



# CHAPTER 6

## Alerts

---

The Cisco PVM Alert Viewer displays a list of alerts occurring over time or based on specific filtering criteria. You can filter the list of alerts based on time period, source, type, severity, or cause, as well as view individual alert details.

This chapter contains the following sections:

- [Alert Types, page 6-1](#)
- [Alert Severity Color Codes, page 6-3](#)
- [Displaying Alerts, page 6-3](#)
- [Displaying Alert Details, page 6-7](#)
- [Suspending and Resuming Alerts, page 6-9](#)



**Note**

---

The functions discussed in this chapter apply to Cisco PVM Administrators only.

---

## Alert Types

Alerts consist of three general types:

- **NAM alarms**—violations of criteria set in an external interface and sent through SNMP.
- **Threshold violations**—violations of criteria set in Cisco PVM.
- **System events**—notifications of licensing errors, timeouts, and system health information.

For every data aggregation period, the system performs the following functions for each statistic:

1. Aggregates all the data collected for a specific metric (measurement) during the specified aggregation period
2. Compares the results with the Dynamic Threshold value calculated based on the deviation from the baseline that corresponds to the severity level assigned to the specific Threshold
3. Raises an alert if the result is greater than the percentage deviation assigned to the Threshold.

System-generated alerts include system health events. Cisco PVM monitors the following metrics:

- CPU utilization of each CPU on the system
- RAM utilization
- Disk utilization for each of the locally and remotely mounted file systems and
- Tablespace utilization for all tablespaces in the Cisco PVM database.

This section contains the following topics:

- [NAM Alarms, page 6-2](#)
- [Threshold Violations, page 6-2](#)
- [System Events, page 6-2](#)

## NAM Alarms

NAM-generated alerts result from a violation of criteria configured for the device in either the NAM Traffic Analyzer or a third-party SNMP application. The violations are read from the RMON MIB, and include violations for:

- Rising Threshold Crossed
- Falling Threshold Crossed.

All NAM alerts are listed as minor in the Cisco PVM alert viewer.

## Threshold Violations

Threshold-generated alerts result from violations of user-defined criteria set in Cisco PVM. These alerts appear when a Threshold is violated for an assigned traffic metric with data aggregated for any data source in a specified Data Source Group. Administrators assign specific metrics, Data Source Groups, and alert severity levels using **Setup > Thresholds**.

Administrators can define two types of Thresholds in Cisco PVM:

- **Dynamic Thresholds**—the Cisco PVM server performs automatic baselining for each statistic-specific attribute and metric combination based on previous data collection. User-defined percentage deviations from the baseline are translated into alerts, increasing in severity with the degree of deviation.
- **Fixed Thresholds**—the system generates an alert once a user-defined minimum value for a specific metric has been exceeded.

**Note**

---

For a discussion of Threshold calculations, see [Threshold Setup, page 2-31](#).

---

## System Events

Cisco PVM monitors system health and utilization metrics for CPUs, RAM, disks, and database tables. System events that generate alerts include:

- Success or failure of resource inventory import status.
- NAM connectivity failure or reconnect.
- NAM SNMP timeout.
- NAM Application Response Time (ART) configuration change.
- NAM general configuration change.
- Switch/Router connectivity failure or reconnect.
- Switch/Router general configuration change.

- Switch/Router SNMP timeout.

## Alert Severity Color Codes

Cisco PVM displays a color-coded icon next to each alert in the list indicating severity. [Table 6-1](#) shows the color assigned to each severity level:

**Table 6-1** Alert Severity Color Codes

Severity	Color
Critical	Red
Major	Orange
Minor	Yellow
Warning	Cyan
Cleared	Green
Indeterminate	Blue
Information	Gray



**Note**

A **Cleared** alert has either had its Threshold adjusted, or the current traffic level no longer violates the Threshold level of the previous alert. A given alert might go through all the severity levels unless it is cleared quickly or the severity level set in Thresholds is adjusted.

## Displaying Alerts

Cisco PVM displays a paginated, continuous list of performance alerts in descending order by date, and allows you to filter alerts by time period and other criteria. The display time period defaults to the last hour.



**Note**

The maximum number of alerts that the GUI will display is 1,000. An alert will remain in the GUI list until it falls to greater than the last 1,000 alerts logged in the system.

**Step 1**

On the Cisco PVM dashboard, click **Alerts**.

The Alerts window appears, showing the alerts for the hour (see [Figure 6-1](#)).



**Tip**

You can sort the list in ascending or descending order by clicking any of the column headers.

Figure 6-1 Alerts Window

Cisco Performance Visibility Manager Your EVAL license will expire in 71 days. Server Time: 02/07/2006 8:53:05 AM EST

Generate Reports | Setup | Monitor | Reports | ART | **Alerts** | Admin

Alerts

From Date: 02/07/2006 07:53 AM To Date: 02/07/2006 08:53 AM Description:  Clear  
 Log Type:  Severity:  Cause:  Filter

79 items found, displaying 1 to 12. [First/Prev] 1 2 3 4 5 6 7 [Next/Last]

Severity	Date	Description	Log Type	Statistic	Log Source Type
Critical	02/07/2006 08:52:41	App Threshold	Generic	Application Statistics	Cisco PVM
Warning	02/07/2006 08:52:41	App Threshold	Generic	Application Statistics	Cisco PVM
Minor	02/07/2006 08:52:18	Giga4_47_packets	Rising Threshold Crossed		Switch
Minor	02/07/2006 08:52:16	External_bytes	Rising Threshold Crossed		NAM
Minor	02/07/2006 08:51:46	External_bytes	Falling Threshold Crossed		NAM
Minor	02/07/2006 08:51:39	Giga4_47_packets	Falling Threshold Crossed		Switch
Minor	02/07/2006 08:50:45	sep octets	Rising Threshold Crossed		NAM
Minor	02/07/2006 08:50:16	External_bytes	Rising Threshold Crossed		NAM
Minor	02/07/2006 08:50:08	Giga4_47_packets	Rising Threshold Crossed		Switch
Minor	02/07/2006 08:49:42	Giga4_47_packets	Falling Threshold Crossed		Switch
Minor	02/07/2006 08:48:11	Giga4_47_packets	Rising Threshold Crossed		Switch
Minor	02/07/2006 08:47:45	Giga4_47_packets	Falling Threshold Crossed		Switch

Table 6-2 describes the fields available in the Alerts Window.

**Table 6-2 Alerts Window Field Descriptions**

<b>Field</b>	<b>Type</b>	<b>Description</b>
From Date	Field	Displays the starting date and time of the alerts in the list, and accepts the date selection from the pop-up calendar.
Calendar	Icon	Displays a pop-up calendar for selection of date and time.
To Date	Field	Displays the ending date and time of the alerts in the list, and accepts the date selection from the pop-up calendar.
Log Type	Drop-down list	Allows selection of the type of violation for filtering the list: <ul style="list-style-type: none"> <li>• Generic</li> <li>• Unknown</li> <li>• Rising Threshold Crossed</li> <li>• Falling Threshold Crossed</li> <li>• Cisco PVM System Health</li> <li>• ARCHIVE</li> <li>• PURGE</li> </ul>
Description	Text box	Allows entry of characters (including the wildcard) for filtering the list of events.
Severity	Drop-down list	Allows selection of the severity type for filtering the list: <ul style="list-style-type: none"> <li>• Indeterminate</li> <li>• Critical</li> <li>• Major</li> <li>• Minor</li> <li>• Warning</li> <li>• Cleared</li> <li>• Information</li> </ul>
Cause	Drop-down list	Allows selection of the cause of the violation for filtering the list: <ul style="list-style-type: none"> <li>• Generic</li> <li>• Unknown</li> </ul>
Clear	Button	Clears all of the fields in the filter area for performing a new filter operation.
Filter	Button	Filters the list of alerts based on one or more criteria entered in the filter area.
Severity	Column header	Lists the severity level next to a color code and links to the Alert Detail window for the individual alert.
Date	Column header	Displays the date and time the violation was generated.

Table 6-2 Alerts Window Field Descriptions (continued)

Field	Type	Description
Log Type	Column header	Displays the type of violation that created the alert: <ul style="list-style-type: none"> <li>• Generic</li> <li>• Unknown</li> <li>• Rising Threshold Crossed</li> <li>• Falling Threshold Crossed</li> <li>• Cisco PVM System Health</li> <li>• ARCHIVE</li> <li>• PURGE</li> <li>• ART</li> </ul>
Description	Column header	Displays the device, metric, Threshold, or system check that generated the alert.
Statistic	Column header	Displays the type of traffic (statistic) upon which the violation is based.
Log Source Type	Column header	Displays the originating source of the type of alert log created for the violation: <ul style="list-style-type: none"> <li>• Switch</li> <li>• NAM</li> <li>• Cisco PVM</li> <li>• Generic or</li> <li>• Unknown</li> </ul>

## Filtering Alerts

The Alerts list can be filtered based on time interval, log type, alert severity, description, or cause. You can filter the list using any or all of the fields at the top of the Alerts window.

- 
- Step 1** Click **Alerts** in the Cisco PVM dashboard.
- The Alerts window displays a paginated list of all of the alerts generated in the hour, in descending order by date and time.
- Step 2** Select the start date by clicking the calendar icon next to the **From** field.
- Step 3** Select the end date by clicking the calendar icon next to the **To** field.
- Step 4** Select the log type from the **Log Type** drop-down list.
- Step 5** Enter descriptive characters in the **Description** box, using the percent symbol (%) as a wildcard to broaden your search.
- Step 6** Select the severity level from the **Severity** drop-down list.
- Step 7** Select the alert cause from the **Cause** drop-down list.

**Step 8** Click **Filter**.

The window displays the Alerts list containing only the alerts that match the filter criteria.

**Tip**

If you want to begin filtering with a new set of criteria, click **Clear** to reset all of the fields in the filter area to blank. To display the original, unfiltered list of Alerts, click **Alerts** under Generate Reports on the left side of the window.

## Displaying Alert Details

- Step 1** Click the link in the Severity column of the alert you wish to view. The Alert Detail window (Figure 6-2) displays the individual alert's description along with the traffic type (statistic), database information, and additional information indicating what constraint has been violated.

**Figure 6-2** Alert Detail

Alert Detail	
<b>Log Id:</b>	7536
<b>Log Type:</b>	Generic
<b>Date:</b>	2006-02-07 08:52:41.0
<b>Severity:</b>	Critical
<b>Statistic:</b>	Application Statistics
<b>Cause:</b>	Generic
<b>Managed Object Id:</b>	3
<b>Managed Object Name:</b>	All NAM
<b>Description:</b>	App Threshold
<b>Log Content:</b>	ThresholdValue==1.95575e+06 Bytes/Second MeasuredValue==2.19202e+06 Bytes/Second DataSource==ALL_SPAN Device==NAM 161 Metric==Bytes / Second TrafficType==Application Statistics Period=Last 5 minutes DataSourceGroupName==All NAM Application==All Applications
<input type="button" value="Back"/>	

149737

Table 6-3 describes the fields in the Alert Details window.

**Table 6-3** Alert Details Field Descriptions

Field	Description
Log Id	The sequential number of the alert as it appears in the database.
Log Type	The type of alert generated: <ul style="list-style-type: none"> <li>• Generic</li> <li>• Unknown</li> <li>• Rising Threshold Crossed</li> <li>• Falling Threshold Crossed</li> <li>• System Health</li> <li>• Purge</li> <li>• Archive</li> </ul>
Date	The date and time the alert was generated.
Severity	The severity level of the alert: <ul style="list-style-type: none"> <li>• Indeterminate</li> <li>• Critical</li> <li>• Major</li> <li>• Minor</li> <li>• Warning</li> <li>• Cleared</li> <li>• Information</li> </ul>
Statistic	The type of traffic (statistic) upon which the violation is based.
Cause	Either Generic (known to the system) or Unknown.
Managed Object Id	The classification of the managed object as it appears in the database.
Managed Object Name	The name of the managed object as it appears in the database.
Description	The device, metric, Threshold, or system check that generated the alert.
Log Content	Detailed information about the actual alert as contained in the database, such as: <ul style="list-style-type: none"> <li>• the baseline value at the time of the alert.</li> <li>• the value that was actually violated (based on severity level, baseline, and standard deviation calculations).</li> <li>• the Data Source Group assigned to a Threshold (for Threshold violations only).</li> <li>• the Data Source that generated the traffic.</li> <li>• the traffic metric monitored, such as bytes, packets, or errors.</li> <li>• device-specific identifier.</li> </ul>
Back [button]	Closes the Alert Details and returns to the Alerts window.

- Step 2** Close the details by clicking **Back**.  
The system returns to the Alerts window.
- 

## Suspending and Resuming Alerts

Administrators can suspend alerts for individual thresholds defined in Setup. Under the Setup GUI, thresholds can be disabled if you no longer need or want to view traffic-related violations in the Alert Viewer. The threshold definitions remain in the system, and they can be re-enabled if desired. Disabled thresholds do not generate alerts.

With access to a NAM's external interface (NAM Traffic Analyzer), you can make configuration adjustments that also affect whether alerts appear in the Cisco PVM alerts viewer. Such alerts are sent through SNMP to the Alert Viewer directly from the NAM, and are not managed in Cisco PVM.

**Note**

For a complete discussion of thresholds and how they relate to alerts, see [Threshold Setup, page 2-31](#). See the NAM Traffic Analyzer documentation for information on adjusting NAM alarm settings and trap destinations.

---

Follow these steps to disable or enable thresholds:

---

- Step 1** Click **Setup** in the Cisco PVM dashboard.
- Step 2** Click **Thresholds** in the Setup navigation menu.
- Step 3** Check the box(es) next to the threshold(s) you want to enable or disable.
- Step 4** Click:
- **Disable** to suspend the alerts related to the specific threshold(s) or,
  - **Enable** to resume alerts.

The Thresholds window refreshes to reflect the new status of the selected thresholds in the Status column.

---

