Creating and Managing Thresholds

You can create thresholds for any key performance indicators (KPIs) displayed in Prime Performance Manager reports, views, or dashboards. Thresholds help you monitor network performance by sending notifications when a KPI exceeds or falls below a desired tolerance or performance target. In addition, you can have Prime Performance Manager define a baseline performance range for a KPI and notify you when performance changes significantly from the baseline range. Creating baselines alerts you to network problems before they cross the prescribed thresholds.

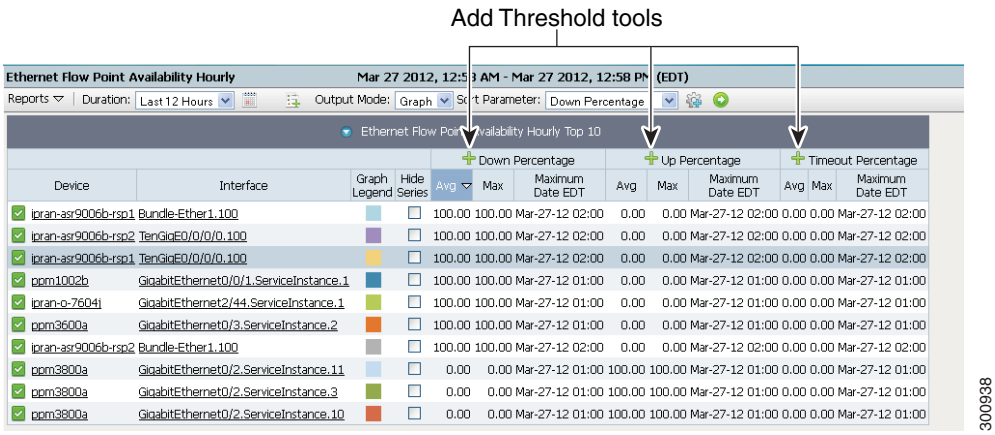
Prime Performance Manager gives you considerable flexibility in defining threshold ranges and the threshold crossing alerts that are issued when threshold ranges are exceeded. The following topics provide information about configuring thresholds in Prime Performance Manager:

- Creating Thresholds, page 11-1
- Creating Compound Thresholds, page 11-8
- Creating Baseline Thresholds, page 11-10
- Managing Thresholds, page 11-12

Creating Thresholds

Prime Performance Manager allows you to create thresholds to generate alarms when a given report key performance indicator rises or falls to a specified point. Threshold-eligible report KPIs are identified by Add Threshold tools in the report KPI column header. Figure 11-1 shows an example.

Figure 11-1 Add Threshold Tools



You can create thresholds on device objects, such as CPUs and memory pools. For example, if you navigate to the Resources CPU, click a slot or CPU. Thresholds can be created on the CPU utilization.

In addition, you can create and apply report policies that modify report intervals when thresholds are crossed. For example, if a CPU nears 100% utilization, you can create and apply a report policy that reduces the polling frequency until it returns to normal. Conversely, you can create and apply report policies that increase polling frequencies when KPIs pass critical thresholds. For information about creating report policies, see Creating Report Policies, page 7-33.

Note By default, only numeric KPIs are enabled for thresholds. However, Prime Performance Manager does provide the capability to create thresholds for string KPIs. For information, see Entering Thresholds for String KPIs, page 11-8.

To create a threshold, you provide the KPI onset and abate points. Onset is the rising or falling KPI value that, when reached, generates an alarm. Abate is the rising or falling KPI value that, when reached, clears the alarm. Additionally, you can specify the type of alarm you want raised, the days and times you want the threshold to run, and the number of required threshold-crossing occurrences before the alarm is raised or cleared.

As you prepare to create thresholds in Prime Performance Manager, keep the following in mind:

- Prime Performance Manager includes predefined thresholds that you can use as is or duplicate and modify to meet your needs. For a list of predefined thresholds, see Appendix C, “Predefined Thresholds.”
- Prime Performance Manager validates your threshold entries based on the KPI type, either rising or falling. For a rising threshold, for example interface availability down percentage, the higher alarm threshold value must be greater than the lower alarm. For a falling threshold, for example, interface availability up percentage, the higher alarm threshold must be lower than the one entered for the lower alarm.
- To avoid flooding the system with alarms, test thresholds on a small group of devices before you roll them out to the full network.
- To avoid alarm flapping, set the abate value at a reasonable distance from the onset value. The distance depends on the expected KPI fluctuation. KPIs with larger fluctuations should have a wider onset-to-abate gap than KPIs with smaller fluctuations.

- Prime Performance Manager displays Add Threshold tools for any threshold-capable KPI, and excludes report, view, or dashboard data that cannot have thresholds created, such as name and description.
- The TCA is generated if the beginning of the data period falls within the active TCA range. For example, if data crosses a threshold between 1:15-1:30 and the TCA active period is defined as 1:00-5:00, the TCA is generated. If the TCA active period is 12:00-1:00, the TCA is not generated.

To create a Prime Performance Manager threshold:

Step 1 Log into Prime Performance Manager GUI as a System Administrator user.

Step 2 Display the report, view, or dashboard containing the KPI for which you want to create a threshold.

Step 3 Click the Add Threshold tool (green + icon) in the KPI column header.

Step 4 In the Add Threshold window, enter the threshold parameters. Threshold parameters are grouped into Threshold Configuration and Threshold Values tabs described in the following sections:

- Threshold Configuration, page 11-3
- Threshold Values, page 11-6

Threshold Configuration

- Name—Enter a unique name for the threshold. The name cannot be the same as any existing threshold name. The field accepts any alphanumeric text. Spaces are not permitted.
- Enabled—The threshold is enabled by default. If you want to create the threshold but do not want it enabled, uncheck this box. You can enable the threshold later on the Threshold Editor window. For example, you might want to create all thresholds first, review them in the Thresholds Editor window, then enable them at one time. For information, see **Managing Thresholds, page 11-12.**
- Report Data Interval—Choose the time interval when you want Prime Performance Manager to check the data point value identified by the threshold. Threshold intervals include:
  - 1 Minute
  - 5 Minute
  - 15 Minute (default)
  - Hourly
  - Daily
  - Weekly
  - Monthly

Note Verify that the report has these intervals enabled. Prime Performance Manager enables the 15-minute, hourly, daily, weekly, and monthly intervals by default. To run a threshold every 5 minutes, you must enable 5-minute report interval. For information, see Chapter 7, "Managing Reports, Dashboards, and Views."

If you implemented multi-tenancy in Prime Performance Manager, complete the following tenancy fields. If not, continue with the Description field.

- Tenancy—Indicates the tenants that should be included in the threshold:
  - ALL—(default) Choose this option if you do not want to assign tenants to the threshold.
  - ALL_TENANTS—Includes all tenants in the threshold.

  - SELECTED—Allows you to choose the tenants added to the threshold
- Selected Tenants—If you chose SELECTED in the Tenancy field, displays the tenants that added.

  To add tenants, click **Change** then chose the tenants you want in the Select Tenants dialog box using the **Add**, **Add All**, **Remove**, **Remove All** buttons.
- Description—As needed, add any notes to describe the threshold. The field accepts any alphanumeric text.
- Alarm Type—Indicates the alarm type you want raised. Select the Alarm type with these options: Communications, Processing Error, Environmental, QoS, or Equipment
- Probable Cause—Threshold Crossed is the default probably cause. If you want to assign a different one, choose it from the displayed list.
- Alarm Nature—Choose the method for clearing the alarm, either ADAC (automatically detected and automatically cleared), or ADMC (automatically detected and manually cleared). ADAC is the default.

  Note If you set Alarm Nature to ADMC, abate values are not allowed. If you change a threshold from ACAC to ADMC, existing abate values are cleared.

- Continuous Alarm—If enabled, alarms are sent every polling cycle until the threshold falls below the abate value. If not enabled, the alarm is only sent once.
- Run Script—If you want to execute a script when the threshold is crossed, enter the script path here. The script can reside anywhere on your file system as long as you specify the full path, and the root user has the appropriate file and directory permissions to execute it. If you enter an OSS host automation script, you can specify whether the threshold script has priority. See Editing Upstream OSS Hosts, page 10-15 and Tuning Event and Alarm Parameters, page 10-18 for more information. In addition, you can use the ppm extrarunpathcommand to define the script directory in the PATH variable. For information, see ppm extrarunpath, page B-39.

  You can also pass variables to scripts as $params, for example:

  - $abateValue—The threshold abate value.
  - $AckBy—The user who acknowledged the alarm.
  - $Action—The action performed on the alarm or event, for example: NEW("New", "0, New")/ UPDATE("Update", "1, Update")/ DELETE("Delete", "2, Delete").
  - $AlarmNature—The alarm nature, ADAC or ADMC.
  - $AlarmType—The alarm or event type.
  - $AlarmID—The alarm ID (alarm ID is the event ID).
  - $Category—The alarm or event category.
  - $ClearBy—The user who cleared the alarm or event.
  - $currentValue—The current sample value.
  - $DeviceType—The device type
  - $Element—The unique network element to which the alarm or event pertains.
  - $ID—A unique ID assigned to all alarm or event objects.
  - $Name—The alarm or event name.
  - $onsetValue—The threshold onset value.

  - $OriginalSeverity—The original alarm or event severity.
  - $Owner—The alarm or event owner.
  - $ProbableCause—The alarm or event probable cause.
  - $relation—The TCA value
  - $Severity—The alarm or event severity.
  - $Tenant—The tenant name.
  - $TenantDisplayName—The tenant display name.
  - $TcaName—The TCA name.
  - $TcaMetric—The TCA metric.
  - $thresDetail—Threshold details.
  - $TimePeriod—The alarm or event time period.
  - $TimePeriod24Hrs—The customized time period in the format yyyy-mm-dd with 24 hrs clock.

  In addition, context-dependent variables are available that allow you to add any non-key column from any KPI in the form ${kpi<index>.<column header name>}. For simple thresholds these are all kpi0. More complicated thresholds could have any number of KPIs.

- Email From Address—If you want to send an email when the threshold is crossed, enter from email address here.

  Note If a global email from address is configured, that address automatically populates the Email From Address field. You can remove or edit the global address, however. The global email from address is configured in Administration > System Settings > System Configuration.

- Email To Addresses—If you want emails sent when the threshold is crossed, enter the recipient address(es). Separate multiple addresses with semicolons and no spaces.
- Email Subject—Allows you to customize the email subject to make the email more readable and helpful. You can use any parameter in the email subject that can be sent to scripts (see Run Script above), except AlarmID. AlarmID is not supported in messages.
- Message Text—Allows you to customize the message displayed when the TCA occurs. For example,

  TCA: $Severity: $TcaName: $TcaMetric: $relation

  Displays a message like the following when the alarm is raised:

  TCA: Critical: CPU_AverageUtilization_duplicate: CPU 5 Min Utilization 5 Minute/Average Utilization: value ‘23’ threshold ‘20’

  Click **Insert Variable** to insert variables in the message text. These are the same variables that can be sent to scripts except AlarmID (see Run Script above).

- Occurrence—In the Occurrence area, enter the days for which you want the threshold applied. For example, you might only want to check some thresholds once a week, in which case, you would pick the day of the week when you want the threshold to apply.

  After selecting the days, enter the beginning and ending time in the Begin Time and End Time fields (hours and minutes) for which you want the threshold applied. If you enter the same value, the threshold is always applied.

Threshold Values

The Threshold Values tab is where you provision the threshold parameters for minor, major, and critical alarms. Warning and informational thresholds are not enabled by default. To enable them, choose **Administration > System Settings**. In System Configuration Settings, enable **TCA Warning Severity** and/or **TCA Informational Severity**.

- Onset Occurrences—The number of onset threshold crossings that must occur before the alarm is raised.

  The alarm is triggered when the incoming data exceeds the configured Onset value repeatedly.

  For example, if the onset value is 90 and if the onset occurrence is 3, then the following alarm conditions might occur:

  - Critical Alarm is triggered when the incoming data is 90, 95, 92.
  - Critical alarm is trigged at 90 when the incoming data is 90,85,92, 95, and 90.
  - Critical alarm is not trigged when the incoming data is 90, 85, 92, and 95.
- Abate Occurrences—The number of abate occurrences that must occur before the alarm is cleared.
- Report Policy Override—If you created a report policy for the specific alarm threshold, select the report policy here. Only user-created report policies are displayed. You can apply report policies to take effect when thresholds are crossed. For example, if a resource crosses a maximum usage value, you might decrease the report interval to reduce usage on the resource. Conversely, you might increase report intervals for other types of TCAs to get more timely data.

  If you create report policies for each threshold level, the minor report policy is applied when the threshold crosses the minor level, the major report policy is applied when the threshold cross the major threshold, and the critical report policy is applied when it crosses the critical threshold level. If a threshold level does not have an associated report policy, the default report policy is applied.

Note If you define a report policy for one severity level, you must define a report policy for all severity levels.

Individual TCA definitions and their associated report policy overrides are based on the KPI interval. If you apply a report policy to the threshold that excludes the TCA interval, the threshold will never clear. For example, suppose you create a default interface usage report policy that includes the 5-minute, 15-minute, hourly, and daily intervals. You then create a custom interface usage report policy X that includes the 15-minute, hourly, and daily report intervals, but not the 5-minute interval. Suppose you create an interface usage TCA for the 5-minute interval and assign report policy X to the Critical level report policy Override. When this threshold is exceeded, report policy X is applied but the TCA will never clear because the underlying KPI is not generated by the report policy (X).

The intent is to reduce the polling load on the device. This can be accomplished by reducing the number of reports polled at each interval or eliminating reports for a particular interval. If you add an override report policy, be sure not to remove the report or interval on which the TCA is based.

Note Report Policy Override does not apply to devices that have collectd provisioned because Prime Performance Manager polls the device on a prescribed minimum interval that supersedes report policy intervals.

KPI Values

- KPI—Select the KPI from the drop down list. Normally only one KPI is shown. Multiple KPIs are shown when you create compound thresholds. For more information, see Creating Compound Thresholds, page 11-8.
- Baseline—If you want the threshold to be based on a calculated value based on a collection of KPI values over a period of time and not an individual KPI value, check this box. To create a baseline threshold, you must specify the baseline method, window size, and onset and abate factors. For more information, see Creating Baseline Thresholds, page 11-10.
- Baseline Method—If you enabled baseline thresholds, choose the baseline method:
  - Average—The average of KPI values collected within the specified threshold window.
  - Exponential Average—Applies a calculation to the KPI values gathered in the specified window that places greater weight on recent values over older ones.
- Window Size (in intervals)—The number of intervals to include in the baseline. Intervals are defined by the Report Data Intervals field.
- Name—A read-only field displaying the name generated automatically from the report, view, or dashboard attribute name.
- Report—A read-only field displaying the report name.
- Type—Choose the KPI type, either rising or falling. For a rising threshold, the critical alarm threshold must be higher than the major alarm threshold, and the major alarm threshold must be higher than the minor alarm. For falling KPI thresholds, the critical alarm entry must be lower than the major alarm, and the major alarm must be lower than the minor alarm.
- Scope—Set the threshold scope. Scope indicates the devices for which you want the threshold reported. The default value means report the threshold for any reportable device. You can set the scope for a subset of devices, for example, you can choose Cisco7606s to report the threshold only for Cisco 7606 routers, and so on. The device groups that appear come from the Polling Groups tab. Device groups are based on the device types that are found during device discovery.

Note If you create a threshold on a device element, for example, a CPU, the element will be displayed in the Scope, for example, "...CPUNum=123".

- Onset—Enter the onset threshold value(s) in the alarm box(es) that you want raised. You can set values for any or all alarm types. However, alarm entries must match the KPI type. For a rising KPI, the critical alarm threshold entry must be higher than the major alarm, and the major alarm threshold must be higher than the minor alarm. For a falling KPI type, the critical alarm threshold must be lower than the major alarm, and the major alarm must be lower than the minor alarm.
- Abate—Enter the threshold value in the box of the alarm(s) when you want the alarm cleared. For a rising KPI type, the abate value must always be lower than the onset value. For a falling KPI type, the abate value must be higher than the onset.

Note A small number of KPIs allow you to define thresholds using strings. For details, see Entering Thresholds for String KPIs, page 11-8.

If you do not define threshold values for all alarm levels, Prime Performance Manager skips them and goes to the next defined threshold level. For example, if you only define critical alarms, the threshold will go to normal after the critical alarm reaches the abate level.

Note If you selected Baseline, Onset and Abate change to Onset Factor and Abate Factor to indicate the number you enter is a factor multiplied by the baseline calculation to determine whether an alarm should be raised or cleared. For more information, see Creating Baseline Thresholds, page 11-10.

Step 5 Click **OK**.

The TCA is added to the gateway. To edit or perform other threshold actions, see Managing Thresholds, page 11-12. To create compound or baseline thresholds, see:

- Creating Compound Thresholds, page 11-8
- Creating Baseline Thresholds, page 11-10

Entering Thresholds for String KPIs

By default only numeric KPIs are enabled for thresholds. However, a small number of string KPIs are enabled so that you can enter thresholds for them, for example, operationalState Up, Degraded, or Down. If you choose an enabled string KPI, boxes appear below the Onset and Abate fields allowing you to define the point when TCAs are raised. To define thresholds for string KPIs:

- You can use any of the following operators: Equals, Does Not Equal, Contains, Does Not Contain, Begins With, Ends With.
- Test values can contain any printable characters except quotes.
- All matches are case-sensitive.
- For multiple test values:
  - If the operator is positive (Equals, Contains, Begins With, Ends With), the condition is true when the value matches any test value.
  - If the operator is negative (Does Not Equal, Does Not Contain), the condition is true when the value does not match any test value.
- You generally should not specify abates for string thresholds. If no abate is specified, the abate condition is true as soon as the onset condition is false.
- String thresholds always test severities from Critical to Normal (which always matches), and take the first value that matches.

Note You can enable additional string KPIs by setting thresholdable=true in the report XML. For information, see the *Cisco Prime Performance Manager 1.7 Integration Developer Guide*.)

Creating Compound Thresholds

You can create thresholds for multiple KPIs and have alarms generated when the specified conditions exist for one or all of the KPIs. For example, you can define thresholds for CPU routing processors and specify the alarm to be raised when one or more processors exceed or fall below a specified value.

Compound thresholds can only be created for a single device object residing within the same device. For example, if you create a threshold for a CPU utilization KPI, you must do it for a single CPU. If you base it on multiple CPUs, the last CPU value polled will be the one used for the TCA calculation.

Compound threshold requirements are enforced by the Prime Performance Manager GUI. You can create compound thresholds based on objects across multiple devices by creating XML files and using Prime Performance Manager macros. For information, see the *Cisco Prime Performance Manager 1.7 Integration Developer Guide*.

To create a compound threshold:

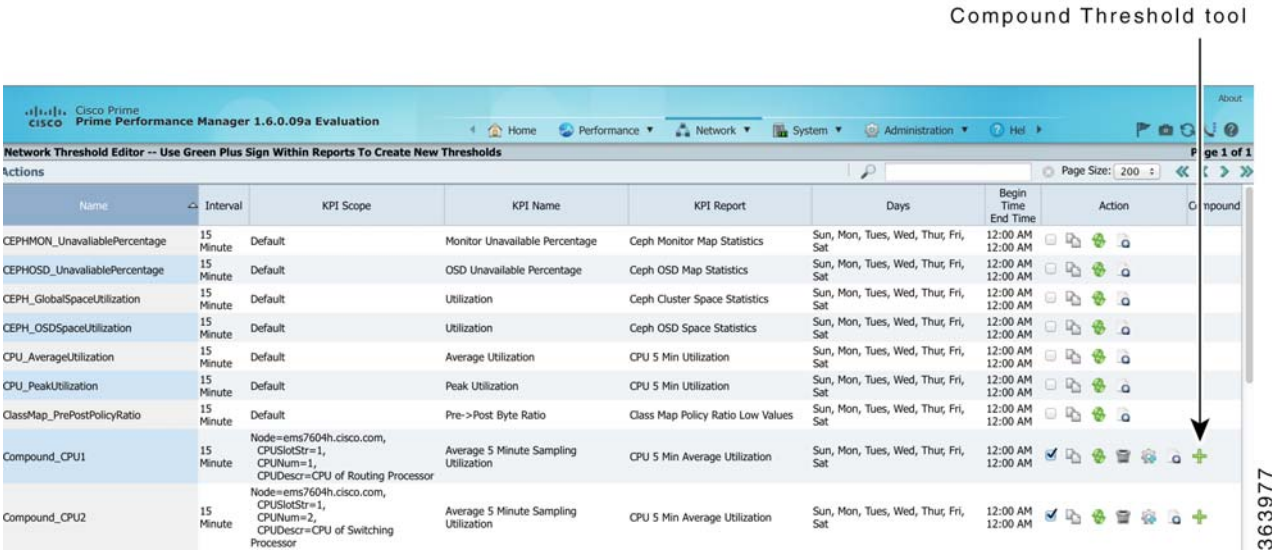
Step 1 Log into Prime Performance Manager GUI as a System Administrator user.

Step 2 If the thresholds that you want to compound are not created, create them using the "Creating Thresholds" procedure on page 11-1.

Step 3 From the Network menu, choose **Threshold Editor**.

Thresholds that can be joined into a compound threshold display the Compound Threshold tool under the Action column, as shown in Figure 11-2. Thresholds that do not display the tool cannot be compounded either because they were created for objects that don't reside within the same device or if on the same device, a single device object.

Figure 11-2 Compound Threshold Tool



Step 4 Select one of the thresholds you want to compound and click the **Compound Threshold** tool. The threshold you choose to start the compound will have the following impact on the compound threshold:

- The threshold days will be used for the compound threshold.
- For AND compound operations, the alarm level of the starting threshold will be displayed for the compound one.

The Create Compound Threshold dialog box displays a list of thresholds that you can compound with the selected threshold.

Step 5 Choose a threshold and click **OK**.

The Add Compound Threshold window appears. It is identical to the Create Threshold window with the following exceptions:

- The Compound Operation field is added so you can choose the compound type.
- The Select KPI field allows you to switch between or among the compounded KPIs. As you switch KPIs, the KPI values are displayed.

For information about other Add Compound Threshold fields, see the following topics:

- Threshold Configuration, page 11-3
- Threshold Values, page 11-6

Step 6 If desired, modify the compounded threshold name in the Name field. By default, the compounded threshold name is the name of the KPI from which you started the compound with "-compounded" appended to it.

Step 7 In the Compound Operation field, choose the compound operation:

- AND—An alarm is not displayed until conditions in all compounded thresholds meet their respective onset requirement.
- OR—An alarm is raised when any compounded KPI meets its onset requirement.

Step 8 Click **OK**.

The Threshold Editor displays the new compounded threshold. The values of all compounded thresholds are displayed. In addition, the Compound Threshold too is available under the Action column to add more thresholds to the compounded one, should you so choose.

Creating Baseline Thresholds

While you can create thresholds for individual KPI values, you can also create thresholds that create alerts when deviations to average values occur. For example, device object utilization might run 30% most of the time. You might want to know whenever a spike to that average occurs, in which case, you would create a baseline threshold. In a baseline threshold, a calculation is made on a specified number of KPI values over a specified time period. The value is multiplied by a specified factor to determine whether an alarm should be raised.

To create a baseline threshold complete the "Creating Thresholds" procedure on page 11-1 and complete the following baseline threshold fields:

- Baseline—Must be checked.
- Baseline method—Sets the method used to calculate the baseline value. Prime Performance Manager supports the average and exponential average methods, described in the following topics:
  - Average Baseline Method Overview, page 11-11
  - Exponential Baseline Method Overview, page 11-12
- Window size—The time period used to calculate the baseline. Window size is expressed as a number of report data intervals, which are specified in the Create Threshold window Report Data Interval field. For example, if you set the report data interval to 15 minutes and enter a window size of 4, the baseline window is one hour.

Note Prime Performance Manager begins calculating baselines with the first received KPI value and proceeds forward until all intervals specified in the window size are collected. If you set a large window size, you do not need to wait until all window values are accumulated before a baseline calculation is performed.

- Onset Factor and Abate Factor—The number that is multiplied by the calculated KPI values from the baseline method and window size to determine whether or an alarm should be raised or cleared. For example, if you want an alarm raised when the KPI rises 10% above the average, you would enter 1.1 as the onset factor. Similarly, if you want an alarm raised if the KPI falls 10% below the average, you would enter .9 as the onset factor.

Average Baseline Method Overview

For average baseline calculations, Prime Performance Manager averages the data points specified by the window size. For example, if the window size is four and the report data interval is 15 minutes, Prime Performance Manager collects the KPI values for the last four 15-minute periods and divides the total by four. This value is multiplied by the onset and abate factors to determine whether an alarm should be generated or cleared.

The following examples show the average baseline calculation method in actual practice. The examples are based on the following window size and onset and abate factors:

- Window Size = 10
- Onset Factor = 1.05
- Abate Factor = 1.01

Example 1

- Baseline values: 200, 200, 200, 200, 200, 200, 200, 200, 200, 200
- Calculated average = 200
- Calculated onset = 210
- Calculated abate = 202

Example 2

- Baseline values: 200, 200, 200, 200, 200, 200, 200, 200, 200, 205
- Calculated average = 200.50
- Calculated onset = 210.525
- Calculated abate = 202.505

Example 3

- Baseline values: 200, 200, 200, 200, 200, 200, 200, 200, 205, 205
- Calculated average = 201
- Calculated onset = 211.05
- Calculated abate = 203.01

Example 4

In this example, the last baseline value, 220, is higher than the calculated onset, 213.05, so an alarm is raised. The next baseline value is 205, which is lower than the calculated abate value, so the alarm is cleared.

- Baseline values: 200, 200, 200, 200, 200, 200, 200, 205, 205, 220 (alarm raised)
- Calculated average = 203
- Calculated onset = 213.05

- Calculated abate = 205.03
- Baseline values: 200, 200, 200, 200, 200, 200, 200, 205, 205, 205 (alarm cleared)

Averaging is based on the last set of collected data values based on the window size and report interval, and therefore can change over time.

Exponential Baseline Method Overview

The exponential moving average (EMA) of KPI values collected in the selected threshold window. An EMA is a moving average for time-series data which places greater weight on more recent data. Using the exponential average baseline method provides a smoother running-average curve. It also requires less computing memory because fewer window size values must be stored. For large window sizes or scenarios where memory is restricted, exponential average might be a better choice over the average baseline calculation method.

Managing Thresholds

Prime Performance Manager thresholds can be viewed, edited, disabled, enabled, and deleted from the Thresholds Editor, shown in Figure 11-2. The editor displays thresholds added from the Prime Performance Manager reports GUI (see Creating Thresholds, page 11-1), and ones created using an XML editor and added directly to the gateway. Threshold management is covered in the following topics:

Editing Thresholds from the Threshold Editor, page 11-12

Enabling and Disabling Thresholds, page 11-14

Deleting Thresholds, page 11-16

Editing Thresholds from the Alarms Window, page 11-13

Displaying Threshold Events, page 11-16

Editing Thresholds from the Threshold Editor

You can edit thresholds either by displaying the Threshold Editor, selecting a threshold, and entering your edits, or by selecting a threshold alarm in the Active Alarms window and editing the threshold there.

To edit a threshold using the Threshold Editor:

Step 1 Log into Prime Performance Manager GUI as a Network Operator or higher user.

Step 2 From the Network menu, choose **Threshold Editor**.

Step 3 In the Actions column of the threshold you want to edit, click **Edit This [*Rising/Falling*] Threshold**.

Step 4 In the Edit Thresholds dialog box, edit any of the following threshold parameters described in the following topics:

- Threshold Configuration, page 11-3

Note You cannot edit the threshold name.

- Threshold Values, page 11-6

Step 5 When finished, click **OK**.

The edits are displayed in the Thresholds Editor.

Editing Thresholds from the Alarms Window

From the Prime Performance Manager Alarms window can perform the following perform the following actions from a threshold crossing alarm:

- Display threshold parameters (all users).
- Edit threshold parameters (administrator users only).
- View a report for the threshold crossing (all users).

When threshold crossing alarms occur, you can display the threshold parameters from the Alarms window:

Step 1 Log into the Prime Performance Manager GUI.

Step 2 From the Network menu, choose **Alarms/Events**.

Step 3 In the Active Alarms window, choose a Threshold Crossing alarm.

Step 4 From the Active Alarms window toolbar, click **Help for Event**.

Step 5 The View Thresholds dialog box or the Edit Threshold dialog box (administrator users) displays the following threshold parameters described in the following topics:

- Threshold Configuration, page 11-3

  Note You cannot edit the threshold name.

- Threshold Values, page 11-6

Step 6 When finished, click **OK**.

Step 7 To view a report for the threshold crossing, in the Alarms window toolbar, click **Event**. A threshold report is displayed. The report is in graph format by default. For information about

The threshold crossing report window appears.

Step 8 When finished, click **OK**.

Displaying Thresholds by Device

You can display thresholds that apply only to a specific device, either thresholds for physical device elements, such as CPU, ports, and interfaces, or thresholds applied to networking technologies provisioned on the device.

To display thresholds by device:

Step 1 Log into the Prime Performance Manager GUI.

Step 2 From the Network menu, choose **Devices**.

Step 3 In the Network Devices window, click the device link for the device whose thresholds you want to view.

Step 4 In the individual device window, click the **Thresholds** tab.

Thresholds that apply to the device, including the polling or device group to which the device belongs, with the report enabled are displayed.

For information about the displayed threshold parameters, or to edit the threshold, see Creating Thresholds, page 11-1.

Actions you can perform from the device thresholds window are described in the following topics:

- Duplicating Thresholds, page 11-14
- Enabling and Disabling Thresholds, page 11-14
- Rearming Thresholds, page 11-15

Duplicating Thresholds

You might occasionally want to create a new threshold with only one or two changes from an existing threshold. If so, you can duplicate the existing threshold, modify the parameters and save the new threshold.

To duplicate a threshold:

Step 1 Log into Prime Performance Manager GUI as a System Administrator user.

Step 2 From the Network menu, choose **Threshold Editor**.

Step 3 In the Actions column of the threshold you want to edit, click **Duplicate This Threshold**.

Step 4 In the Duplicate Threshold dialog box, edit any of the threshold parameters described in the following topics:

- Threshold Configuration, page 11-3
- Threshold Values, page 11-6

Step 5 Click **OK**.

Enabling and Disabling Thresholds

To enable or disable one or more thresholds:

Step 1 Log into Prime Performance Manager GUI as a System Administrator user.

Step 2 From the Network menu, choose **Threshold Editor**.

Step 3 Choose the threshold(s) that you want to enable or disable. (To choose multiple thresholds, press the **Shift** key to select contiguous thresholds, or **Ctrl** to choose noncontiguous thresholds.

Step 4 From the Actions menu, choose **Enable Selected Thresholds** or **Disable Selected Thresholds**.

Prime Performance Manager will update the threshold information.

Note You can also enable and disable thresholds using the "Editing Thresholds from the Alarms Window" procedure on page 11-13.

Filtering Thresholds

To filter the displayed thresholds:

Step 1 Log into Prime Performance Manager GUI as a System Administrator user.

Step 2 From the Network menu, choose **Threshold Editor**.

Step 3 In the Search field, enter the text that you want to use to filter the thresholds. For example, to filter the thresholds by response time, enter Responsetime.

Step 4 Press **Enter**.

Prime Performance Manager filters the thresholds by the text you entered.

Step 5 To display all thresholds, delete the text from the Search field and press **Enter**.

Rearming Thresholds

Rearming thresholds means you have reset the threshold so it can be raised again. In a normal threshold sequence, the TCA alarm is raised when a value crosses the onset value. The threshold is not reset until the parameter value crosses the abate value entered for the threshold at the next polling cycle.

For example, suppose you have a critical threshold defined with onset value of 95 and abate of 80. You have three devices: DevA, DevB, and DevC.

- Poll 1: DevA=98, DevB=97, DevC=98

  Three alarms will appear on the Alarms page, one for each device. You select and clear the alarms for DevB and DevC. You now have one alarm for DevA.

  Note Clearing an alarm rearms the TCA only for DevA and DevB. Rearming the threshold on the Threshold Editor clears all alarms and rearms the threshold for all devices.

- Poll 2: DevA=75, DevB=87, DevC=98

  You now have one alarm. The alarm for DevA is cleared now because the value is below the abate setting. DevB is not above onset. DevC has an alarm because the value is above onset.

- Poll 3: DevA=96, DevB=89, DevC=98

  You have two alarms. DevA is above onset value and DevC is still above abate. You go to Threshold Editor and click Rearm Threshold. Both of the above alarms are cleared. No alarms for this threshold appear on the alarms page.

- Poll 4: DevA=96, DevB=88, DevC=98

  Two alarms will be displayed again.

To rearm a threshold:

Step 1 Log into Prime Performance Manager GUI as a System Administrator user.

Step 2 From the Network menu, choose **Threshold Editor**.

Step 3 In the Network Threshold Editor window, find the threshold you want to rearm then under the Action column (located on the far right of the threshold parameters), choose **Rearm Threshold**.

The threshold is reset and any existing threshold alarms are cleared.

Deleting Thresholds

You cannot delete thresholds provided the Prime Performance Manager installation, but you can delete user-created thresholds.

To delete one or more thresholds:

Step 1 Log into Prime Performance Manager GUI as a System Administrator user.

Step 2 From the Network menu, choose **Threshold Editor**.

Step 3 Choose the threshold(s) that you want to delete. (To choose multiple thresholds, press the **Shift** key to select contiguous thresholds, or **Ctrl** to choose noncontiguous thresholds.)

Step 4 From the Actions menu, choose **Delete Selected Thresholds**.

Step 5 On the confirmation, click **OK**.

Prime Performance Manager will remove the threshold from the table.

Displaying Threshold Events

To view threshold events, from the Navigation menu, choose **Alarms/Events**, then click **Event History**. The types of threshold events that appear include:

- All threshold crossing events, for example:

```
Threshold : 'rising1' - 'Node=csr-c-2941d,ifDescr=ATM0/IMA23' crossed threshold for
'Interface Availability 15 Minute/Down Percentage' time period : '2011-12-06
10:30:00.0' - value '50.0' threshold '5.0'.
```

  and

```
Threshold : 'rising1' - 'Node=csr-c-2941d,ifDescr=ATM0/IMA23' is below threshold for
'Interface Availability 15 Minute/Down Percentage' time period : '2011-12-06
10:15:00.0'
```

- All threshold user creation or edition activities, for example:

```
Gateway: node123- Threshold rising1 - Threshold2811 - 15 Minute was overwritten by
user123.
```

Displaying Recent TCAs

You can view current TCAs in the TCA View. As TCAs occur, TCA View automatically displays the following subviews:

- TCA View—Displays one graph for each threshold with active TCAs. Each graph displays the top ten series for the TCA metric.
- Threshold View—Displays one graph for each defined threshold severity with active TCAs: Critical, Major, Minor. Each graph displays the severity top 10 series.
- Severity View—Displays one graph for each severity. Each graph displays the threshold top 10 series. No data is displayed if the severity level has no TCAs.

As you use TCA View, keep the following in mind:

- Each TCA graph displays the full TCA time range beginning with the first TCA (or the earliest time for which Prime Performance Manager has data) minus one 5-minute interval.
- TCA View is dynamic. Any TCA graph changes that you make are removed when you reload the page.
- TCA View is updated once every five minutes. If a TCA occurs right after an update, it could take up to five minutes to appear in TCA View.

Note For more information about Prime Performance Manager views, see Creating and Managing Custom Report Views, page 7-39.