.

When viewing events, you will be able to filter and search events based on assets, severity, state, time range or any text desired. Tags can be created to match on patterns within an event, and all tags that match a selected event can be viewed.

When managing events, you can create rules that filter incoming events and can perform various actions when an event matches those filters. For instance, you could create rules that would email one group of people when warnings arise on web server systems, but notify another group in the event of critical events.

### 2.2 Getting Started

The *Neuron Event Viewer* and *Neuron Event Manager* are used to view and manage Neuron Events. To receive events, you will need to discover and manage assets within Neuron (refer to the *Neuron Inventory Manager*, *Neuron Configuration Manager* and *Neuron Health Manager User's Guides*), deploy Neuron Agents to report to the Neuron Server (refer to the *Neuron Inventory Manager User's Guide*) or configure a third party product to forward events to the Neuron Server (refer to README.Solutions).

## 3 Viewing Events (Event Viewer)

By default, the Events Tab starts in View Mode where you can view Neuron Events. This is also referred to as the Event Viewer as you use it to view events.

The screenshot displays the Neuron Event Manager interface. On the left is a 'Systems Topology' tree showing a domain with SPARC and x86 systems. The central 'Events' table is the primary focus, listing events with the following columns: Event ID, Time Received, Source Host, Severity, and Message. The table shows a mix of event severities, including Critical (CPU Util), Warning (Mem Util, Configuration), and Info (Discovery, Agent, RSA keys). On the right, the 'Status' panel indicates 57 events displayed and 0 pending, with a 'Refresh' button. Below it, the 'Actions' panel offers options for event details, tagging, and management. A 'Filter By Severity' dropdown is also present.

| Event ID | Time Received      | Source Host       | Severity | Message                                       |
|----------|--------------------|-------------------|----------|---|
| 279      | 23 Nov 11 10:16:04 | kenny             | Critical | CPU Util (CPU) is 99 % > 95 %                 |
| 260      | 23 Nov 11 10:06:53 | kenny             | Warning  | Mem Util (Memory) is 84 % > 80 %              |
| 247      | 23 Nov 11 10:03:32 | kenny             | Warning  | Configuration operation 'System Model' run    |
| 246      | 23 Nov 11 10:02:55 | opal              | Warning  | Configuration operation 'System Model' run    |
| 236      | 23 Nov 11 10:02:24 | SolarisBaseModule | Warning  | Error executing configuration operation 'Ava  |
| 226      | 23 Nov 11 10:02:24 | archer            | Info     | Finished discovery.                           |
| 221      | 23 Nov 11 10:02:13 | archer            | Info     | Discovered Physical Host kenny.               |
| 220      | 23 Nov 11 10:02:13 | archer            | Info     | Discovered Asset kenny.                       |
| 214      | 23 Nov 11 10:02:13 | archer            | Info     | Discovered Physical Host opal.                |
| 213      | 23 Nov 11 10:02:13 | archer            | Info     | Discovered Asset opal.                        |
| 202      | 23 Nov 11 10:02:13 | archer            | Info     | Discovered Neuron Agent on kenny.             |
| 198      | 23 Nov 11 10:02:13 | archer            | Info     | Discovered Neuron Agent on opal.              |
| 197      | 23 Nov 11 10:02:03 | kenny             | Info     | Added RSA host key for host kenny (SshSer     |
| 196      | 23 Nov 11 10:02:03 | opal              | Info     | Added RSA host key for host opal (SshServi    |
| 195      | 23 Nov 11 10:02:03 | archer            | Info     | Started discovery for hosts [kenny, opal] wit |
| 194      | 23 Nov 11 10:00:31 | archer            | Warning  | Configuration operation 'System Model' run    |
| 177      | 23 Nov 11 10:00:00 | archer            | Info     | Finished discovery.                           |
| 174      | 23 Nov 11 09:59:50 | archer            | Info     | Discovered that Non-Global Zone hero resid    |
| 173      | 23 Nov 11 09:59:50 | archer            | Info     | Discovered that Non-Global Zone iceberg re    |
| 126      | 23 Nov 11 09:56:19 | archer            | Info     | Discovered Global Zone mammoth with zone      |
| 125      | 23 Nov 11 09:56:19 | archer            | Info     | Discovered Global Zone coolthreads with zone  |
| 124      | 23 Nov 11 09:56:19 | archer            | Info     | Discovered Physical Host twilight.            |
| 123      | 23 Nov 11 09:56:19 | archer            | Info     | Discovered Asset twilight.                    |
| 122      | 23 Nov 11 09:56:19 | archer            | Info     | Discovered Physical Host mammoth.             |

Figure 3-1: Events Tab Event Viewer

The center panel is dominated by a table that displays events in the Neuron Server Events database. The panels around the table allow you to filter what events appear in the events table as well as view more details about individual events.

As events occur and are received and processed by the Neuron Server, they will not automatically appear in the Event Viewer's events table. Instead you will see the "events pending" count in the Status Panel (see section 3.2) increase. To have any new/pending events be loaded into the Event Viewer, click the Refresh button in the Status Panel. This action will also be reflected in the Last Refreshed time, regardless of whether new events are added to the events table or not.

Events displayed within the Event Viewer's events table can be sorted by clicking the column headers. Clicking the same header again will reverse the sort (an arrow should indicate the sort direction). To sort by multiple columns (such as sort by severity, then sort by host), click the area of the header next to the text (where the arrow appears).

Sorting does not impact what events appear in the table, just their order. By default events are sorted by descending Event ID.

## 3.1 Topology Panel

The Topology Panel can be found in the left hand panel of the display.

This panel presents topology views of assets Neuron Server is aware of. In order for an asset to appear within a topology, the Neuron Server must first be aware of that asset. This can happen either by manually discovering the asset (refer to the *Neuron Inventory Manager User's Guide*) or when the Neuron Server receives an event for that asset (such as from Oracle Enterprise Manager Ops Center).

In order for assets to appear in some topologies, Neuron must be aware of certain details of the asset. For instance, in order to appear in the Systems Topology, Neuron must know whether the system has a SPARC or x86 architecture. If an asset is not appearing in a topology you expect it to appear in, you should try and do a discovery of that asset. Depending on how the asset was added to Neuron (type of discovery or incoming event), some details may have been unavailable. Refer to the *Neuron Inventory Manager User's Guide* for details on discovery.

If an asset or group in the Topology has a plus (+) box next to it, that asset or group has at least one child under it. Click the + to view the children. When the children are in view, the + will change to a minus (-) box. Click the - to collapse the asset and hide the children.

### 3.1.1 Topologies

There are 8 different topologies that may be available to view via the drop-down in the Topology Panel header:

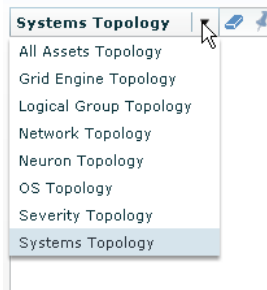


Figure 3-2: Select Topology to View

#### 3.1.1.1 All Assets Topology

The All Assets Topology view shows all Systems, Network Devices, and Storage assets grouped in those categories. If an asset does not fit into any of these categories, it is displayed under Unknown.

#### 3.1.1.2 Grid Engine Topology

The Grid Engine Topology view shows all configured Grid Engine Master Hosts and their associated Queues and Execution Hosts.

You must have the Grid Engine Module configured and enabled in order to see this topology. Updating the module's configuration will update the Master Hosts that appear in this topology. Please refer to README.config for details about accessing the *Neuron Management Suite's Server Configuration* page and configuring the Grid Engine Module.

### 3.1.1.3 Logical Group Topology

The Logical Group Topology shows all Logical Groups and the assets within those groups. Logical Groups are created and assets added to them via the Logical Group Manager. Please refer to the *Neuron Inventory Manager User's Guide* for details on creating and managing Logical Groups.

### 3.1.1.4 Network Topology

The Network Topology view shows all Network Devices. This would include, for instance, assets discovered using the Energy Wise discovery protocol.

### 3.1.1.5 Neuron Topology

The Neuron Topology view shows all Neuron Server and Neuron Agent assets. The top-level entry is the host on which the Neuron Management Server runs. The Neuron Server itself is shown as the "Control Agent".

Neuron Agents can be discovered along with other assets. Refer to the *Neuron Inventory Manager User's Guide* for details on discovery.

### 3.1.1.6 OS Topology

The OS Topology view shows all assets grouped by their operating system family. If an asset's operating system is not known, it is displayed under Unknown.



Figure 3-3: OS Topology

### 3.1.1.7 Severity Topology

The Severity Topology view shows all assets sorted based on their highest severity event that appears in the Event Viewer.

Only events that appear within the Event Viewer are considered for this topology. Only assets that have at least one event appearing in the Event Viewer will appear in this topology.

### 3.1.1.8 Systems Topology

The Systems Topology view is the default topology and shows all assets grouped by the architecture of their hardware (SPARC or x86). If an asset's hardware is not known, it is displayed under Unknown. If an asset's hardware architecture has not been discovered, the asset will not appear in this topology.

This is the topology under which you can see the relationship of virtualized assets (such as global and non-global zones). See section 3.1.3 for more details.

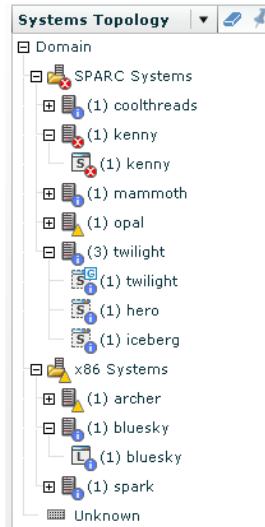


Figure 3-4: Systems Topology

### 3.1.2 Topology Asset Display Format

Most topologies display assets within a group where the group shows a possible severity icon, and the assets themselves show a possible severity icon and an event count in parenthesis.

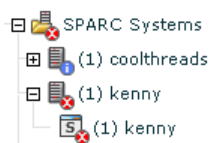


Figure 3-5: Topology Asset Display

The severity icon on an asset or group indicates the highest severity event that appears within the Event Viewer that is associated with the asset or a child of the asset or group. The count on the asset is the number of events within the Event Viewer of the indicated severity that are associated with the asset or a child of the asset.

The Severity Topology is a special case and displays things a little differently. Here the severity groups indicate the number of assets within the group (the number of assets that have that group's severity as its highest associated event within the Event Viewer). The assets themselves don't indicate any event counts.



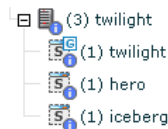
Figure 3-6: Severity Topology Asset Display

Regardless of the topology, you can select an asset or group to view all the events that appear within the Event Viewer and are tied to the selected asset/group and any children of the asset/group. Refer to section 3.1.4 for more details.

In all cases, the asset is identified by the asset's host name if it could be resolved. If the hostname could not be resolved, then the host's ip is displayed.

### 3.1.3 Viewing Virtualization

If assets have been properly discovered for virtualization (refer to the *Neuron Inventory Manager User's Guide*) then virtualization relationships can be viewed using the Systems Topology. For instance, you can use this topology to see all the zones that have been discovered on a given system. The following shows the Global Zone twilight and Non-Global Zones hero and iceberg that were discovered on the twilight system.



**Figure 3-7: Viewing Solaris Zones in Systems Topology**

Relationships among Oracle VMs for SPARC (formerly known as LDOMs) can also be similarly viewed here.

### 3.1.4 Filtering Events using the Topology

You can filter events that appear in the Event Viewer events table by asset or by group simply by clicking on the desired asset or group. When you click on an asset within a topology, only events associated with that asset (and its children) will appear in the events table. When you click on a group, the event table will show events associated with all assets in that group (and their children).

When an asset or group is selected, it will appear bolded. To change which asset or group is selected, simply click the next asset or group you want to filter on (you can only have one asset or group selected in each topology at a time).

To remove a filter (to de-select an asset or group), you can either click on the selected asset or group, or you can click the clear button in the header of the Topology Panel (🧼).

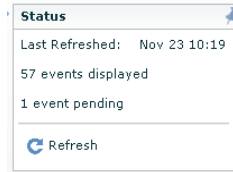
#### 3.1.4.1 What Events Get Filtered On?

The topology filtering is strictly display filtering, so while the number of events shown in the events table may change, the number of events the Event Viewer has loaded does not change. Because of this, the event counts and event severities shown by the assets in the Topology Panel will not change when one asset or group is selected.

Please refer to sections 3.4.1 and 3.4.1.1.

## 3.2 Status Panel

Information on the status of the Event Viewer can be found in the Status Panel on the top right side of the Event Viewer.



**Figure 3-8: Event Viewer Status**

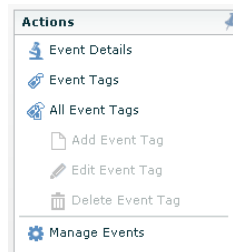
Last Refreshed: This is the last time the display of events was refreshed.  
 Y events displayed: This indicates the number of events being shown in the events table.  
 X events pending: This indicates the number of events that have occurred since the Event Viewer was last refreshed. These events are not yet shown in the events table.

Clicking Refresh will update the events table to include the new Pending events.

Clicking Refresh while a Search (3.5) or a Database Query Filter (3.4.1.2) has been applied may have no impact on the events displayed if none of the pending events match the search or filter criteria.

## 3.3 Actions Panel

The Actions Panel is located on the right side of the Event Viewer, below the Status Panel.



**Figure 3-9: Event Viewer Actions**

### 3.3.1 Event Details

Clicking “Event Details” in the Actions Panel will either show or hide the Event Details Panel below the events table.

The Event Details Panel will show details about the event that is currently selected in the events table. All fields in this panel are selectable, so you can copy and paste any of the event’s details (such as the message) from this panel.

NOTE: Right clicking any of the fields will provide a “Select all” option for that field.

| Events   |                    |             |          |   |  |
|----------|--------------------|-------------|----------|---|--|
| Event ID | Time Received      | Source Host | Severity | Message                                   |  |
| 1437     | 23 Nov 11 14:21:12 | hero.1161   | Critical | craigD PrimeAlert ScriptRunner all Last M |  |
| 1436     | 23 Nov 11 14:21:02 | kenny       | Critical | CPU Util (CPU) is 100 % > 95 % (value r   |  |
| 1435     | 23 Nov 11 14:20:42 | hero.1161   | Info     | craigD PrimeAlert ScriptRunner two Last   |  |
| 1434     | 23 Nov 11 14:20:42 | hero.1161   | Critical | craigD PrimeAlert ScriptRunner all Last M |  |
| 1433     | 23 Nov 11 14:20:42 | hero.1161   | Warning  | craigD PrimeAlert ScriptRunner all Last M |  |
| 1423     | 23 Nov 11 14:19:41 | hero.1161   | Info     | craigD PrimeAlert ScriptRunner two Last   |  |
| 1422     | 23 Nov 11 14:19:41 | hero.1161   | Warning  | craigD PrimeAlert ScriptRunner all Last M |  |

| Event Details for Event ID: 1436 (Critical) |                    |            |            |
|---|--------------------|------------|------------|
| Source Host                                 | Time Occurred      | Proxy Host | Proxy Type |
| kenny                                       | Nov 23 11 14:20:59 |            |            |

**Event Message:** CPU Util (CPU) is 100 % > 95 % (value now 24 %)

**Event Source:** rule://os/Health/kenny

| Vendor  | Time Received      | Correlation ID                   | Source ID |
|---------|--------------------|----------------------------------|-----------|
| unknown | Nov 23 11 14:21:02 | 215fd9f21129473d92d1e161baf4bce9 |           |

Figure 3-10: Event Details Panel

### 3.3.2 Event Tags

Clicking “Event Tags” in the Actions Panel will either show or hide the Event Tags Panel below the events table. The Event Tags Panel will display all Event Tags that are associated with the event selected in the events table.

| Events   |                    |                   |          |   |  |
|----------|--------------------|-------------------|----------|---|--|
| Event ID | Time Received      | Source Host       | Severity | Message                                     |  |
| 260      | 23 Nov 11 10:06:53 | kenny             | Warning  | Mem Util (Memory) is 84 % > 80 %            |  |
| 247      | 23 Nov 11 10:03:32 | kenny             | Warning  | Configuration operation 'System Model' run  |  |
| 246      | 23 Nov 11 10:02:55 | opal              | Warning  | Configuration operation 'System Model' run  |  |
| 236      | 23 Nov 11 10:02:24 | SolarisBaseModule | Warning  | Error executing configuration operation 'Av |  |
| 226      | 23 Nov 11 10:02:24 | archer            | Info     | Finished discovery.                         |  |
| 221      | 23 Nov 11 10:02:13 | archer            | Info     | Discovered Physical Host kenny.             |  |
| 220      | 23 Nov 11 10:02:13 | archer            | Info     | Discovered Asset kenny.                     |  |

| Event Tags for Event ID: 260 (Warning) |             |                         |  |
|--|-------------|-------------------------|--|
| Tag Name                               | Pattern     | Description             | Notes  |
| Memory Usage                           | Mem Util .* | Memory usage has spiked | Go back to the system in question and check the memory usage trend. If this is an isolated spike, make a note of it but don't carry out further action. If memory usage has been trending higher, look at what processes have been consuming it. |

Figure 3-11: Event Tags Panel

If you wish to copy the notes for a given tag, you can select the tag and click Edit Event Tag in the Actions Panel to open the Event Tag Editor where you can copy the values from any of the fields. To return to the Event Tags Panel, simply click “Event Tags” in the Actions Panel.

NOTE: Only one of “Event Tags” or “All Event Tags” can be displayed at once.

#### 3.3.2.1 What are Event Tags?

Event Tags are a way of classifying or grouping events. Each Tag is defined with a regular expression pattern that gets matched against each event's message. If the message matches the pattern, that event is tagged with that Event Tag. A list of tags can be viewed for each event by selecting the event and opening the Event Tags Panel.

Event Tags can also be created with a “Notes” section that can contain verbose details about the type of event being tagged. These details could include likely causes, where to look for the source of the problem or any actions to take to remedy the problem.

Event Tags can also be managed in bulk using Neuron command line utilities. Please refer to the *Neuron Utilities User's Guide* for more details.

### 3.3.3 All Event Tags

Clicking “All Event Tags” in the Actions Panel will either show or hide the All Event Tags Panel below the events table. This panel will display all Event Tags that exist. Anything displayed here is independent from any event that is selected. This provides a way to review all Event Tags that have been created.

| Tag Name     | Pattern     | Description             | Notes  |
|--------------|-------------|-------------------------|--|
| CPU Usage    | CPU Util .* | CPU Util Spike          | There was a spike in CPU usage. Check if this is an isolated spike of whether usage has been steadily trending higher. If it's been trending higher, check which processes have been responsible for it.   |
| Memory Usage | Mem Util .* | Memory usage has spiked | Go back to the system in question and check the memory usage trend. If this is an isolated spike, make a note of it but don't carry out further action. If memory usage has been trending higher, look at what processes have been consuming it. |

Figure 3-12: All Event Tags Panel

NOTE: Only one of “Event Tags” or “All Event Tags” can be displayed at once.

#### 3.3.3.1 Add Event Tag

To add a new Event Tag, open the All Event Tags Panel and then click “Add Event Tag” in the Actions Panel to open the Event Tag Editor used to create new Event Tags.

|                     |  |
|---------------------|--|
| <b>Name:</b>        | CPU Usage  |
| <b>Description:</b> | CPU Util Spike   |
| <b>Pattern:</b>     | CPU Util .*  |
| <b>Notes:</b>       | There was a spike in CPU usage. Check if this is an isolated spike of whether usage has been steadily trending higher. If it's been trending higher, check which processes have been responsible for it. |

Apply Clear

Figure 3-13: Event Tag Editor

With the Event Tag Editor open, enter all the details for your tag and click the Apply button (📄) to save it. If you wish to add more tags, click the Clear button (🗑️) to clear all the fields, then repeat.

You must enter in a regular expression in the Pattern field, which will be matched against each event's message. The following are some examples:

Example 1: To tag system load average events that look like:

"PrimeAlert SystemMonitor 1 Min system load average > 2"

The regular expression could be `.*load average.*`, which will match all events whose message contains "load average". You could instead use a regular expression like `.*load average >.*` which will match events when the load average exceeds a threshold.

Example 2: To tag both swag usage and cpu usage events, such as:

"PrimeAlert SystemMonitor Swap Space Used > 30%"

"PrimeAlert SystemMonitor Average CPU Usage > 80%"

The regular expression could be `.*([sS]wap|[cC][cP][uU]).*`, which will match events whose messages contain "swap", "Swap", "cpu" or "CPU".

Example 3: To tag events whose messages do not contain some phrase, such as "Performance data collection failed", you could use the following regular expression:

`(?!.*Performance data collection failed).*`

This will match events whose messages do not contain "Performance data collection failed".

You must be in the "Managers" or "Admins" user group to add an Event Tag. Refer to the *Neuron Management Server User's Guide* for more details about Users and Groups.

### 3.3.3.2 Edit Event Tag

Tags can be edited via the Event Tag Editor by:

- Selecting a row in either the "Event Tags" table or the "All Event Tags" table and clicking on the "Edit Event Tag" button in the Actions Panel.

With the Event Tag Editor open, any of the fields can be edited and saved by clicking on the Apply button. To return to the previous panel, select that panel from the Actions Panel, or close the editor by clicking the X in the top right of the Event Tag Editor.

NOTE: Changing the name of a tag will create a new tag with that name. To change the name of a tag, you will need to create a new tag with the new name, then delete the existing tag.

You must be in the "Managers" or "Admins" user group to edit an Event Tag. Refer to the *Neuron Management Server User's Guide* for more details about Users and Groups.

### 3.3.3.3 Delete Event Tag

To delete an existing Event Tag, simply select the tag in either the Event Tags Panel or the All Event Tags Panel and click "Delete Event Tag" in the Actions Panel. Confirming that the tag should be deleted will permanently remove it from the database. It will no longer appear be associated with any events.

You must be in the “Managers” or “Admins” user group to delete an Event Tag. Refer to the *Neuron Management Server User's Guide* for more details about Users and Groups.

### 3.3.4 View Neuron Agent

This button becomes available when an event that came from a Neuron Agent is selected in the events table, or when a Neuron Agent asset is selected in the Neuron Topology (see section 3.1.1.5). Clicking this button will load that Neuron Agent into the Event Viewer.

When you are finished viewing the agent, click “Return...” in the top left corner of the screen.

The screenshot displays the Neuron Management Portal interface for viewing a specific Neuron Agent. The page title is "neuron management portal" and the agent name is "Neuron Agent :: twilight". A "Return ..." button is visible in the top left corner. The main content area is divided into several sections:

- Host Summary:** Displays the agent name "TWILIGHT - 10.20.5.90" and system information: "Sun-Fire-T200, 32 CPU, 16256 MB" and "SunOS 5.10, Generic\_141444-09". It includes links for "Event History" and "Agent Log".
- Module Explorer:** A tree view showing the agent's structure:
  - twilight [10.20.5.90]
    - Hardware
      - PrimeAlert Hardware Monitor
    - Operating System
      - PrimeAlert MIB-II System
      - PrimeAlert SystemMonitor
        - User Statistics
        - Process Statistics
        - System Load
        - CPU Usage
        - Physical Memory
        - Swap Usage
        - Filesystem Usage
        - ZFS Statistics
        - Network Statistics
        - Zone Statistics
        - TCP Connections
        - IPC Facilities
        - PrimeAlert DirectoryMonitor [Var Monitoring]
        - PrimeAlert FileSizeMonitor [File Monitoring]
      - Local Applications
      - Remote Systems
- Agent Log Event History:** A table showing the agent's status and events. The table has columns for Name, Status, and Timestamp.
 

| Name               | Status  | Timestamp           |
|--------------------|---|---------------------|
| Hardware           | Hardware OK                                     | 2011-11-04 18:15:22 |
| Operating System   | PrimeAlert SystemMonitor Average CPU Usage > 1% | 2011-11-16 15:00:56 |
| Local Applications | Local Applications OK                           | 2011-11-04 18:15:22 |
| Remote Systems     | Remote Systems OK                               | 2011-11-04 18:15:23 |

**Figure 3-14: View Neuron Agent**

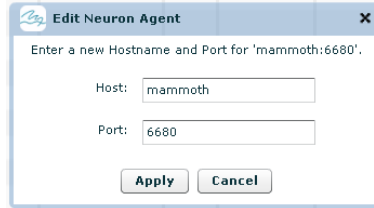
Each Neuron Agent has a username and password associated with it that is used to login when viewing the agent. If the agent was provisioned from the *Neuron Inventory Manager*, then the credentials should be correct. If the agent was discovered, the credentials may have been discovered. To check and/or set the agent credentials, please refer to the *Neuron Inventory Manager User's Guide*.

If the agent's username and/or password are wrong, the login will fail and a warning will appear in the agent's log file:

```
warning WebAgent: Incorrect username or password: admin
```

### 3.3.5 Edit Neuron Agent

This button becomes available when a Neuron Agent asset is selected in the Neuron Topology (see section 3.1.1.5). Clicking this button will open the Edit Neuron Agent Window where you can change the agent's host or port.



**Figure 3-15: Edit Neuron Agent Window**

**IMPORTANT:** This will edit the Neuron Agent properties on the Neuron Server, but has no impact on the agent itself. The agent should first be updated accordingly, then Neuron Server should be updated to reflect those changes.

Changing the agent's host will impact all assets that are tied to that agent (such as the asset for the system the agent is on).

The Port refers to the Neuron Agent's WebAgent HTTP Port.

### 3.3.6 Manage Events

Clicking "Manage Events" will change the Events Tab to Manage Mode which will load the Event Manager in place of the Event Viewer. Please refer to section 4 for details about Managing Events.

**NOTE:** If you are in Manage Mode, you can return to the Event Viewer by clicking "View Events" in the Event Manager Actions Panel.

## 3.4 Filters Panel

The Filters Panel is located at the bottom right of the Event Viewer screen (below the Actions Panel).

The Filters Panel is one area within the Event Viewer that event filtering can be performed. The drop-down at the top of the panel allows you to choose what filter criteria you want to define (you can define as many as you want).

Before reviewing the details of each criteria available in the panel (Severity, Time Received and State), please review the types of filters used in the Event Viewer and what their impact on the events is:

### 3.4.1 Types of Event Viewer Filtering

The Neuron Event Manager displays only the most recent events from the Neuron Management Suite's Event Database. By default, only the most recent 1000 (one thousand) events will be displayed. This number of events can be configured up to 10 000 (ten thousand) or down to 100 (one hundred). Refer to section 3.6.3.

After any filtering is applied, some events will no longer appear in the Event Viewer events table. They are of course still stored within the Neuron Events Database.

Please note that even if filtering has not been applied, the Event IDs that appear in the events table may not be sequential. Some events are strictly internal to Neuron and will never be visible externally and some events may be discarded via the de-duplication process (if an event is created that is identical to an existing event, Neuron will discard it).

Events that are loaded into the Event Viewer and the events that are actually displayed in the events table can be affected by 2 different types of filtering operations:

### 3.4.1.1 Display Filtering

Display filtering is filtering that only affects what events are shown in the events table, not what events are loaded by the Event Viewer (see Query Filtering in section 3.4.1.2 below for more details).

By default, the Event Viewer will query the Neuron Events Database for the most recent 1000 (one thousand) events and display them all in the events table. You will then be able to use display filtering to tell the Event Viewer to only show a subset of those events in the events table.

This type of filtering is used via the Topology Panel (see section 3.1.4).

In order to get a different set of events from the database, you need to either adjust how many events are loaded by default (see section 3.6.3), use a Database Query Filter (see section 3.4.1.2) or do a Search (see section 3.5).

### 3.4.1.2 Database Query Filtering

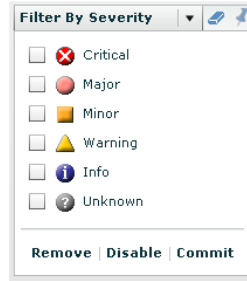
Database Query Filtering is filtering that affects what events are loaded into the Event Viewer from the Neuron Events Database. The Event Viewer will query the Events Database for events based on the criteria defined in the applied filters and retrieve the most recent events that match the criteria up to the maximum number of events the Event Viewer can load (3.6.3).

When applied, all events are loaded into the Event Viewer and displayed in the events table. You can then enable a Display Filter (3.4.1.1) to further filter the events that are displayed.

This type of filtering is used via the Filters Panel as well as the Search Panel (see section 3.5).

## 3.4.2 Filter By Severity

When "Filter By Severity" is selected from the Filters Panel drop-down, six check boxes appear that allow you to choose the severities of the events loaded by the Event Viewer. By default events of all severities are loaded.



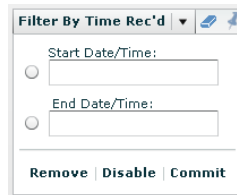
**Figure 3-16: Severity Filter**

If you would like to view only events of a certain severity, check that severity type and click the Commit button. You can select multiple severities and only events that are of any of the selected severities will get loaded on Commit.

Active filters appear with a check mark. To de-activate a filter, un-check the box next to the severity icon and click the Commit button.

### 3.4.3 Filter By Time Received

When “Filter By Time Received” is selected from the Filters Panel drop-down, two fields will appear allowing you to select the date and time range for the events you want to see in the Event Viewer. By default no range is used.



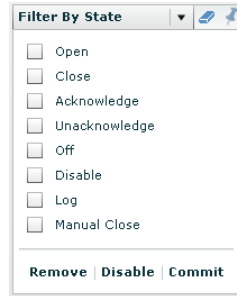
**Figure 3-17: Time Received Filter**

To set a date/time range, click the button next to the “Start Date/Time” field which will open a calendar next to it. From the calendar, choose the appropriate date, then use the slide below to choose the time. Click anywhere outside the calendar to accept the chosen date and time. Repeat this for the “End Date/Time”, then click the Commit button. This will cause only events that fall within the specified range to be shown in the Event Viewer, where the most recent will be loaded first, up to the max that can be shown.

**IMPORTANT:** This filter applies to the “Time Received” event field.

### 3.4.4 Filter By State

When “Filter By State” is selected from the Filters Panel drop-down seven check boxes will appear below that allow you to choose the states of the events loaded by the Event Viewer. By default events of all states are loaded.



**Figure 3-18: State Filter**

If you would like to view only events of a certain state, check that state type and click the Commit button. You can select multiple states and only events that are of any of the selected states will get loaded on Commit.

Active filters appear with a check mark. To de-activate a filter, un-check the box next to the state and click the Commit button.

### 3.4.5 Filter Panel Controls

Next to the Filters Panel drop-down, there is a clear button (🗑️) available for each filter. Clicking it will clear all the selections from that specific filter. Also, if the filter had been applied/committed, it will be removed. This will not impact any other filters that may be applied.

There are four possible actions that can be performed on the filters defined in this panel. These actions are represented by the three buttons at the bottom of the Filters Panel.

#### 3.4.5.1 Remove

Clicking this button will remove all filtering settings. All filtering criteria will be cleared causing only the most recent events to be loaded into the Event Viewer and appear in the events table. Also, if filtering had been disabled, it will be re-enabled.

NOTE: See section 3.4.5.2 below for details on disabling filters. While clicking disable will also turn off filtering, in that case the criteria will be preserved.

#### 3.4.5.2 Disable

If you have no filters active, this will prevent you from turning any filters on. If you have one or more filters active, this will disable them and thus show all the most recent events in the Event Viewer.

NOTE: The Disable button will become the Enable button when clicked.

#### 3.4.5.3 Enable

This appears only after the Disable button has been clicked. Clicking the Enable button will cause all filters to become active once again. Any filters that were active when Disable was clicked will be re-activated.

NOTE: The Enable button will become the Disable button when clicked.

### 3.4.5.4 Commit

Once filtering criteria are specified, clicking the Commit button will cause the filter to be applied. This triggers a query to the Events Database to load into the Event Viewer those events that match the criteria, and thus update what appears in the events table.

## 3.5 Search Panel

The Search Panel can be opened (or closed) by clicking on the Search button in the top right corner of the *Neuron Management Portal*. The panel will appear above the events table.



**Figure 3-19: Search Panel**

This panel includes a status indicator that will appear anytime events are being retrieved from the Events Database. When this is happening, you have the ability to stop the event retrieval at anytime by clicking the stop button next to the status bar.

To remove a search (clear a search so that events are loaded without keyword matching), click the Clear button (🗑️).

Clicking Refresh while a search has been applied will simply refresh the applied search (re-retrieve events from the database that match the search keywords).

Deleting all text from the search field and clicking the Search button (🔍) will do nothing. If you do not specify anything in the Search field, no search will occur. To clear a search, please click the Clear button (🗑️).

### 3.5.1 Doing a Simple Search

To do a keyword search, simply enter any keywords into the Search field and click the Search button (🔍). This will run a search through the Events Database for those events that contain any of the keywords in any of the following fields:

- Event ID (this must match exactly)
- Source Host
- Message
- Proxy Type
- Proxy Host
- Event Source (viewable via the Event Details panel).

The most recent events that match will be returned up to the maximum number of events the Event Viewer can display.

If you are not finding what you are looking for with a simple keyword search, you can attempt to refine your search criteria (see section 3.5.2 below).

**IMPORTANT:** All keyword search matching is case insensitive.

### 3.5.2 Refining a Search

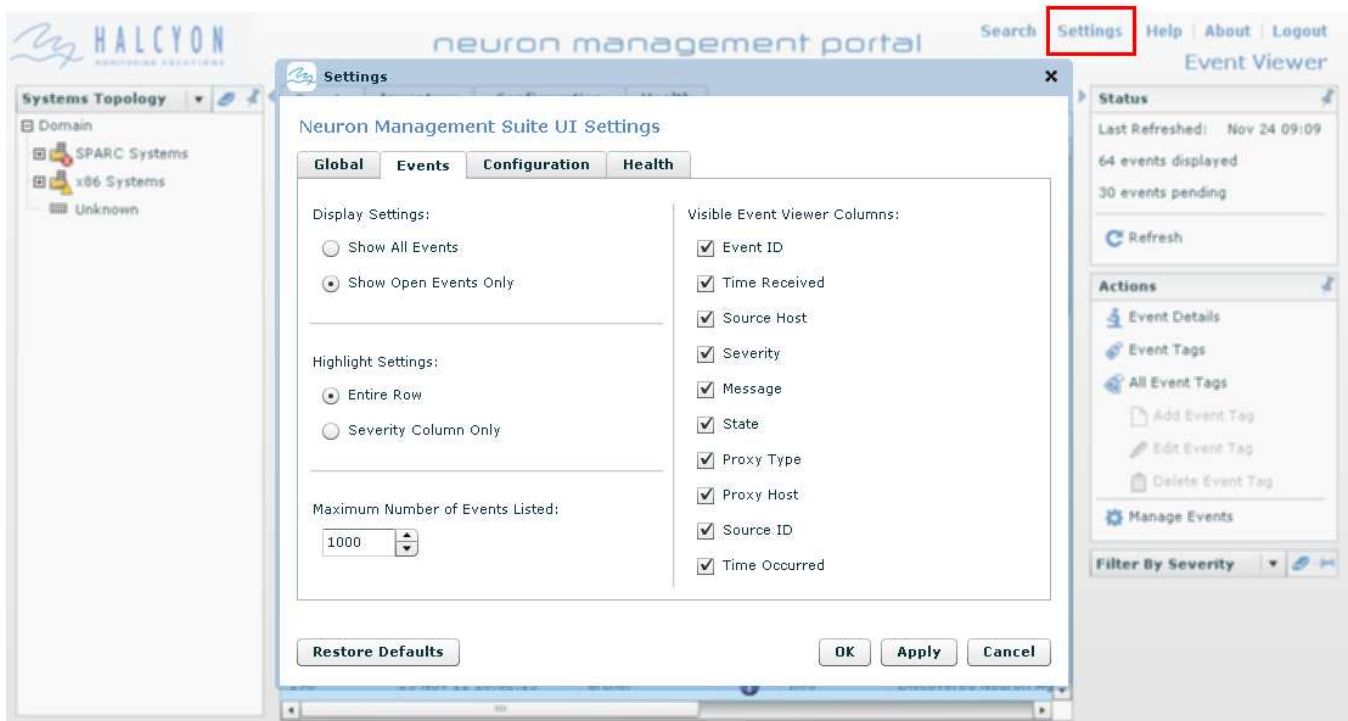
A keyword search can be refined by changing the keywords used, but it can also be refined to target only events of specific severities, in specific states and/or within a certain date/time range.

In order to apply any of these additional criteria, please make the required selections from the Filters Panel in the bottom right of the Event Viewer (see section 3.4). After making any selections within the Filters Panel and entering any keywords, click the Search button to start the search.

**NOTE:** If additional criteria have been specified, the search Clear button will NOT clear the additional criteria. To clear everything, please use the Remove button in the Filters Panel (3.4.5.1).

## 3.6 Event Viewer Settings

There are several ways to customize the look and behaviour of the Event Viewer by adjusting some of the available settings. To adjust the settings, open the Settings window by clicking "Settings" in the top right hand of the screen and then select the Events Tab. Make any desired changes and then click OK to save and close the window, or Apply to just save the changes.



**Figure 3-20: Event Viewer Settings**

### 3.6.1 Display Settings

By default, only active events (such as log events and open events that have not been closed) will be loaded into the Event Viewer. You can choose to show all events and then all events (including inactive/closed events) will be loaded into the Event Viewer (up to the max).

### 3.6.2 Highlight Settings

By default, each row of the events table is highlighted with that event's severity color. You can choose to instead only highlight the severity column.

### 3.6.3 Maximum Number of Events

Adjust the number of events loaded by the Event Viewer (max number of events that will be displayed in the events table). This value must be in the range of 100 to 10 000 (one hundred up to ten thousand).

### 3.6.4 Visible Columns

Check the box next to each column you want to see in the Event Viewer events table.

## 4 Managing Events (Event Manager)

By default, the Events Tab starts in View Mode where you can view Neuron Events. To switch to Manage Mode (also known as the Event Manager), click the "Manage Events" button (⚙️) in the Actions Panel to the right of the screen. This will open the Event Manager in the Events Tab.

The screenshot shows the Neuron Event Manager interface. The main panel displays a table of rules with the following columns: Status, Name, Type, Category, Description, Run Policy, and Pending. The table contains 11 rules, including 'Accept Incoming SNMP', 'Email Sys Admin', and 'Ops Center Acknowledged'. To the right of the table is an 'Actions' panel with options like 'New Rule', 'Edit Rule', 'Import Rules', 'View Rule Details', 'Run Pending Actions', 'Clear Pending Actions', 'Test Actions', 'Copy Rules', 'Enable Rules', 'Disable Rules', 'Delete Rules', and 'View Events'. Below the actions panel is a 'Filter By Rule Type' section with a tree view showing 'Inbound', 'SNMP', 'Ops Center', and 'Response'.

| Status | Name                       | Type     | Category       | Description                                   | Run Policy  | Pending |
|--------|----------------------------|----------|----------------|---|-------------|---------|
| ⏻      | Accept Incoming SNMP       | Response | SNMP-IN        | Rules for incoming SNMP                       | Immediately | 0       |
| ⏻      | Email Sys Admin            | Response | CRITICAL - SYS | Notify sys-admin for critical systems issues. | Immediately | 0       |
| ⏻      | Ops Center Acknowledged    | Inbound  |                | Rule Ops Center Acknowledged Fault Events     | immediately | 0       |
| ⏻      | Ops Center Automatic Clos  | Inbound  |                | Rule Ops Center Automatic Closed Fault Ever   | immediately | 0       |
| ⏻      | Ops Center Fault Events    | Inbound  |                | Rule Ops Center Fault Events                  | immediately | 0       |
| ⏻      | Ops Center Problem Create  | Inbound  |                | Rule Ops Center Problem Created Fault Ever    | immediately | 0       |
| ⏻      | Ops Center Problem Repea   | Inbound  |                | Rule Ops Center Problem Repeated Fault Eve    | immediately | 0       |
| ⏻      | Ops Center Raised Alert Fa | Inbound  |                | Rule Ops Center Raised Alert Fault Events     | immediately | 0       |
| ⏻      | Ops Center UnAcknowledgt   | Inbound  |                | Rule Ops Center UnAcknowledged Fault Ever     | immediately | 0       |
| ⏻      | Ops Center User Closed Fa  | Inbound  |                | Rule Ops Center User Closed Fault Events      | immediately | 0       |
| ⏻      | Tivoli                     | Response | TIVOLI         | Forward all events to Tivoli                  | Immediately | 0       |

Figure 4-1: Events Tab Event Manager

The center panel is dominated by a table that displays Rules that have been setup to manage events. The panels around the table allow you to create and manage your Rules.

Event Manager Rules can be Inbound or Response Rules.

Inbound Rules define which messages from 3<sup>rd</sup> party products are converted into Events.

Response Rules are sets of event filters, actions and schedules. During the period defined by the schedules, when an event occurs that matches the filters, the actions will be executed on the *Neuron Management Suite* Server.

**IMPORTANT NOTE 1:** The *Neuron Management Portal* has a 30 minute session timeout. After 30 minutes of inactivity (no typing, no mouse movement, etc) you will automatically be logged out. If you have any unsaved changes and your session does timeout, those changes will be lost. Please save changes regularly.

**IMPORTANT NOTE 2:** While the *Neuron Event Manager* does not prevent you from using special characters, under certain circumstances some characters may result in unexpected behaviour. This may be as severe as causing all your rules to stop functioning. It is strongly recommended that only alpha-numeric and underscore characters be used unless otherwise explicitly stated.

Table 4-1: Rules Table

| Column      | Description  |
|-------------|--|
| Status      | Whether this Rule will be applied against incoming messages (Inbound Rules) or events (Response Rules).<br>A green icon (🟢) indicates that the Rule is both Active and Enabled (see below) and will thus be applied.<br>A white icon (🔕) indicates the Rule is Inactive, Disable or both Inactive and Disabled and thus will not be applied. |
| Name        | The unique name of the Rule.   |
| Type        | The type of the Rule.<br>Inbound Rules are applied against incoming 3 <sup>rd</sup> party messages and can be defined for incoming SNMP traps or Oracle Enterprise Manager Ops Center notifications.<br>Response Rules are applied against Neuron Events and are used to act in response to a matching event.                                |
| Category    | The category the Rule was assigned to (specified when the Rule is created or edited).  |
| Description | A description of what the Rule does (specified when the Rule is created or edited).  |
| Run Policy  | Used for Response Rules, this indicates how the Rule's actions will be run if an event matches the Rule. Refer to section 4.2.5 for more details.  |
| Pending     | Used for Response Rules to indicate the number of actions that the rule is waiting to execute (if the Run Policy is not "run immediately")   |
| Last Run    | Used for Response Rules to indicate the last time the Rule matched an event and ran its specified actions.   |
| Active      | Whether or not the Rule is within the defined schedule. If no schedule is defined, the rule will always be Active.   |
| Enabled     | Whether or not the Rule has been manually Enabled or Disabled. By default, all new Rules are Disabled and will need to be manually Enabled.  |

## 4.1 Status Panel

Information on the status of the Event Manager can be found in the Status Panel on the top right side of the Event Manager.

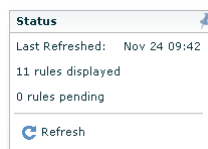


Figure 4-2: Event Manager Status

Last Refreshed: This is the last time the display of Rules was refreshed.  
 Y rules displayed: This indicates the number of Rules being shown in the Rules table.  
 X rules pending: This indicates the number of Rules that have actions pending.

## 4.2 Creating and Editing Response Rules

Response Rules are sets of event filters, actions and schedules. During the period defined by the schedules, when an event occurs that matches the filters, the actions will be executed on the *Neuron Management Suite* Server.

To create a new Response Rule from the Event Manager window, just click the New Rule button in the Actions Panel to launch the "Event Manager :: New Rule" window. By default you are creating a Response Rule.

To edit an existing Response Rule, select the Rule from the Rules table and click the Edit Rule button in the Actions Panel to launch the "Event Manager :: Edit Rule" window.

All details concerned with creating and editing Response Rules are the same after this point.

When in Create or Edit Mode, clicking the Apply Button in the Actions Panel will save the Rule up to that point in time. Clicking the Cancel Button will discard any changes that have not been saved/applied and return you to the Event Manager's main window.

You must be in the "Managers" or "Admins" user group to Create or Edit a Rule. Refer to the *Neuron Management Server User's Guide* for more details about Users and Groups.

### 4.2.1 Overview

General information about the Rule is defined in the Overview Tab.

**Table 4-2: Response Rule Overview Tab Fields**

| Field            | Description  |
|------------------|--|
| Type             | The type of the Rule.  |
| Stream           | The Inbound Rule Stream.   |
| Name             | The Rule's name must be unique and must contain at least one alpha-numeric character.  |
| Description      | A description of what the Rule is for (optional).  |
| Category         | The category the Rule is being assigned to (optional).   |
| Last Modified    | This is recorded automatically by Neuron and is not editable. Once the Rule has been created, this will show the date and time the Rule was last saved.      |
| Last Modified By | This is recorded automatically by Neuron and is not editable. Once the Rule has been created, this will show the username of the last user to save the Rule. |

## 4.2.2 Filters

The Filters defined for a Response Rule will determine which events satisfy the Rule. If the event matches the filters, the Actions defined in the Rule will be triggered. If there are no filters defined, the Rule will match all events.

To create a Filter, click "Filter by...". Once the Filter is created, select the field to filter on from the "Field" column's drop-down and then choose the operation to use in comparing the value of that field from the event to the filter's value. Finally, enter a value or values to match against in the Value field. For Severity and State you will be given a list to choose from. For all others, enter a single value or multiple values separated by commas.

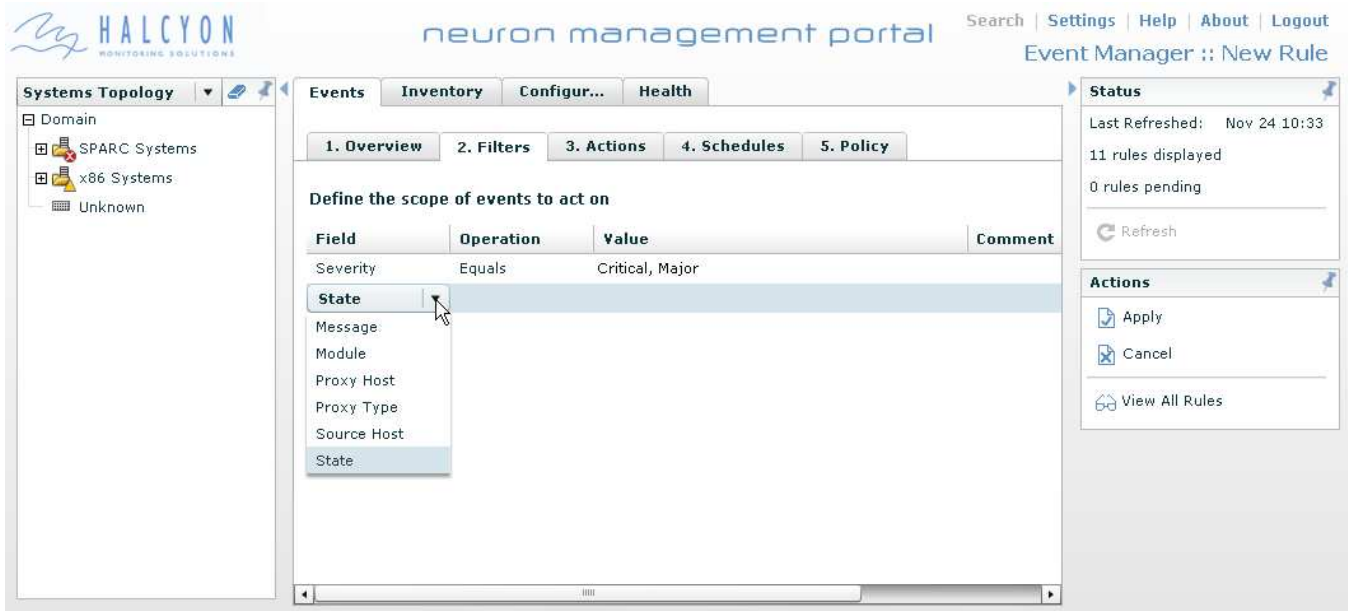


Figure 4-3: Response Rule Filters Tab

The Filter fields used for the Response Rules match Event fields that can be seen in the *Neuron Event Viewer* (see section 3).

Table 4-3: Response Rule Filter Types

| Field   | Description   |
|---------|---|
| Message | <p>A Message filter allows you to create a Rule that will match on the contents of an event's Message field. You can create a filter that will accept events when the message contains or does not contain the text specified in the Value field.</p> <p>NOTE: The Value to match against the message cannot contain the comma character, as this is used to delimit a list of values (a Contains filter with a Value of "This, That" will match messages that contain "This" or "That").</p> |
| Module  | <p>Creates a Rule that will only match events that contain (or do not contain) the specified text as part of the event's Module value. This property is generally used to identify the component or subcomponent within an enterprise monitoring framework that detected the initial fault or error condition.</p>  |

For example, if you have an existing Sun Management Center server layer with the PrimeAlert EventAction module configured to forward alarms to *Neuron Management Suite*, the Module field is set to the Sun Management Center module and instance (if applicable) in the generated alarm in the form of *module[.instance]*.

Furthermore, Rules imported from PrimeAlert EventAction for Sun Management Center (see section 4.4.1) may have Module type filters defined.

The Module value is derived from the eventSource URI of the event (if the value is set).

To determine the Module value from the eventSource of a Sun Management Center alarm:

- 1) Open the *Neuron Event Viewer* (see section 3) and select the alarm that came from Sun Management Center.
- 2) Open the Event Details for the selected event (see section 3.3.1).
- 3) Look at the Event Source field, it will display a value that looks like this:

```
sunmc://100.200.1.1:1161/mod/health-monitor/DISK/diskTable/diskEntry/disk-rule#sdl/
```

The Module value is the string after “sunmc://<host>:<port>/mod/” and before the next “/”. In the above example, the Module is “health-monitor”.

To determine the Module value from the eventSource of a Neuron Agent alarm, follow the above steps. The eventSource of a Neuron Agent alarm will look like this:

```
neuron://100.200.1.1:1161/mod/HALSolarisSystemAlert/cpu/average/
```

The Module value is the string after “neuron://<host>:<port>/mod/” and before the next “/”. In the above example, the Module is “HALSolarisSystemAlert”.

|             |  |
|-------------|--|
| Proxy Host  | <p>You may have <i>Neuron Management Suite</i> configured to receive events from a 3<sup>rd</sup> party proxy (such as Oracle Enterprise Manager Ops Center).</p> <p>The Proxy Host allows you to filter on the host the proxy is running on. For instance, if you have Oracle Enterprise Manager Ops Center running on host bedrock, you can create a Rule with a “Proxy Host equals bedrock” filter that will then act on all the events that come through bedrock.</p> <p>NOTE: This filter is handled the same way as the “Source Host” filter below.</p>  |
| Proxy Type  | <p>You may have <i>Neuron Management Suite</i> configured to receive events from a 3<sup>rd</sup> party proxy (such as Oracle Enterprise Manager Ops Center).</p> <p>The Proxy Type allows you to setup your Rule to apply to events that have come from (or not come from) a specific proxy. For instance, if you want to take a specific action against events that have come in from Oracle Enterprise Manager Ops Center, create a Rule with a “Proxy Type equals Ops Center” filter. Separate actions can then be taken for all other events by creating a Rule with a “Proxy Type not equals Ops Center” filter.</p> |
| Severity    | <p>Allows you to create a Rule that will only match events that are of (or are not of) the specified severity (or severities).</p> <p>Once you have selected an Operation (Equals or Not Equals), click on the Value field and check all severities the filter should match on. The selected severities will appear as a list which will be ORed when matching, so “Severity equals CRITICAL, MAJOR” matches events that have a Critical or a Major severity.</p>  |
| Source Host | <p>Allows you to create a Rule that will only match events that occurred on the specified host (or hosts).</p> <p>For instance, if you would only like the Rule to match events coming from your New York datacenter where all hosts are of the form [shortName].nycdatcenter.com, you could specify a Source Host filter using the Contains operation with the value “nycdatcenter”.</p> <p>To filter on multiple hosts, you can provide a list of values to match on, separating each with a comma. For instance, if you only want the Rule to apply to events coming from</p>   |

|       |  |
|-------|--|
|       | <p>hosts twilight and mammoth, create a Source Host filter using the Equals operation and "twilight, mammoth" as the Value.</p> <p>NOTE: If specifying a list, values must be separated by a comma and then no more than one space, otherwise those values will not be taken to be a list.</p>   |
| State | <p>Allows you to create a Rule that will only match events that are (or are not) of the specified state (or states).</p> <p>Like the Severity filter, after selecting either Equals or Not Equals as the Operation, click the Value field and check all the states the filter should match on. The selected states will appear as a list which will be ORed when matching, so "State not equals CLOSE, LOG" matches all events except those of the Close or Log state.</p> |

### 4.2.2.1 Using Multiple Filters

You can create multiple filters for a single Rule by simply clicking "Filter by..." at the bottom of the Field column. This will cause a new filter row to be created and you can define your next filter just as outlined above.

If there are multiple filters, they will be ANDed together when matching against events.

Once one filter is defined, the available Fields and Operations will dynamically adjust based on what is valid:

- 1) Once a Filter has been setup with a Field using an Equals Operation, that field cannot be used in any other filter for that rule. In other words, once you define "Source Host equals twilight", "Source Host" will no longer appear in the Field list until the previous filter is deleted or change to use a different operation.
- 2) Once a Filter has been setup with a Field using an Operation other than Equals, Equals will no longer be available as an operation for other filters using that field. In other words, once you define "Source Host contains mammoth", Equals will no longer appear in the Operation list for other Source Host filters.

If you need to setup filters that are ORed together, you will need to create two separate Rules, each with one of the ORed filters.

### 4.2.2.2 Deleting Filters

To delete a filter from a Rule, simply click the "X" that appears in the last column of the Filter table (to the right of the Comment column). The filter will be removed immediately, but you will need to click Apply to save the change.

### 4.2.2.3 Additional Notes about Filters

- 1) If you define a filter, changing the filter type (Field column) afterwards will cause the Operation and Value fields to be reset.
- 2) If you create a filter but don't select an Operation, the default Operation (the first in the list) will be used.

## 4.2.3 Actions

The Actions defined for a Response Rule are used to determine what to do when an event occurs that matches the given Rule's Filters. If the event matches the filters, the Actions defined in the Rule will be triggered. This action could be to send an Email to someone to alert them of the situation or it could be to run a script that could take restorative action. All possible Actions are documented below.

To create an Action, click "Select and option...". Once the Action is created, select the action to run from the Action column's drop-down. With the action selected, click in the Parameters field and enter the parameters required to run that operation.

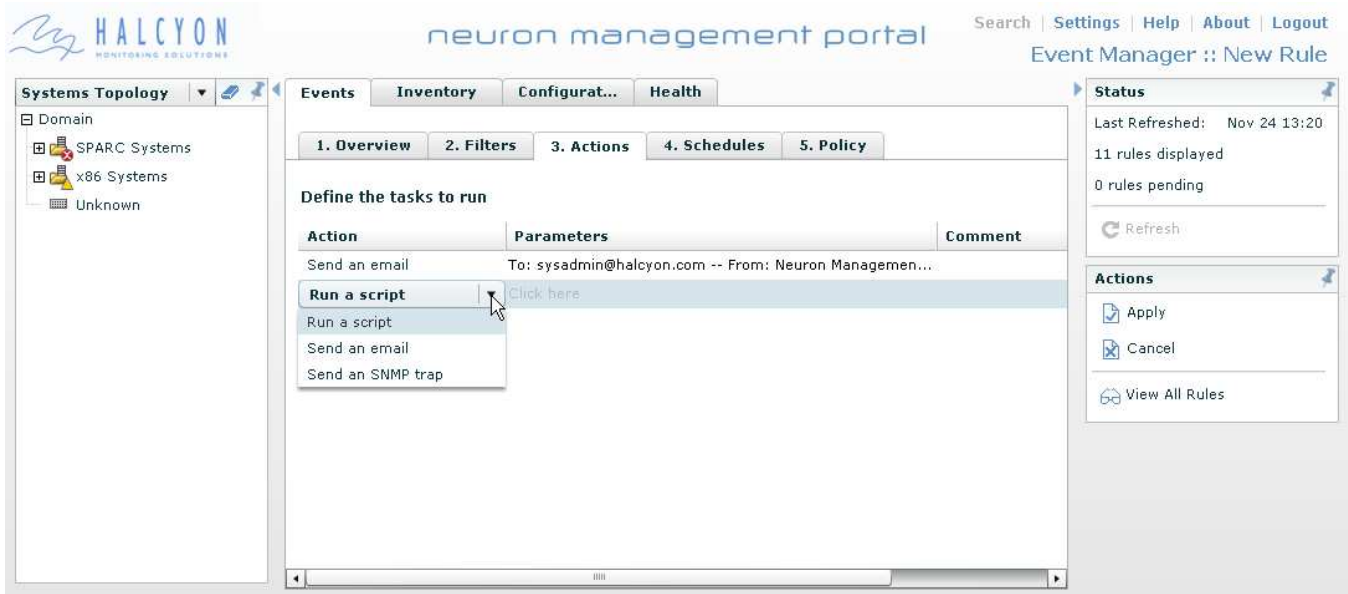


Figure 4-4: Response Rule Actions Tab

### 4.2.3.1 Default Actions Available

The *Neuron Management Suite* provides a few Actions for use out of the box with no additional licenses required. Please refer to section 4.2.3.2 for information on additional actions available using Halcyon's *Neuron Integration Adapters*.

Table 4-4: Response Rule Default Actions

| Action       | Description   |
|--------------|---|
| Run a script | <p>A Script action allows any executable to be run when an event matches the Rule. The script will run on the <i>Neuron Management Suite Server</i> and must be executable by the <i>halcyon</i> user.</p> <p>The Command is the path to the script to execute. If the path is not absolute, it will be taken to be relative to [LOCALDIR]/bin (refer to <i>Neuron Management Suite Installation Guide</i> for details on LOCALDIR).</p> <p>If the script expects any arguments, provide them in the Arguments field the same as you would on the command line.</p> |

The Email Action will send an email alert when an event matches the Rule. In this case, all characters that are acceptable in email addresses are acceptable here.

In the From field, enter what you would like to appear as the sender of the email.  
 In the To field, enter all the recipient email addresses. Multiple addresses must be separated by a single space (no comma)  
 In the Subject field, enter what you would like to appear as the subject of the email. Refer to section 4.2.3.4 for all available options.

For email actions to work, *Neuron Management Suite* must be pointed to your mail server. Please refer to the "Halcyon Email Adapter Configuration Instructions" in README.config.

Send an  
SNMP  
Trap

The SNMP Trap Action will send an SNMP trap to any host with the provided event details when an event matches the Rule. The MIBs can be found in the [LOCALDIR]/conf/module directory as GenericAdapter\_v1.mib and GenericAdapter\_v2.mib (refer to *Neuron Management Suite* Installation Guide for details on LOCALDIR).

The trap's Target should be specified as <targetHost>:<targetPort>. You can specify multiple targets by separating each with a space.

### 4.2.3.2 Additional Actions from Adapters

Beyond the default Actions, other Actions can be made available using Halcyon's *Neuron Integration Adapters*. For any of these Actions to appear in the Actions list, the following must be done:

- 1) The associated Adapter must be configured. Please refer to README.config for details on configuring each Adapter.
- 2) The associated Adapter must be Enabled from the Server Configuration Tab (see "Accessing Server Configuration Page" in README.config).
- 3) The associated Adapter must be licensed.

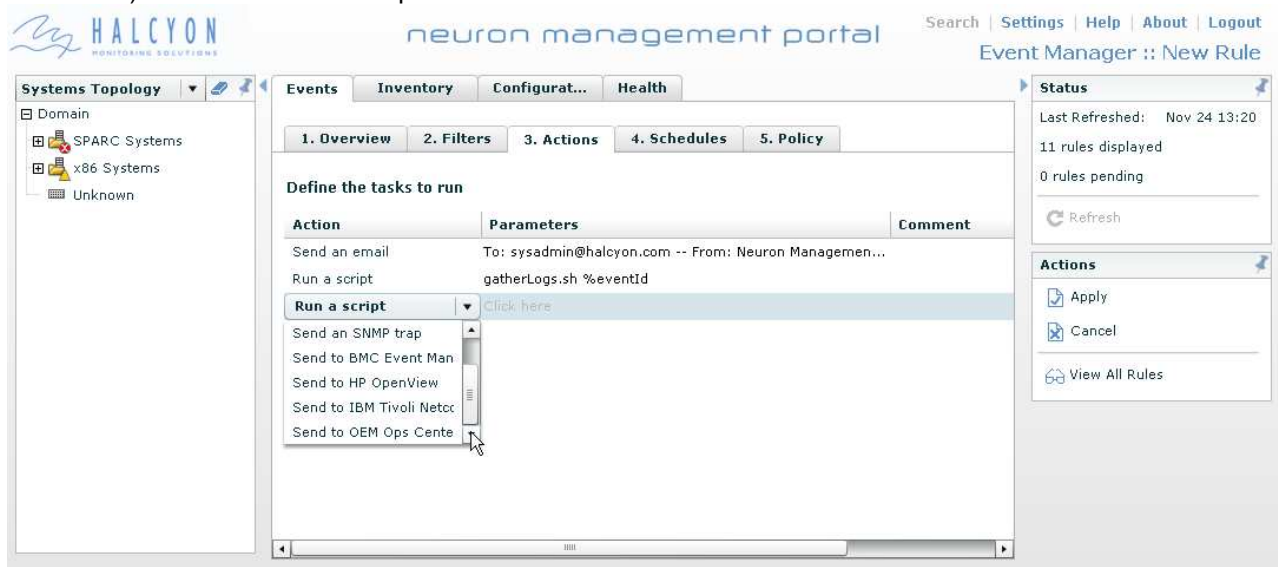


Figure 4-5: Response Rule Additional Actions

**Table 4-5: Response Rule Additional Actions from Adapters**

| Action                     | Adapter           | Description  |
|----------------------------|-------------------|--|
| Send to BMC Event Manager  | BEM Adapter       | This Action will send a trap to the specified BMC Event Manager. The parameter for this Action should be the BMC host and port the trap is to be received at (such as twilight:2125).  |
| Send to HP OpenView        | OpenView Adapter  | This Action will send a trap to the specified HP OpenView installation. The parameter for this Action should be the OpenView host and port the trap is to be received at (such as twilight:2123).  |
| Send to IBM Tivoli         | Tivoli Adapter    | This Action will forward the Neuron Event to IBM Tivoli using Tivoli's postmsg. The Action can be configured with either an IBM Tivoli TEC configuration file, or the IBM Tivoli hostname. If both parameters are specified, the configuration file will be used.<br><br>The TEC configuration file should be located in the [LOCALDIR]/conf directory as indicated in the Tivoli configuration instructions in README.config. |
| Send to IBM Tivoli Netcool | Netcool Adapter   | This Action will send a trap to the specified IBM Tivoli Netcool installation. The parameter for this Action should be the Netcool host and port the trap is to be received at (such as twilight:2121).  |
| Send to OEM Ops Center     | OpsCenter Adapter | This Action will inject a notification into Oracle Enterprise Manager Ops Center. For the parameter, select from the drop-down list the Ops Center connection to inject the notification to. The connections are setup during the Adapter configuration (see README.config).   |

### 4.2.3.3 Using Multiple Actions

A single Rule can have multiple Actions associated with it, and if an event does match the Rule, all the defined Actions will be executed. While you can have several distinct Actions for a single Rule (such as Send an email and Run a script), it is also possible to have several Actions of the same type. For instance, you could setup several email actions that go to different recipients, but perhaps have a different From address or subject line which would then be filtered differently by those individuals.

### 4.2.3.4 Event Data for use in Actions

Much of the data from the event that matched the Rule can be used in the Action the Rule triggers. For SNMP trap actions, this data is automatically included in the trap varbinds (see the provided MIBs). For other actions, however, it may be desirable to include information, such as the event's proxy type as a script parameter or the event's severity as part of the email subject line.

The following is a list of the parameters that can be used in the Rule Actions. This list can be viewed in a tooltip when hovering over any parameter field that accepts them.

An example email Subject line could be "A %eventSeverity event occurred on %asset" which could then appear as "A CRITICAL event occurred on twilight".

**Table 4-6: Response Rule Event Data Parameters**

| Parameter      | Description   |
|----------------|---|
| %eventMessage  | The contents of the event's Message field.  |
| %asset         | The host the event pertains to (Source Host).   |
| %eventState    | The state of the event (Open, Close, etc).  |
| %eventSeverity | The severity of the event (Info, Critical, etc).  |
| %proxy         | The proxy host the event came from (if the event came from a proxy; blank otherwise).   |
| %proxyType     | The type of proxy the event came from (if the event came from a proxy; blank otherwise).  |
| %eventId       | The event's unique identifier within the <i>Neuron Management Suite</i> (can be matched up to Event ID in the Event Viewer).      |
| %nativeEventId | The original id of the event on the originating system, if one is specified/provided.   |
| %eventSource   | A URI formatted string indicating where the event came from (such as snmp://twilight:1161/1.3.6.1.4.1.42.12.2.1.2.2.1.8).         |
| %eventTags     | A list of the names of the Event Tags whose patterns match with the event (see section 3.3.2 for more information on Event Tags). |

### 4.2.3.5 Deleting Actions

To delete an Action from a Rule, simply click the "X" that appears in the last column of the Action table (to the right of the Comment column). The Action will be removed immediately, but you will need to click Apply for the change to be saved.

### 4.2.4 Schedules

The Schedules defined for a Response Rule are used to determine when the Rule will be active or inactive. A Rule can have as many schedules as necessary to define the time windows during which a Rule should be active.

If an event matches the Rule, but occurred outside the time windows defined by the Schedules, the Rule's Actions will not be executed. If an event matches the Rule and occurred while the Rule was active, the Rule's Actions will be executed, even if by the time the event is processed the Rule is inactive. The schedules work on the time the event occurred, not necessarily the current time.

If no Schedule is defined, the Rule will always be active.

You create a Schedule by clicking "Add schedule..." and then defining the Schedule's Type, Value and value comparison Operator that will indicate when the Rule should be active.

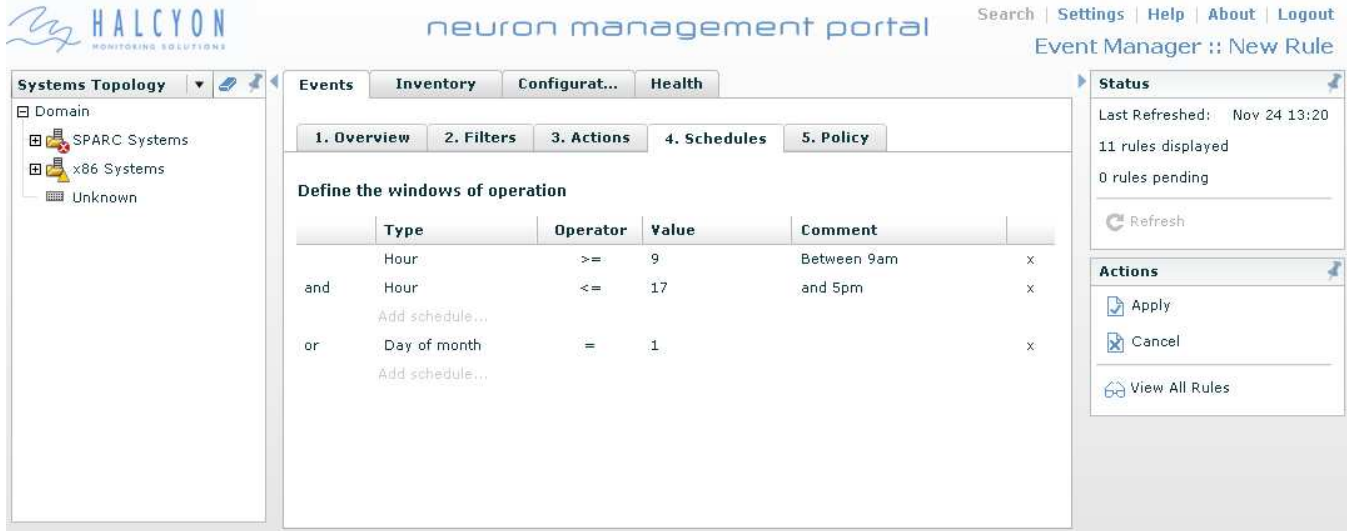


Figure 4-6: Response Rule Schedules Tab

Table 4-7: Response Rule Schedule Types

| Type          | Description  |
|---------------|--|
| Hour          | This is the hour during the day falling between 0 and 23. The default is the current hour.                             |
| Month         | This is the name of the month (January, February, etc) with the default being the current month.                       |
| Year          | This is the year in the form of YYYY with the default being the current year.  |
| Date          | This is a full date of the form "<Month> DD YYYY" that can be picked from a calendar. The default is the current date. |
| Time          | This is a time value of the form HH:MM where HH is the hour between 0 and 23. The default will be the current time.    |
| Day of week   | This is the name of the day of the week (Sunday, Monday, etc) with the default being the current day.                  |
| Day of month  | This is the day of the month with the default being the current day in the current month.                              |
| Week of month | This is a number for the week of the month. The default is the current week of the current month.                      |
| Week of year  | This is the number for the week of the year. The default is the current week of the current year.                      |

#### 4.2.4.1 Creating Schedules

A Rule's Schedule is defined by one or more Time Windows that indicate when the Rule should be active. In the screenshot above, there are 2 Time Windows defined: Between 9:00am and 5:00pm, everyday and all day on the 1<sup>st</sup> of each month.

When scheduling when a Rule should be active, you are building a set of Time Windows defining when it should be active. Time Windows are made more restrictive by selecting “and” in the first column and additional Time Windows get created by selecting “or” in the first column.

To add to a Time Window, just click “Add schedule...” below the Time Window you want to add to and then define the part of the Window on the row that is created.

To create a new Time Window, click any “Add schedule...” that appears on the screen, then click in the left most column of the created row. In the drop-down that appears, select “or” and click anywhere on the screen. This will break that new row away from the existing Time Window to create a new Time Window in the Schedule.

After creating all the Time Windows for the Schedule, a Rule will be active if all the ANDed conditions (which make up a single Time Window) are satisfied. If there are multiple Time Windows (ORed), the Rule will be active when all the ANDed conditions of a single Time Window are satisfied.

#### 4.2.4.2 Example Schedule: Active 9:00am to 5:00pm Mon-Fri

The following will walk you through defining a typical Schedule:

- 1) Click “Add schedule...” under the Type column and then select Time from the Type drop-down.
- 2) Click the Operator field for that row and select “between” for the first part of the Time Window.
- 3) Click in the Value field and enter 9:00 and 17:00 in the window that appears to define the active time as being between 9:00am and 5:00pm.

Define the windows of operation

| Type            | Operator | Value   | Comment |
|-----------------|----------|---------|---------|
| Time            | between  | 9 : 0   | x       |
| Add schedule... |          |         |         |
|                 | and      | 17 : 00 |         |

**Figure 4-7: Create a Between Time Window**

- 4) Click “Add schedule...” at the bottom of the Type column and then select Day of week from the Type drop-down.
- 5) Click the Operator field for that row and select “between” for the second part of the Time Window.
- 6) Click in the Value field, and in the window that appears select Monday from the first drop-down and Friday from the second drop-down.

#### 4.2.4.3 Schedule Time Zones

If your *Neuron Event Manager Client* and *Neuron Management Suite Server* are in two different time zones, the Schedule must be defined for the Server time zone. All Rules are applied against events on the Server and thus the Schedule must be based on the centralized Server time.

#### 4.2.4.4 Deleting Schedules (or parts of Schedules)

There is a small “X” in the right most column of each row in the Schedules table that is used to delete that particular row. To delete part of a Schedule, click the “X” for the row that defines the part of the Schedule to delete. To delete an entire Schedule, you will need to click the “X” for each row of the Schedule.

You will need to click Apply to save the changes.

## 4.2.5 Policy

The Policy defined for a Response Rule indicates when and how the specified Actions are executed. By default, the Actions will be run immediately, as soon as an event matches the Rule. However, it is possible to delay this execution and even repeat it.



Figure 4-8: Response Rule Policy Tab

### 4.2.5.1 Run Policy (Immediate vs Delay)

When the Run Policy is set to “run immediately”, the Actions setup for the Rule will be executed as soon as an event matches the Rule.

When the Run Policy is set to “run after a Y minute delay”, the Rule’s Actions will be executed only if the event that matched the Rule has not been closed or acknowledged within the Y minute period. Perhaps there is something that is only a problem if it persists for more than 5 minutes, then setting up a Rule for that event with a delay of 5 minutes would ensure appropriate people would only be notified if the condition does persist for that period of time.

### 4.2.5.2 Repeat Policy

Both immediate and delayed Actions can be executed repeatedly until the event is acknowledged or closed. Simply click the check-box and specify how often (in minutes) the actions should be executed. They will continue to execute until the event is acknowledged or closed, or the Pending execution is cancelled (see section 4.4.4 for clearing pending actions).

**NOTE:** Some versions of Oracle Enterprise Manager Ops Center do not send out notifications to close events. If this is the case, a Rule setup for Ops Center and set to have a Repeat Policy could continue to execute actions until they are manually cancelled (see section 4.4.4 for clearing pending actions).

## 4.3 Creating and Editing Inbound Rules

Inbound Rules examine incoming 3<sup>rd</sup> party data and are used to determine whether the incoming data (such as an SNMP trap or an Ops Center Notification) should become an event within Neuron.

To create a new Inbound Rule from the Event Manager window, click the New Rule button in the Actions Panel to launch the “Event Manager :: New Rule” window, and then change the Type in the Overview tab to Inbound.

To edit an existing Inbound Rule, select the Rule from the Rules table and click the Edit Rule button in the Actions Panel to launch the “Event Manager :: Edit Rule” window.

All details concerned with creating and editing Inbound Rules are the same after this point.

When in Create or Edit Mode, clicking the Apply Button in the Actions Panel will save the Rule up to that point in time. Clicking the Cancel Button will discard any changes that have not been saved/applied and return you to the Event Manager’s main window.

You must be in the “Managers” or “Admins” user group to Create or Edit a Rule. Refer to the *Neuron Management Server User’s Guide* for more details about Users and Groups.

### 4.3.1 Overview

General information about the Rule is defined in the Overview Tab.

**Table 4-8: Inbound Rule Overview Tab Fields**

| Field            | Description  |
|------------------|--|
| Type             | The type of the Rule. In this case, choose Inbound.  |
| Stream           | The Inbound Rule Stream. Right now Neuron supports SNMP and Ops Center Inbound data.   |
| Name             | The Rule’s name must be unique and must contain at least one alpha-numeric character.  |
| Description      | A description of what the Rule is for (optional).  |
| Category         | The category the Rule is being assigned to (optional).   |
| Last Modified    | This is recorded automatically by Neuron and is not editable. Once the Rule has been created, this will show the date and time the Rule was last saved.      |
| Last Modified By | This is recorded automatically by Neuron and is not editable. Once the Rule has been created, this will show the username of the last user to save the Rule. |

### 4.3.2 Ops Center Stream Filters

The Filters defined for an Ops Center Stream Inbound Rule will determine which Ops Center Notifications satisfy the Rule and thus become events within Neuron. If the notification matches the filters, it will

become a Neuron Event. If there are no filters defined, the Rule will match all incoming Ops Center Notifications.

To create a Filter, click “Filter by...”. Once the Filter is created, select the field to filter on from the “Field” column’s drop-down and then choose the operation to use in comparing the value of that field from the notification to the filter’s value. Finally, enter a value or values to match against in the Value field.

For Ops Center Stream Inbound Rules, the Proxy Type filter is set to Ops Center and cannot be changed.

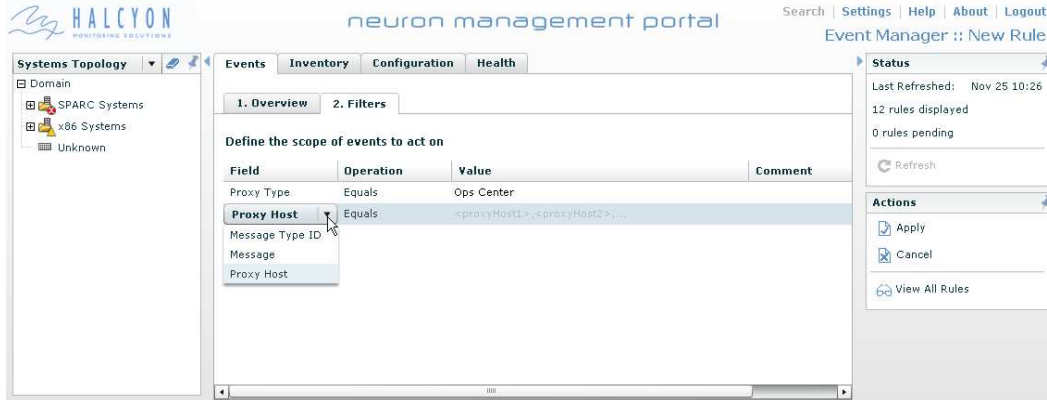


Figure 4-9: Ops Center Stream Inbound Rule Filters Tab

The Filter fields used for the Ops Center Stream Inbound Rules match details from the Ops Center Notification.

Table 4-9: Ops Center Stream Inbound Rule Filter Types

| Field           | Description  |
|-----------------|--|
| Message Type ID | A Message Type ID filter allows you to create a Rule that will only match Ops Center Notifications that contain specific Message Type IDs. Oracle Enterprise Manager Ops Center sets an ID for each notification as part of the message.   |
| Message         | A Message filter allows you to create a Rule that will match on the contents of an Ops Center Notification Message field. You can create a filter that will accept events when the message contains or does not contain the text specified in the Value field.<br>NOTE: The Value to match against the message cannot contain the comma character, as this is used to delimit a list of values (a Contains filter with a Value of “This, That” will match messages that contain “This” or “That”). |
| Proxy Host      | The Proxy Host allows you to filter on the host the proxy is running on. For instance, if you have Oracle Enterprise Manager Ops Center running on host bedrock, you can create a Rule with a “Proxy Host equals bedrock” filter that will then act on all the events that come through bedrock.<br>If you want to filter on multiple hosts, separate them using commas.   |

### 4.3.2.1 Using Multiple Filters

You can create multiple filters for a single Rule by simply clicking “Filter by...” at the bottom of the Field column. This will cause a new filter row to be created and you can define your next filter just as outlined above.

If there are multiple filters, they will be ANDed together when matching against incoming notifications.

If you need to setup filters that are ORed together, you will need to create two separate Rules, each with one of the ORed filters.

### 4.3.2.2 Deleting Filters

To delete a filter from a Rule, simply click the “X” that appears in the last column of the Filter table (to the right of the Comment column). The filter will be removed immediately, but you will need to click Apply to save the change.

### 4.3.2.3 Additional Notes about Filters

- 1) If you define a filter, changing the filter type (Field column) afterwards will cause the Operation and Value fields to be reset.
- 2) If you create a filter but don't select an Operation, the default Operation (the first in the list) will be used.

### 4.3.3 SNMP Stream Filters

The Filters defined for an SNMP Stream Inbound Rule will determine which incoming SNMP traps satisfy the Rule and thus become events within Neuron. If the trap matches the filters, it will become a Neuron Event. An SNMP Stream Inbound Rule cannot be created without filters.

You first must define the required Snmp Version filter and that will determine what other filters will be required. For instance, for SNMPv1, the Enterprise OID, Generic Trap Type and Specific Trap Type must be defined.

To create a Filter, click “Filter by...”. Once the Filter is created, select the field to filter on from the “Field” column's drop-down and then choose the operation to use in comparing the value of that field from the SNMP trap to the filter's value. Finally, enter a value or values to match against in the Value field.

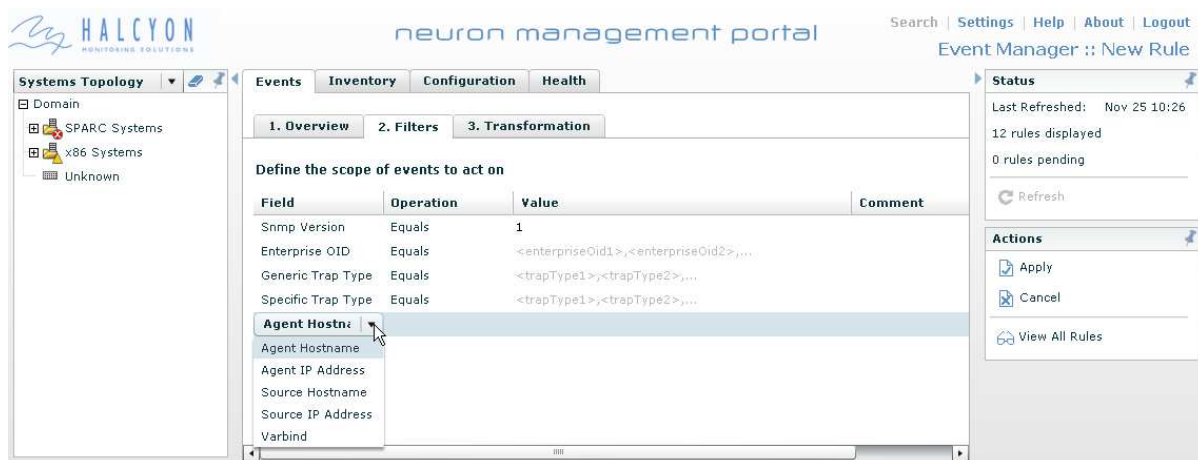


Figure 4-10: SNMP Stream Inbound Rule Filters Tab

The Filter fields used for the SNMP Stream Inbound Rules match details from the SNMP Trap.

**Table 4-10: SNMP Stream Inbound Rule Filter Types**

| Field                        | Description  |
|------------------------------|--|
| Snmp Version                 | Specify the SNMP version of the SNMP traps that should be processed. Currently, SNMP versions 1, 2, and 3 are supported.<br>After you select an SNMP version from the drop-down box, additional filters will be made available.  |
| Enterprise OID               | SNMP v1 only<br>The Enterprise OID of the v1 traps to accept. You may use the "Begins With" Operator to accept a large set of traps.   |
| Generic Trap Type            | SNMP v1 only; valid values are 0 to 6 inclusive.<br>The Generic Trap Type of the v1 traps to accept.   |
| Specific Trap Type           | SNMP v1 only when Generic Trap Type Equals 6.<br>The Specific Trap Type of the v1 traps to accept.   |
| Trap OID                     | SNMP v2/v3 only<br>This filter is similar to the Enterprise OID for SNMP v1 traps. You can select the operator "Begins With" together with this filter in order to specify traps whose trap OID only needs to start with the provided value.   |
| Agent Hostname / IP Address  | Allows you to create a Rule that will only match SNMP traps that occurred on a specific agent host. The Agent Hostname expects a host name while the Agent IP Address expects an IP address.<br>NOTE: The values of the Agent and Source host fields depend on the particular implementation of the device or application that sends an SNMP trap. If in doubt, use the Source host. |
| Source Hostname / IP Address | Allows you to create a Rule that will only match SNMP traps that occurred on a specific source host. The Source Hostname expects a host name while the Source IP Address expects an IP address.  |
| Varbind                      | Allows you to create a Rule that will only match SNMP traps that contain a varbind OID that contains the specific value.<br>If the trap does not contain the varbind at all, the Rule will not match.  |

### 4.3.3.1 Using Multiple Filters

You can create multiple filters for a single Rule by clicking "Filter by..." at the bottom of the Field column. This will cause a new filter row to be created and you can define your next filter just as outlined above.

If there are multiple filters, they will be ANDed together when matching against incoming traps.

If you need to setup filters that are ORed together, you will need to create two separate Rules, each with one of the ORed filters.

### 4.3.3.2 Deleting Filters

To delete a filter from a Rule, simply click the “X” that appears in the last column of the Filter table (to the right of the Comment column). The filter will be removed immediately, but you will need to click Apply to save the change.

### 4.3.3.3 Additional Notes about Filters

- 1) If you define a filter, changing the filter type (Field column) afterwards will cause the Operation and Value fields to be reset.
- 2) If you create a filter but don't select an Operation, the default Operation (the first in the list) will be used.

## 4.3.4 SNMP Stream Transformation

The Transformation defines how an SNMP trap that matches the Rule's filters gets converted into a Neuron Event. You can customize this behaviour by specifying values for one or more of the transformation fields on this tab.

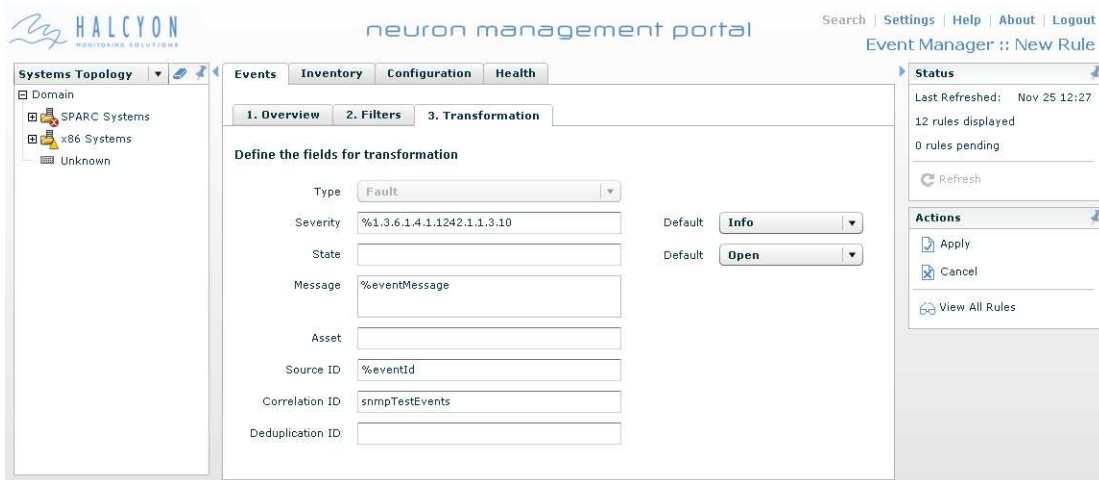


Figure 4-11: SNMP Stream Inbound Rule Transformation Tab

Table 4-11: SNMP Stream Inbound Rule Filter Types

| Field    | Description  |
|----------|--|
| Type     | Currently all SNMP traps are converted into fault events. This value cannot be changed.  |
| Severity | Specify the Severity of the generated event. Enter %<OID> or %<varName> and select the default severity for when the OID or varName could not be found. Refer to Parameter Substitution in section 4.3.4.1 for details on OID and varName. |
| State    | Specify the state of the generated event. Enter %<OID> or %<varName> and select the default state for when the OID or varName could not be found. Refer to Parameter Substitution in section 4.3.4.1 for details on OID and varName.       |

|                  |   |                                    |   |                                   |                 |   |                                    |                 |   |                                  |                |   |                                   |
|------------------|---|------------------------------------|---|-----------------------------------|-----------------|---|------------------------------------|-----------------|---|----------------------------------|----------------|---|-----------------------------------|
| Message          | <p>Specify the message of the generated event. You can enter a custom message that can contain %&lt;OID&gt; and %&lt;varName&gt; parameters.<br/>Refer to Parameter Substitution in section 4.3.4.1 for details on OID and varName.</p>   |                                    |   |                                   |                 |   |                                    |                 |   |                                  |                |   |                                   |
| Asset            | <p>Specify the asset of the generated event. You can enter a specific asset (static host name) or use one of the following values:</p> <table border="0"> <tr> <td>\$sourceHostName</td> <td>-</td> <td>Host name of the SNMP trap source</td> </tr> <tr> <td>\$sourceAddress</td> <td>-</td> <td>IP address of the SNMP trap source</td> </tr> <tr> <td>\$agentHostName</td> <td>-</td> <td>Host name of the SNMP trap agent</td> </tr> <tr> <td>\$agentAddress</td> <td>-</td> <td>IP address of the SNMP trap agent</td> </tr> </table> <p>The specified value will be replaced with the appropriate host name or IP address from the SNMP trap.<br/>If no value is specified, the default of \$sourceHostName will be assumed.</p> <p>NOTE: The values of the Agent and Source host fields depend on the particular implementation of the device or application that sends an SNMP trap. If in doubt, do not specify a value.</p> | \$sourceHostName                   | - | Host name of the SNMP trap source | \$sourceAddress | - | IP address of the SNMP trap source | \$agentHostName | - | Host name of the SNMP trap agent | \$agentAddress | - | IP address of the SNMP trap agent |
| \$sourceHostName | -   | Host name of the SNMP trap source  |   |                                   |                 |   |                                    |                 |   |                                  |                |   |                                   |
| \$sourceAddress  | -   | IP address of the SNMP trap source |   |                                   |                 |   |                                    |                 |   |                                  |                |   |                                   |
| \$agentHostName  | -   | Host name of the SNMP trap agent   |   |                                   |                 |   |                                    |                 |   |                                  |                |   |                                   |
| \$agentAddress   | -   | IP address of the SNMP trap agent  |   |                                   |                 |   |                                    |                 |   |                                  |                |   |                                   |
| Source ID        | <p>Specify the Source ID (Native Event ID) of the generated event. You can enter a custom static ID, %&lt;OID&gt; or %&lt;varName&gt;.<br/>Refer to Parameter Substitution in section 4.3.4.1 for details on OID and varName.</p>   |                                    |   |                                   |                 |   |                                    |                 |   |                                  |                |   |                                   |
| Correlation ID   | <p>Specify the Correlation ID of the generated event. You can enter a custom static ID, %&lt;OID&gt; or %&lt;varName&gt;.<br/>Refer to Parameter Substitution in section 4.3.4.1 for details on OID and varName.</p>  |                                    |   |                                   |                 |   |                                    |                 |   |                                  |                |   |                                   |
| Deduplication ID | <p>Specify the Deduplication ID of the generated event. You can enter a custom static ID, %&lt;OID&gt; or %&lt;varName&gt;.<br/>Refer to Parameter Substitution in section 4.3.4.1 for details on OID and varName.</p> <p>NOTE: If two or more SNMP traps are converted to events using the same Deduplication ID, only the first event will appear in the Event Viewer.</p>  |                                    |   |                                   |                 |   |                                    |                 |   |                                  |                |   |                                   |

### 4.3.4.1 Parameter Substitution

The Severity, State, Asset, Source ID, Correlation ID, and Deduplication ID fields may be set to %<OID> or %<varName>. Also, the Message field may contain one or more %<OID> and/or %<varName> parameters.

#### **OID**

When specifying %<OID>, replace "<OID>" with the actual varbind oid to use in the substitution. When the substitution then happens, the value of that varbind will replace %<OID>.

For instance, if the Severity was set to "%1.3.6.1.4.1.1242.1.1.3.10" and the value of that varbind in the incoming trap was MAJOR, then the severity of the event created from that trap would be MAJOR.

If the trap has no varbind that matches the specified <OID>, no substitution will occur.

**varName**

When specifying %<varName>, replace "<varName >" with the name of the varbind to use in the substitution. When the substitution happens, the value of that varbind will replace %<varName>.

For instance, if the Source ID was set to "%eventID" and the value of that varbind in the incoming trap was 125, then the Source ID (Native Event ID) of the event created from that trap would be 125.

The varbind name comes from the MIB file that describes the varbind. In order for varName substitution to work, the MIB for the SNMP trap and varbind in question must be loaded into *Neuron Management Suite*. The %<varName> parameter is then looked up in the Halcyon MIB database and replaced with the corresponding OID.

To load MIB files into Neuron Management Suite, just drop them into [LOCALDIR]/mibs. This directory is monitored and the processing of new or modified files occurs periodically and on startup. Please refer to the *Neuron Management Suite* Installation Guide for information on LOCALDIR.

**IMPORTANT:** The MIB files in [LOCALDIR]/mibs must be readable by user "halcyon". Make sure the MIB files are either owned by this user, or are world-readable.

## 4.4 Actions Panel

In addition to Creating and Editing Rules (see sections 4.2 and 4.3), the Actions Panel also makes available many other actions.

### 4.4.1 Import Rules

If you have been using Halcyon's PrimeAlert EventAction, you likely have several EventActions defined in your HALEventAction.dat file. *Neuron Event Manager* provides a way for you to import those EventActions into the *Neuron Event Manager* as Rules to avoid the need to define all new Rules.

- 1) You will first need a copy of your HALEventAction.dat file on the system you are using to access the *Neuron Event Manager* (the system your web browser is running on). This file is typically found in /var/opt/SUNWsymon/cfg on your Sun Management Center Server host.
- 2) Click the Import Rules button in the Event Manager Actions Panel.
- 3) In the file browser dialog that appears, select the HALEventAction.dat file and click Open. This will cause the EventActions in the file to be read and sent to the Neuron Server for importing as Event Manager Rules.
- 4) Once the EventActions have been uploaded and imported, a message will appear indicating the success of the operation. The EventActions will then appear as Rules in the table with their category set to EventAction.

Once EventActions have been imported as Event Manager Rules, they can be edited as regular Rules by following the instructions outlined in section 4.2.

All Rules created by importing EventActions will initially indicate they were last modified by "system". This will change when an actual user edits the Rule.

## 4.4.2 View Rule Details

To view all the details of a Rule, select it in the Rules table and click the View Rule Details button in the Actions Panel. The Rule Details Panel will open below the Rules table and show all the details about the selected Rule in a single view. The Rule Details Panel can be closed by clicking View Rule Details again, or by clicking the X at the top of the panel.

You cannot view more than one Rule at a time.

The screenshot displays the Neuron Event Manager interface. On the left is a 'Systems Topology' tree showing 'Domain', 'SPARC Systems', 'x86 Systems', and 'Unknown'. The main area is titled 'neuron management portal' and contains a 'Rules' table. The table has columns for Status, Name, Type, Category, Description, Run Policy, and Pending. The 'My Test Rule' is selected and highlighted. Below the table, the 'Rule Details for Rule 'My Test Rule'' panel is open, showing the following information:

| Type     | Category | Last Modified      | Last Modified By | Description                               |
|----------|----------|--------------------|------------------|---|
| Response | TEST     | Nov 25 11 09:07:59 | admin            | A test rule created during documentation. |

Below the table, the 'Filters' section contains the text: 'Actions execute when all the following are true: Event severity equals 'CRITICAL' or 'MAJOR' and Event state equals 'OPEN''. The 'Actions' section lists: 'Send event to email adapter in html format with subject "Event on %asset - %eventSeverity : %eventMessage" from "Neuron Management Server - neuron@localhost" for recipients neuronAlerts@localhost' and 'Send event to script adapter run script gatherLogs.sh with arguments %eventId'. The 'Schedules' section shows: 'Rule is active when: Hour >= 9 and Hour <= 17 or Day of month = 1'. On the right side, the 'Status' panel shows 'Last Refreshed: Nov 25 09:22', '12 rules displayed', and '0 rules pending'. The 'Actions' panel includes buttons for 'New Rule', 'Edit Rule', 'Import Rules', 'View Rule Details', 'Run Pending Actions', 'Clear Pending Actions', 'Test Actions', 'Copy Rules', 'Enable Rules', 'Disable Rules', 'Delete Rules', and 'View Events'. The 'Filter By Rule Type' panel shows a list of rule types: 'Inbound', 'SNMP', 'Ops Center', and 'Response'.

Figure 4-12: View Rule Details Panel

## 4.4.3 Run Pending Actions

A Rule may have Pending Actions if it has a Run Policy with an execution delay and/or repeat. The Pending Actions are waiting for the delay and/or repeat interval to elapse before executing.

Any Actions that are pending can be manually executed immediately by selecting the Rule in the Rules table and clicking the Run Pending Actions button in the Actions Panel. This will cause any Pending Actions to be executed immediately. If there is a Repeat Policy on the Rule, then that policy will remain in effect until the event that matched the Rule is acknowledged or closed or the Pending Actions are manually cancelled.

You must be in the "Managers" or "Admins" user group to Run Pending Actions. Refer to the *Neuron Management Server User's Guide* for more details about Users and Groups.

## 4.4.4 Clear Pending Actions

A Rule may have Pending Actions if it has a Run Policy with an execution delay and/or repeat. The Pending Actions are waiting for the delay and/or repeat interval to elapse before executing.

Any Actions that are pending can be manually cancelled by selecting the Rule in the Rules table and clicking the Clear Pending Actions button in the Actions Panel. This will cause those Pending Actions to be cancelled. If there was a Repeat Policy, all future repetitions will be cancelled regardless of the state of the event that triggered the Rule.

**NOTE:** It is possible for more than one event to match a single Rule, thus it's possible a single Rule could have actions pending against multiple events. Running or Clearing Pending Actions can only be done for all Actions Pending on a Rule, not for Actions Pending against specific events.

You must be in the "Managers" or "Admins" user group to Clear Pending Actions. Refer to the *Neuron Management Server User's Guide* for more details about Users and Groups.

## 4.4.5 Test Actions

After settings up one or more Actions for a Rule, you may wish to run a test to ensure the Actions execute properly and produce the result you are looking for. *Neuron Event Manager* allows you to do this via the Test Actions button in the Actions Panel.

Select the Rules you want to test, click Test Actions, then confirm you want to test the actions for the selected Rules. The Actions will then be executed with an internally created test event. Once the actions have been executed, a message will appear indicating the number of actions that were successfully executed. You can then check to ensure the results were observed properly (for instance, everyone got the email, or Tivoli received the event).

The details of the test event will be as follows:

**Table 4-12: Test Action Event Details**

| Field       | Value  |
|-------------|--|
| Event ID    | 0  |
| Severity    | INFO   |
| State       | OPEN   |
| Message     | Neuron Event Management Test Event for Rule <RuleName> |
| Source      | internal   |
| Source Host | localhost (Neuron Management Suite's Server Host)      |

**NOTE:** When running Test Action, it is the Actions that are being tested, not the Rule itself, thus any Rule Filters will have no impact on the test.

**NOTE:** The test event is an internal event that is not logged or stored anywhere. It will not be viewable in the Event Viewer.

You must be in the “Managers” or “Admins” user group to Test Actions. Refer to the *Neuron Management Server User's Guide* for more details about Users and Groups.

## 4.4.6 Copy Rules

To copy Rules, select them from the Rules table (ctrl-click to select additional Rules) and then click the Copy Rules button in the Actions Panel. This will cause duplicates of the selected Rules to be created where “Copy” is appended to the name of each copied Rule.

If you want to make multiple copies of a Rule, after the first copy you will need to change the name of either the original Rule or the copied Rule. Alternatively, you can make a copy of the copied Rule. This is because all Rule names must be unique, and the copy action only appends “Copy” to the name of the Rule being copied.

You must be in the “Managers” or “Admins” user group to Copy Rules. Refer to the *Neuron Management Server User's Guide* for more details about Users and Groups.

## 4.4.7 Enable/Disable Rules

It may be desirable at times to manually enable or disable one or more Rules. To do this, select one or more Rules in the Rules table (ctrl-click to select additional Rules) and then click either the Enable Rules or the Disable Rules button in the Actions Panel.

When disabling Rules, the confirmation window will contain an option to Clear Pending Actions. If this box is checked, any Actions that are pending for the selected Rules will be cleared.

If a Rule is disabled, it will not be matched against any events and thus it's Actions will not be executed even if an event occurs that would have matched the Rule.

You must be in the “Managers” or “Admins” user group to Enable or Disable Actions. Refer to the *Neuron Management Server User's Guide* for more details about Users and Groups.

## 4.4.8 Delete Rules

To delete Rules, select them from the Rules table (ctrl-click to select additional Rules) and then click the Delete Rules button in the Actions Panel. Confirming the delete will remove the Rules from the table and they will have no further impact on any incoming events.

**IMPORTANT:** If a Rule has pending actions associated with it, they will need to be cancelled before the Rule can be deleted. Please refer to section 4.4.4 for clearing the Pending Actions.

You must be in the “Managers” or “Admins” user group to Delete Rules. Refer to the *Neuron Management Server User's Guide* for more details about Users and Groups.

### 4.4.8.1 Process Rules Utility

When Rules are deleted in *Neuron Event Manager*, they are removed from the Rules table and are no longer active, but they remain stored in the database. It is possible to list out these Rules that

have been “deleted”, purge them from the database completely or undelete them using the ProcessRule utility ([BASEDIR]/bin/ProcessRule, see the *Neuron Management Suite* Installation Guide for details on BASEDIR).

Run “[BASEDIR]/bin/ProcessRule –help” for more details and how to act on these “deleted” Rules.

### 4.4.9 View Events

Clicking “View Events” will change the Events Tab to View Mode which will load the Event Viewer in place of the Event Manager. Please refer to section 3 for details about Viewing Events.

NOTE: If you are in View Mode, you can return to the Event Manager by clicking “Manage Events” in the Event Viewer Actions Panel.

## 4.5 Filters Panel

The Filters here have nothing to do with Rule Filters. You can click on any entries here to limit the types of Rules that appear in the table. For instance, click Response to view only Response Rules, or SNMP to view only SNMP Stream Inbound Rules.