

Precise 10.3

Alerts User Guide

Exported on 03/17/2021

I D E R A

Table of Contents

Introducing Alerts	5
About Alerts	5
Improved performance management	5
Integrating with other Precise products	5
Components of Alerts	6
Precise FocalPoint.....	7
Alerts FocalPoint.....	7
PMDB	7
Alerts FocalPoint processes.....	7
InformPoint agents	7
How Alerts works	9
Where to get more information	9
Precise Alerts basics.....	10
About the Precise bar.....	10
Tasks common to most tabs	11
Switching to a different tab	11
Determining which table columns to display.....	11
Copying data to the clipboard.....	11
Exporting to Precise Custom Portal	11
Adding, viewing, and deleting Favorites.....	12
Sending an email message	13
About the Alerts user interface.....	13
Launching Alerts	13
Alerts user interface elements.....	14
About the Tab heading	15
About the Metric status legend	15
About the Alerts tree	16
About Alert metrics	16
All Application Alerts.....	16
Working with Alerts.....	19
Investigating alerts	19

Launching Alerts	19
Carrying out further examination of an alert in the Alerts tab.....	19
Manually initiating the metric sampling process	19
Launching other Precise products	20
Configuring Alerts settings	20
Editing metrics	20
Process Availability alerts.....	20
About editing metric properties.....	22
Defining actions on the Actions tab	22
Using dynamic parameters in actions	22
Setting Alerts SNMP connectivity.....	22
Browsing the Alerts MIB.....	22
SNMP trap operation	23
Alerts MOM connectivity	23
Creating customized metrics.....	23
Metric sets.....	24
About Metric sets.....	24
Status set	25
Performance set.....	25
Load set	26
Service set	26
Performance trending set.....	26
Load trending set	27
Precise status set	27
Customized set.....	27

Precise Alerts is an alerting product that helps you manage your system performance proactively. With Alerts, you can effectively detect availability and performance problems and react quickly to solve them.

Alerts samples data collected by other Precise products for the values of a set of metrics and compares these values with a predefined set of values, called thresholds. When the value of a metric exceeds the metric's threshold value, Alerts alerts you through its user interface. It can even perform a defined corrective action.

A major cause of performance problems is imperfect application design. Therefore, monitoring the effectiveness of utilization and the efficient handling of data by the monitored servers are crucial to optimizing performance.

This help content is comprised of the following sections:

- [Introducing Alerts](#)
- [Precise Alerts basics](#)
- [Working with Alerts](#)
- [Metric sets](#)

Introducing Alerts

This section includes the following topics:

- [About Alerts](#)
- [Components of Alerts](#)
- [How Alerts works](#)
- [Where to get more information](#)

About Alerts

In a world where organizations rely on their information systems, avoiding problems that affect service to end-users is of prime concern. Proactive monitoring enables organizations to avoid such conditions by predicting potential problems before they occur. It focuses on identifying conditions that may lead to problems or that indicate that a problem may develop. This enables you to implement corrective solutions before problems surface.

Alerts achieves this by focusing on the following:

- The resources and objects of the sampled devices
- The way your applications use those nodes to detect potential bottlenecks

Improved performance management

IT and operations staffs frequently ask questions like, “I cannot sit next to my console day and night looking for problems in the system. How can I find out immediately when something goes wrong?” and “How can I find out a performance problem exists before receiving complaints from our end-users?”

Using Alerts, IT and operations staffs can focus their valuable time on other activities. Alerts continuously and proactively monitors the health of critical applications.

When Alerts detects a performance problem, it will warn you before the problem affects the service to your end-users. Alerts can even draw your attention to performance problems that occur overnight or while you are away from your desk. To do so, Alerts sends you an email or an SNMP message. In addition, Alerts automatically logs all alerts to keep you fully up-to-date on system performance, no matter when a problem occurred.

When the threshold of a performance metric is exceeded, Alerts alerts you and triggers a user-defined automatic response. You can define thresholds and sampling frequencies for performance metrics using the Alerts user interface, without having to customize the code of your application.

Integrating with other Precise products

Precise consists of the following product suite:

- Alerts
- Report Manager

Alerts and Report Manager are used to support the Detect stage of the Precise methodology. They will alert you to performance problems early in their development and provide you warehouse-type information to support long-term profiling, trend and capacity analysis.

- Precise Custom Portal

The Precise Custom Portal is a lightweight, configurable portal application that provides access to various types of data from different applications. The Precise Custom Portal features a Web-based view. It is highly customizable and extensible, allowing you to build a dashboard for each user or each function within your organization. For example, you can build a dashboard for all the information that a system administrator or director of IT operations

would need to constantly follow up on. This component is automatically installed as part of the Precise framework installation.

- Insight

Insight products monitor the response times of systems and break these times down into the various tiers and components. Insight products also provide tier-specific metrics to help understand the activities in each tier.

- Precise for Web
- Precise for SAP
- Precise for J2EE
- Precise for Microsoft .NET
- Precise for Oracle
- Precise for DB2
- Precise for SQL Server
- Precise for Sybase

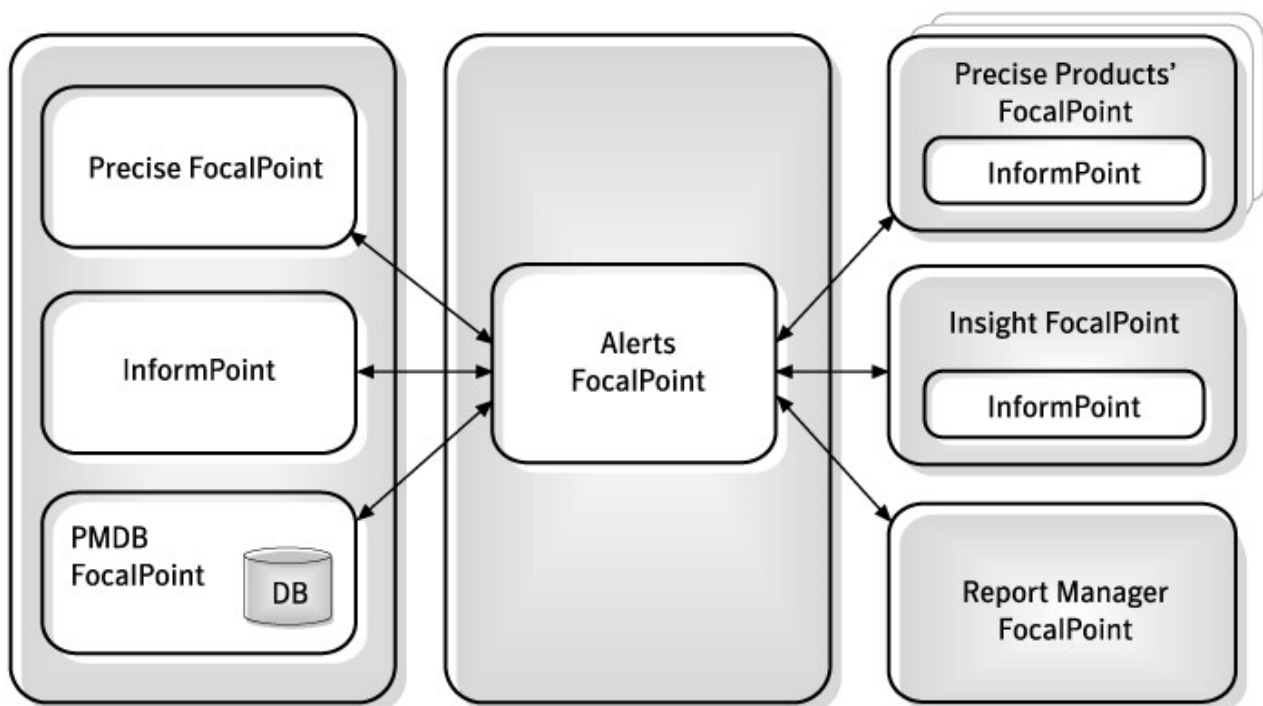
These “Precise for” products provide a way to drill down into problematic tiers to identify and isolate root causes of performance problems. They can also assist in identifying and assessing solutions.

Components of Alerts

Alerts uses a distributed architecture that enables you to monitor performance in your entire application from a single control point.

The figure below illustrates the Alerts architecture.

Figure 1-1 Alerts typical architecture



Alerts consists of the following components:

- Precise FocalPoint and a Web server that communicates with the client’s browser.
- One Alerts FocalPoint that is installed on a system server (or a dedicated server).

- InformPoint agents that are installed on one or more servers in your application. These InformPoint agents sample information from all Precise products (only one agent installation is required for each server).
- One InformPoint agent that is automatically installed on the server where Alerts FocalPoint is installed. This InformPoint agent samples the Status set metrics, and is also available for sampling metrics of Precise products. (If this InformPoint agent is uninstalled, the metrics of the Status set metrics will not be available.) See “Status set” on page 27.
- One or more Internet Explorer windows may be activated on the client-side. Working with Alerts, you may open as many clients as you want.

Precise FocalPoint

Precise FocalPoint is the main FocalPoint of all Precise suite products. FocalPoint is a Precise infrastructure component that communicates with its own distributed agents, each of which gathers information from the other Precise agents on a Tier and stores it locally.

Alerts FocalPoint

Alerts FocalPoint collects data from all InformPoint agents, stores it, and then processes it according to user requests. By processing data in its FocalPoint, Alerts keeps the consumption of your system’s resources at a minimum.

The Alerts FocalPoint software consists of the following components:

- PMDB
- Alerts FocalPoint Processes

PMDB

Alerts FocalPoint stores the sampled data, which is collected by the Alerts agents, in the PMDB. In addition, it stores all Alerts configuration data.

Alerts FocalPoint processes

The Alerts FocalPoint processes perform the following functions:

- Processing sampled data retrieved by InformPoint agents from Precise products. FocalPoint writes the data it receives into the PMDB and, if required, generates actions.
- Communicating with the user interface. Requests issued by users are sent using the user interface to Alerts FocalPoint. The Alerts FocalPoint processes obtain relevant data from either the PMDB or the InformPoint agents, process the data, and send it back to the user by using the user interface.
- Maintaining the PMDB by periodically purging old data.
- Generating pre-defined actions such as:
 - Sending email messages.
 - Displaying popup messages on any open Alerts user interface.
 - Running a program on the FocalPoint server and on the servers where the instance is running.
 - Sending SNMP traps to any SNMP-based management system.

When SNMP is enabled, then Alerts FocalPoint can receive SNMP Get and Set requests, to read or update the PMDB accordingly.

InformPoint agents

The InformPoint agents collect performance data in your system by running pre-defined (generic) metrics and user-defined metrics (customized metrics).

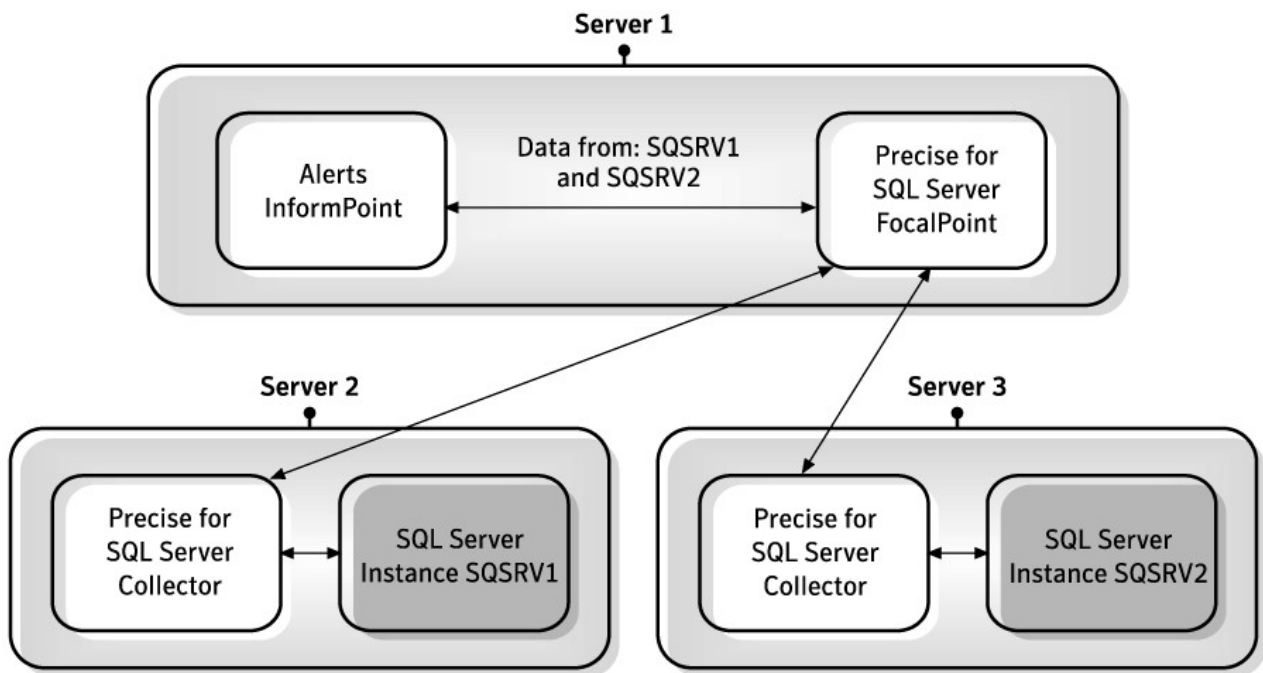
The InformPoint agents process the retrieved data and report to the Alerts FocalPoint. Alerts FocalPoint then correlates this information to provide the current status of the different instances' performance in your application and to alert you to any problematic changes.

The other agents of Precise products collect and process the performance data of the monitored instance and send it to the appropriate FocalPoint of the Precise product. InformPoint, which is installed on the same server as the product's FocalPoint, requests data for all the instances monitored by that product directly from the product's FocalPoint.

Customized Metrics are designed to be executed on the instance server. An InformPoint agent must only be installed on the sampled instance server (using the Agent Installer) if one or more customized metrics for sampling the instance will be defined. For sampling all other Precise product metrics, InformPoint will be installed automatically on the same server of the Precise product FocalPoint server as part of the Precise product FocalPoint installation. InformPoint should not be installed manually using the Server List page (the third stage in the Precise Agent Installer process) if no customized metrics are going to be defined for sampling instances on this server.

The figure below illustrates the typical architecture of InformPoint agents.

Figure 1-2 InformPoint agents



In this example, Alerts monitors a Precise for SQL Server installation. The Precise for SQL Server installation includes two instances on different servers, SQSRV1 and SQSRV2. To enable Alerts to monitor the Precise for SQL Server

product, an InformPoint agent is installed on the Precise for SQL Server FocalPoint (Server 1). Alerts InformPoint collects the alerts data from the Precise FocalPoint product.

See "Creating customized metrics" on page 25.

How Alerts works

Alerts proactively monitors the performance in your application from a centralized location called Alerts FocalPoint. Alerts agents—called InformPoints—query all Precise products. The InformPoints retrieve performance data collected by the Precise products, analyze it, and generate alerts if the predefined thresholds are exceeded.

These alerts are then sent to Alerts FocalPoint, which processes the information, saves it in a local database, and activates any action that is defined for the specific alert.

Once a metric is sampled, the value of the metric is compared to a predefined set of values called thresholds. When the value of the metric exceeds one of the metric's threshold values, an alert is generated and the status of the metric is changed to near-critical or critical.

Metrics are grouped into metric sets. The status of the metric set is the overall status of its metrics. You can monitor the status of metric sets and metrics through the Alerts tab.

To proactively monitor your application, you can define actions that Alerts will automatically perform if it detects a warning or critical status for a specific metric. For example, you can configure Alerts to send an email message, display a pop-up message, run a program, send SNMP traps, or send MOM alerts to the MOM Server.

You can change the default properties of a metric to suit the special requirements of your application. For example, you can change the near-critical and critical thresholds and limit information to be included.

Another important aspect of monitoring is a look at the overall activity to identify current performance problems and compare the load and service of different components.

Where to get more information

More information on Precise, its products, technical notes, and so on, can be found in the [Release Notes](#) for this version.

Precise Alerts basics











This section includes the following topics:

- [About the Precise bar](#)
- [Tasks common to most tabs](#)
- [About the Alerts user interface](#)
- [Launching Alerts](#)
- [Alerts user interface elements](#)

About the Precise bar

The Precise bar enables you to keep track of where you have been and provides various controls. The following table below describes the function of each of the toolbar buttons.

Table 2-1 Precise bar functions

Icon	Name	Description
	Back	During a work session, keeps track of where you have navigated to. The Back button enables you to navigate between previously visited views. The Back control displays your previous view.
	Forward	Enables you to navigate to the next view. This button is only enabled if you clicked Back or if you chose a history option.
	Stop	Stops a request for information from the server.
	Refresh	Updates the data currently displayed.
	Home	Navigates to the highest level entity, usually the instance or tier (all instances). The time frame settings remain the same.
	Send	Opens new email message in your email program with the link to the current application in context.
	Help	Opens the online help in context.
	Favorites	Enables you to add or remove favorites in your Favorites list.
	Settings	Lets you configure process availability settings.
	AdminPoint	Launches Precise AdminPoint.

Tasks common to most tabs

The following tasks are commonly performed in most tabs:

- [Switching to a different tab](#)
- [Determining which table columns to display](#)
- [Copying data to the clipboard](#)
- [Exporting to Precise Custom Portal](#)
- [Adding, viewing, and deleting Favorites](#)
- [Sending an email message](#)

Switching to a different tab

You can easily switch between the different tabs using the Tab Selection bar. When you start your Precise product, the Dashboard tab opens by default. For other Precise products, another tab will open by default. The button of the selected tab is displayed in orange.

To select a tab

- Click a button on the Tab Selection bar to display information on the selected entity in a different tab.

Determining which table columns to display

Tables are used to display information about a set of related entities. It is possible to determine which columns to display in the area tables.

To determine which columns to display in a table

1. Click the Table icon on the upper right-hand side of a table and select **Column Chooser**.
2. In the Table columns dialog box, click the arrows to move the names of the columns that you want to display to the Visible box and the ones that you do not want to display to the Invisible box.
3. Click **OK**.

Copying data to the clipboard

At times you may want to save data displayed in the table area in a Microsoft Excel spreadsheet for further analysis.

To copy data displayed in the table to the clipboard

1. Click the Table icon on the upper right-hand side of the table and select **Copy to clipboard**.
2. Open a Microsoft Excel spreadsheet and choose **Paste** from the Edit menu.

Exporting to Precise Custom Portal

The Export to Precise Custom Portal Portlet feature enables you to export the view of the chosen table or graph and generate a portlet with that view in Precise Custom Portal, so that it will provide you with another way of monitoring your application.

Prerequisites


To be able to use this feature, you need to have the following rights in Precise:

- View permissions to all Tiers in the application.

If you do not have sufficient rights, you will get an error message when trying to execute this feature.

Exporting the information

You can either export a table view or a graph view.

 The name field has the following restrictions: maximum 100 characters.

To export a table view

1. Click the Column Chooser icon.
2. Select **Export to Precise Custom Portal Portlet**.
3. Insert a name in the name field that clearly describes the table view.
4. Click **OK**.

To export a graph view

1. Right-click the graph.
2. Select **Export to Precise Custom Portal Portlet**.
3. Insert a name in the name field that clearly describes the graph view.
4. Click **OK**.

Adding, viewing, and deleting Favorites

The Favorites feature allows you to save a specific location in your application and to retrieve the same location later without having to navigate to it.

About the Favorites feature

The new Favorites feature includes the following options:

- **Relative Time Frame.** Saving relative time frame instead of static date. For example, saving the last 7 days will always display the last 7 days, depending on the day entered.
- **One click to specific location.** Once you open Precise by launching a saved Favorite item, you will not have to enter a login credential nor click the login button.
- **IE Favorites support.** Adding a new Favorite item in Precise will also add it to the IE Favorites menu.
- **Auto Complete.** The Favorites dialog includes a new combo box which supports Auto Complete.
- **Auto Naming.** The Favorites dialog generates item names based on the current location.

UI description

An Add/Delete Favorites option under the Favorites menu allows you to save the current location or delete an existing one.

To add a new Favorite location


1. On the Add/Delete Favorite dialog box, enter the name of the new Favorites entry.
2. Click **Add**. The dialog box is closed and the new Favorite is added to the list.

To view a Favorites location

1. On the Precise bar, click **Favorites**.
2. Select the Favorites location you want to view.

To delete an existing Favorite location

1. On the Add/Delete Favorites dialog box, select the Favorite location to be deleted.
2. Click **Delete**. The dialog box closes and the selected Favorite is deleted from the list.

 The favorite address is displayed in the Address field and cannot be edited.

Sending an email message

You can send an email message to one or more recipients from the Precise toolbar. The default subject for the message will be “Link to a Precise application”.

The email will include a link to the Precise product in the current context (time frame and selected entries).

To send an email message

1. Click the email icon on the Precise toolbar. The default email program opens.
2. Fill in the required fields and click **Send**.

About the Alerts user interface

Alerts is a Web-based application. This means that you do not need to install any special software on your desktop to use Alerts. Instead, the application opens in a normal browser window.

Because Alerts is Web-enabled, you can access it from almost any location that is connected to the World Wide Web as long as you can access your Alerts FocalPoint server.

Although Alerts opens in a browser window it is important to understand that it is an application rather than a Web site. To perform activities within Alerts, you must use the Alerts controls, not the ones of your browser. You should not open information in a New Window, and you should not use the Back or Refresh hot-keys. Instead, use the Precise bar.

Launching Alerts

You launch Alerts from the Application screen or by selecting the Alerts tab on the Dashboard screen. From the Alerts screen, you can view alerts from Application level down to metrics level. Each of these alert levels helps you to isolate the causes of the alerts in the monitored application.

Red or yellow AppTier icon colors indicate a critical or near-critical alert condition. Green AppTier icon colors indicate normal conditions. For a description of the metric status icons see “About the Metric status legend” on page 17.

Alerts can be generated for the following:

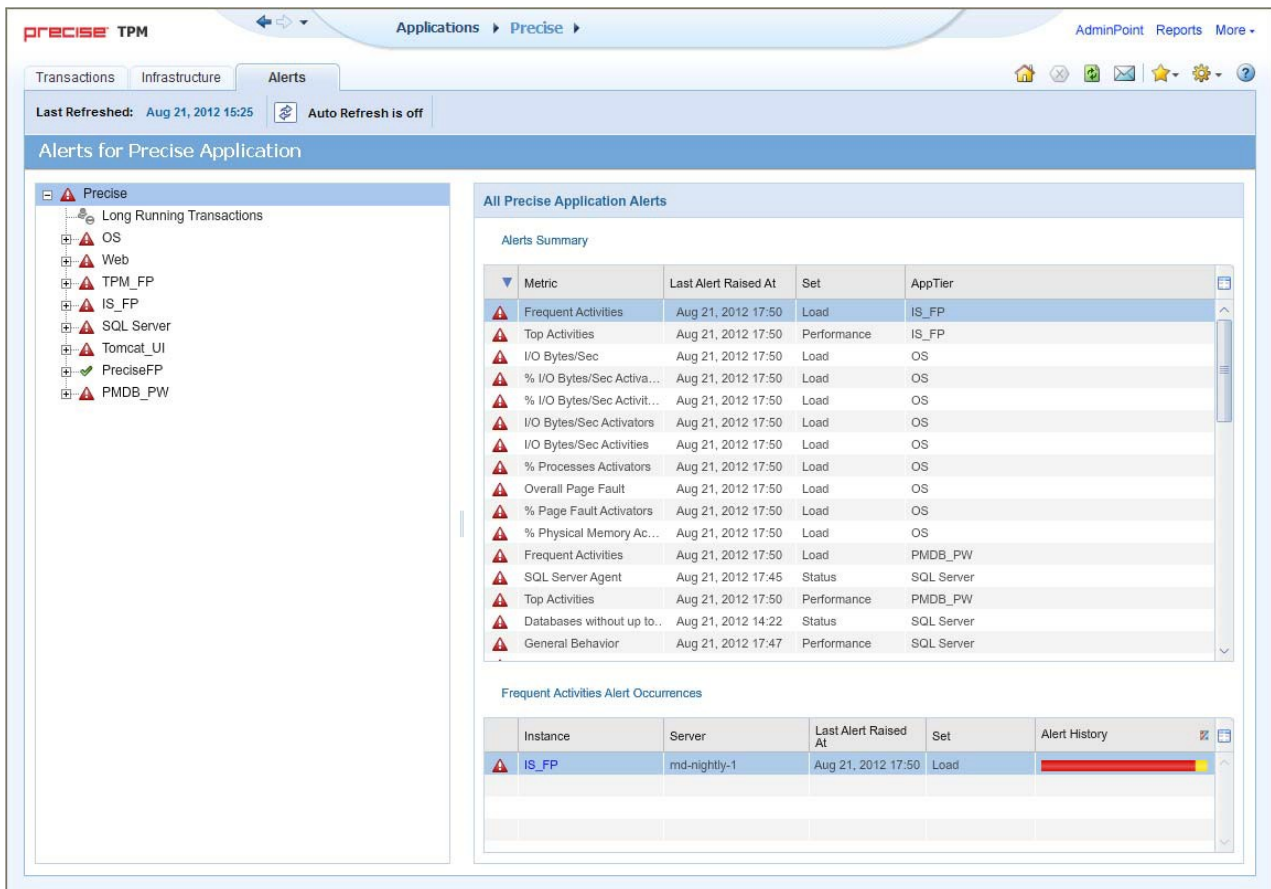
- Activity
- Service
- Trending
- Status

To launch Alerts from the Applications screen:

1. Click the required application from the Applications list.
2. In the Environmental map area, do one of the following:
 - a. Click **Alerts**.
 - b. Click a specific Tier, and from the pop-up menu select **Alerts**. The Alerts screen opens for the specified Tier tab.

The following figure shows an example of the information displayed when you open the Alerts tab for the first time.

Figure 2-1 Alerts Tab



Alerts user interface elements

The Alerts user interface consists of one main screen from which you can access the various alerts.

The Alerts tab display performance, availability, and management data on monitored instances in your application, in table format.

The left side of the main screen lists the Alerts in the following levels:

- Application level
- AppTier level
- Instance level
- Metric level

The right side of the main screen provides details of the alerts according to the element selected in the tree on the left side of the screen as follows:

- **Application level.** All application alerts listing:
 - Alerts Summary
 - Alert Occurrences
- **AppTier level.** AppTier alerts listing:
 - Alerts Summary
 - Alert Occurrences
- **Instance level.** Instance alerts listing all alert instances
- **Metric level.** Details of the instances of the alert including the following details:

- Metric description
- Alert current and historical occurrences
- Alert value
- What to do next

About the Tab heading

The Tab heading provides information about the refresh status. It contains the following:

- Display of the date-and-time when the current tab was last refreshed.
- Auto-Refresh toggle button that also indicates whether it is On or Off. When the Auto-Refresh is On, the tab information is refreshed every one minute.








The Auto-Refresh is On by default, to display the most updated information, in the Cross-Tiers tab and Instances tab of the Tier tab.

The Auto-Refresh is Off by default in the Metrics tab of the Tier tab, because this tab is used for further investigation of specific metrics.

About the Metric status legend

The metric status legend contains icons that indicate the different alert statuses. The table below describes the status icons.

Table 2-2 Status icons

Icon	Status	Description
	Key Metric	Indicates that the metric is defined as a key metric, which is a metric that monitors an important performance aspect. You can define a metric as a key metric through the Thresholds tab of the metric properties.
	Critical	Indicates that the metric value exceeds the defined Critical threshold value.
	Near-Critical	Indicates that the metric value exceeds the defined Near-Critical threshold value.
	Normal	Indicates that the metric value falls in the defined acceptable range.
	Down Time	Indicates that the metric is not sampled due to Down Time definition of the metric's technology or when the sampled instance is not available. You can set the Down Time definition through AdminPoint. See the Precise Administration Guide.
	Disabled	Indicates that the metric is disabled, and therefore it does not sample or generate alerts. A metric is disabled in case the related Precise product is not installed, or the metric properties are set to stop sampling.
	Not Sampled	Indicates that the metric is not sampled since InformPoint was started, or errors occurred during the sampling process.

See “About editing metric properties” on page 24.

About the Alerts tree

The Alerts tree displays the highest alerts in the Tier level, thus simplifying the identification of exceeding metrics.

About Alert metrics

The right side of the Alerts tab displays the following information according to the element selected in the Tiers tree.

- All Application Alerts
- Application Level Metrics
- AppTier Alerts
- Instance Alerts
- Metric Details

All Application Alerts

The table below describes the details displayed in the All Application Alerts table that is displayed when you select the application in the Alerts tree.

Table 2-3 Alerts Summary - All Application Alerts

Column	Description
Alert	Indicates the highest alert severity level of the metric.
Metric	Indicates the metric name.
Last Alert Raised At	Indicates the timestamp of the most recent sample.
Set	Indicates the metric set.
AppTier	Indicates the AppTier name of the metric.

When you select an entry in the Alerts Summary table, details of the instance of the alert are displayed in the Metric Alert Occurrences table.

The table below describes the details displayed in the Metric Occurrences table.

Table 2-4 Metric Alert Occurrences

Column	Description
Instance	Indicates the instance that is sampled by the metric.
Server	Indicates the server name where the instance (that is sampled by the metric) is running.
Last Alert Raised At	Indicates the timestamp of the most recent sample.
Set	Indicates the metric set.

Column	Description
Alert History	<p>Appears only in the Metrics table. Indicates the number of normal, near-critical, and critical alerts that occurred during a pre-defined history period. The number of alerts does not include user-triggered samples (Resamples) from that history period.</p> <p>You can display the bar either in absolute values or relational values (percentage of the total alerts) by clicking the rectangle in the column header.</p> <p>You can modify the history period through the Settings dialog box.</p>

Application Level Metrics

Lists the Application level metrics for all applications. In version 9.5 the only Application level metric is Long Running transactions. The details shown on this page are the same as those show for Instance Alerts, see “Instance Alerts” on page 19.

AppTier Alerts

The table below describes the details displayed in the AppTier Alerts table that is displayed when you select an

AppTier in the Alerts tree

Table 2-5 AppTier Alerts

Column	Description
Alert	Indicates the highest alert severity level of the metric.
Metric	Indicates the metric name.
Last Alert Raised At	Indicates the timestamp of the most recent sample.
Set	Indicates the metric set.

When you select an entry in the AppTier Alerts table details of the instance of the alert are displayed in the Metric Alert Occurrences table.

The table below describes the details displayed in the Metric Occurrences table.

Table 2-6 Metric Alert Occurrences

Column	Description
Instance	Indicates the instance that is sampled by the metric.
Server	Indicates the server name where the instance (that is sampled by the metric) is running.
Last Alert Raised At	Indicates the timestamp of the most recent sample.

Column	Description
Set	Indicates the metric set.
Alert History	Indicates the samples taken organized by time.

Instance Alerts

The table below describes the details displayed in the Instance Alerts table that is displayed when you select an instance in the Alerts tree.

Table 2-7 Instance Alerts

Column	Description
Alert	Indicates the highest alert severity level of the metric.
Metric	Indicates the metric name.
Last Alert Raised At	Indicates the timestamp of the most recent sample.
Set	Indicates the metric set.
Alert History	Indicates the samples taken organized by time.

When you select an entry in the Instance Alerts table details of the instance of the alert are displayed in the Metric Details table (see [Metric Details](#)).

Metric Details

The table below describes the details that displayed when you select a metric in the Alerts tree or in the Instance Alerts table (see [Instance Alerts](#)).

Table 2-8 Metric Details

Column	Description
Metric Description	Detailed description of the metric.
Alert Current and Historical Occurrences	Bar graphic indicating current and historical occurrences.
Alert Value	Displays a sample value for the alert.
What To Do Next	Suggests various option as a next step.

Working with Alerts

This section includes the following topics:

- [Investigating alerts](#)
- [Configuring Alerts settings](#)
- [About editing metric properties](#)
- [Setting Alerts SNMP connectivity](#)
- [Alerts MOM connectivity](#)
- [Creating customized metrics](#)

Investigating alerts

Alerts provides real-time alerts about potential performance problems in your application.

Alerts displays alerts at various levels, which provides alerts summary of the entire application (or few applications if you monitor more than single application). You launch Alerts from the Application screen or by selecting the Alerts tab on the Dashboard screen. From the Alerts screen, you can view alerts from Application level down to metrics level. Each of these alert levels helps you to isolate the causes of the alerts in the monitored application.

The alert levels described in the following topics are ordered from the overview perspective up to the most detailed data:

Launching Alerts

To view the Alerts tab, see [Launching Alerts](#).

Carrying out further examination of an alert in the Alerts tab

The Alerts tab displays the alerts of each AppTier. The Alerts tab includes a Alerts tree that lists all AppTiers, Instances and metrics.

To carry out further examination of an alert

1. In the Alerts tree, click on a row to view the details of a specific alert (for example, a key metric with critical alert).
The details that are displayed on the right side of the screen differ according to the level that you selected in the Alerts tree (see [Alerts user interface elements](#).)
2. Click a row in the table on the right side of the screen to drill down and display details of the specific metric.

Manually initiating the metric sampling process

Metrics are sampled according to the settings of the metric sampling (which can be minutes, hours, or even days). During investigation of an alerted metric, it is important to be sure that the data is the most updated data. Therefore, if you are not sure about the data, you can initiate a sampling process manually.

To manually initiate the metric sampling process

1. On the What To Do Next area, click **Resample**.
2. Wait a few seconds until the sampling process is completed.
3. On the Precise bar, click **Auto Refresh is on** or click **Refresh** to refresh the screen immediately.


i When **Auto Refresh is on**, the screen refreshes automatically according to the settings. You can change the Auto Refresh settings by clicking **Settings** in the Precise bar and choosing **Time Frame Settings**.

Launching other Precise products

To launch the user interface of the relevant Precise product, click the link in the What to do next area.

Configuring Alerts settings

To configure Alerts settings, see [About editing metric properties](#).

 From Alerts version 9.6 forward, all metrics (except for some availability metrics) are enabled by default.

Editing metrics

It is possible to edit the properties of each metric that is available in your Precise application, including the AppTiers metrics (FocalPoints, Agents, Processes, and Licenses) in the system generated “i3 Status” application. You can also add customized metrics to a Tier (excluding the AppTiers), or delete customized metrics.

Go to AdminPoint and see the [Precise Administration Guide](#) to perform the following:

- To configure the Alerts settings
- To edit a metric of a Tier or Tier

Process Availability alerts

Process Availability metrics allow you to monitor a list of processes for specific instances of a specific technology. A process is considered available when running on the server.

The Process Availability monitoring functionality is available for all instances and technologies (Tiers) defined in the Precise installation. You can monitor any process by assigning it to the Process Availability configuration of any instance of any Tier.

The Process Availability metric status is periodically updated every 60 minutes. When a metric status change occurs, the monitoring agent (Insight OS) sends an immediate notification and the status is updated in Alerts within 1 minute.

Functional specification

When you configure Process Availability settings for an instance, a Process Availability metric of the instance is made available. Insight Savvy for OS monitors the availability of instance processes according to the Process Availability settings for the instance. Alerts samples Insight for data that was gathered with a predefined Process Availability metric and sets the metrics alert accordingly. Every change in the Process Availability metric status or content is viewed on the Alerts user interface.

A Process Availability configuration can be defined for all Tier instances as the default configuration (see Instance Association on the Process Availability Settings dialog box). This means that any instance that is recently added to an Tier inherits the Process Availability configuration automatically. In other words, you do not have to manually redefine the configuration for a recently added instance.

Metrics

The Process Availability metric for a specific instance is available on the Alerts user interface only if all of the following conditions are met:

- The Precise framework is installed.
- Alerts and Insight are installed and Insight product is integrated with Alerts.

- Insight OS Agent is installed on the machine the instance is running on.
- The instance is monitored by Alerts (the FocalPoint of the specific instance is integrated with Alerts). This is required so that the instance can be viewed in the Alerts user interface.
- Process Availability settings are defined for the instance.

For more information on the installation of these products, see the Precise Installation Guide.

Settings

A Process Availability configuration includes the list of processes that you want to monitor and their respective details. You configure Process Availability in the Process Availability Settings dialog box, accessible from the Alerts user interface.

To add a new Process Availability setting

1. From the Alerts user interface, on the Precise bar, click **Settings>Process Availability**.
2. In the Process Availability Settings dialog box, select the technology you want to work with and Click **Add**.
3. In the Process Availability Setting - Add dialog box, enter a Process Availability Name. **Do not leave any empty spaces in the name.**
4. Enter User Name (*optional*). Entering the user name limits the availability of processes search to the collection of processes related to the specified user name.
5. To search for processes stored in the PMDB, enter a name or use wildcards (*) at the beginning and/or end of the word (for example, *sql*) and click **Search Now**.
6. Select each process you want to assign to this definition and click the corresponding arrow to move it to the Processes Assigned to this Definition table.
7. You can Add Other Processes/Wildcard Patterns by inserting them in the text box and moving them to the Processes Assigned to this Definition table (for example, sql|Wb*).
8. To create an instance association, select whether to associate to Instances that have not been associated with a Definition or to Specific Instances.
9. If you select Specific Instances, a list of instances that can be monitored (instances that have OS agents installed on the server they are running on) is displayed. Select each instance you want to associate and click the arrow to move it to the table on the right. You can also remove an instance's association by moving the instance back to the table on the left.
10. Click **OK** to accept the settings. The Process Availability Settings dialog box is displayed showing your newly configured Process Availability setting.

The configuration will be deployed and sampled automatically on the selected servers. Data will be available on the Alerts GUI according to the sample rate of the selected metric. If you want to resample, you can do so after a 15 minute wait.

To edit an existing Process Availability definition

1. On the Precise bar, click **Settings>Process Availability**.
2. In the Process Availability Settings dialog box, select the technology you want to edit.
3. Select the Process Availability Name you want to edit.
4. Click **Edit**.
5. In the Process Availability Settings - Edit dialog box, make the changes you want to the processes definitions and instance associations.
6. Click **OK**.

To delete an existing Process Availability definition

1. On the Precise bar, click **Settings>Process Availability**.
2. In the Process Availability Settings dialog box, select the technology in which you want to make a deletion.
3. Select the Process Availability Name you want to delete.
4. Click **Delete**.
5. On displayed confirmation dialog box, click **Yes**.

i If you delete a process availability setting, all instances associated to that setting will automatically be disconnected from the process availability setting and their process availability metric will not be available.

i If you uninstall the OS agent from a server, process availability will not be collected anymore for the instances on this server.

About editing metric properties

Alerts issues alerts according to the metric properties, which must be adjusted to your individual application and organization preferences. The metric definitions must be accurate and adequate. Sampling frequencies and periods require careful considerations. Thresholds need to be set in accordance with the performance level you want to meet.

In addition, alerts must reach the relevant personnel, or in severe cases, management representatives immediately and regardless of their location. Subsequently, the threshold-exceeding values must be examined.

Metric properties are configured by selecting **Settings** in the Precise bar and choosing **Alerts Metric Settings**.

Defining actions on the Actions tab

An application that is monitored by Alerts may generate alerts at any time. Sitting in front of the screen waiting for a metric to go critical may be strenuous and time consuming. Instead, you can set Alerts to inform you about any alert, or to run your repair utility to fix certain problems. See “Defining actions on the Actions tab” in the [Precise Administration Guide](#).

Using dynamic parameters in actions

To use dynamic parameters in actions, go to AdminPoint. See the [Precise Administration Guide](#) for details.

i The dynamic parameters in actions are not the same as used in customized metrics.

Setting Alerts SNMP connectivity

SNMP (Simple Network Management Protocol) is the Internet standard protocol for network management software. See “About setting Alerts SNMP connectivity” in the [Precise Administration Guide](#).

Browsing the Alerts MIB

Before you start browsing the Alerts MIB, it is recommended to be familiar with the following issues:

- Technology representation
- Identifying applications and instances in the MIB
- Identifying metrics in the MIB
- Identifying property fields in the MIB
- MIB structure

See “Browsing the Alerts MIB” in the [Precise Administration Guide](#).

SNMP trap operation

Using SNMP trap operations, you can automatically receive alerts in your SNMP server. The trap message contains critical information about the trap alert.

To enable Alerts to send SNMP traps to your SNMP manager, go to AdminPoint. See the [Precise Administration Guide](#) for details.

Alerts MOM connectivity

See [About Alerts MOM Connectivity](#) in the [Precise Administration Guide](#).

Creating customized metrics

Alerts allows you to monitor any performance aspects using pre-defined metrics for each Tier. For data that is not collected by any of the pre-defined metrics, you can create new customized metrics. (Only users with Administrator privilege are allowed to define customized metrics.)

You can create customized metrics in AdminPoint. See the [Precise Administration Guide](#) for details.

Metric sets

This section includes the following topics:

- [About Metric sets](#)
- [Status set](#)
- [Performance set](#)
- [Load set](#)
- [Service set](#)
- [Performance trending set](#)
- [Load trending set](#)
- [Precise status set](#)
- [Customized set](#)

About Metric sets

Alerts agents, called InformPoints, sample information collected by Precise products for values of a set of metrics and send the sampled data to Alerts FocalPoint. Alerts FocalPoint processes the data, stores it in the FocalPoint database, and, if configured, performs a defined action.

Once a metric is sampled, the value of the metric is compared to a predefined set of values called thresholds. When the value of the metric exceeds one of the metric's threshold values, an alert is generated and the status of the metric is changed to near-critical or critical. You can see full information about the metric on the Metric Properties dialog box.

Metrics are grouped into metric sets. All Metric sets are Tier-dependent (except Status set, which is available for all Tiers and the Precise Status set, which is Cross-Tier dependent), meaning that each set is available for specific Tiers only. The status of the metric set is the overall status of its metrics. You can use the Alerts tab to monitor the status of metric sets and metrics.

The table below describes to which Tiers the metric sets are relevant.

Table 1 Metric set dependency

Tier / Metrics Set	Status	Performance	Load	Service	Performance Trending	Load Trending
OS	✓	✓	✓	✗	✓	✓
Web Client	✓	✓	✓	✓	✓	✓
J2EE	✓	✓	✓	✓	✓	✓
DB2	✓	✓	✗	✗	✗	✗
WebSphere MQ	✓	✓	✓	✓	✗	✗
Tuxedo	✓	✓	✓	✓	✓	✓
Oracle	✓	✓	✓	✓	✓	✓
SQL Server	✓	✓	✓	✓	✓	✓
EMC Storage	✗	✓	✓	✗	✓	✓

Tier / Metrics Set	Status	Performance	Load	Service	Performance Trending	Load Trending
SAP	✓	✓	✓	✓	✓	✓
Oracle Applications	✓	✓	✓	✓	✓	✓
Other	✓	✓	✓	✓	✗	✗
Microsoft .NET	✓	✓	✓	✓	✗	✗
Sybase Replication Server	✗	✓	✗	✗	✗	✗

i The Performance Trending and Load Trending metric sets include metrics that are sampled by Report Manager, that is, each metric alerts to one or more Report Manager exception reports. For more information, see the *Report Manager User's Guide*. Maintenance metrics are available in the Service set.

Status set

The Status set includes metrics that report the status of the instance and maintenance metrics. If the instance applies to several components, then several metrics may appear. If the instance has any other status indication, a relevant metric should also appear. For example, in Oracle Tier, the Oracle alert log indicates information relevant to the general activity of the instance.

The Maintenance metrics report on maintenance issues relevant to the specific instance type, for example, for an Oracle database, report on objects with a high number of extents. The Maintenance metrics are relevant to Oracle and SQL Server Tiers.

Performance set

The Performance set helps find performance bottlenecks in your system. It includes the following metrics that measure the level of performance currently achieved by the system:

- **General Behavior.** Measures the resources consumption of the instance to detect times when the instance consumes a higher level of resources than is normal (according to definition), for example when the instance level memory usage is high.
- **Top Activities.** Reports on resource consumption of activities to allow the detection of activities that are high resource consumers, for example, Oracle programs using a high percentage of Oracle resources. The alert is generated on an activity level, that is, as a percentage of the resources the activity used out of the resources that the instance consumed. For example, when an SQL statement in the Oracle Tier is using 20% of the total resources consumed by the Oracle instance.
- **Top Activators.** Report on resource consumption of activators to allow the detection of activators that are high resource consumers, for example, Oracle users consuming a high percentage of Oracle resources. The alert is generated on an activator level (such as, Users, Locales, and IPs). The Top Activators are displayed as a percentage of the resources the activator consumed out of the resources that the Oracle instance consumed.
- **Long I/O waits.** Reports on I/O waits to allow the detection of objects that have a long access time and are causing activities to have a long I/O wait time while accessing them. The alert is generated on an I/O object level, that is, as a percentage of the I/O wait time the I/O file spent out of the total I/O wait time that the Oracle instance spent.

- **Internal performance metrics.** Reports on internal components and procedures of the instance. These metrics are Tier-specific, for example, for an Oracle database, a report on SGA utilization, on Oracle sessions that are waiting for a lock, and so on.


Load set

The Load set helps to identify any increase of load on the system, which can cause a decrease in the performance. It includes the following metrics that measure the load on the system:

- **Frequent Activities.** Reports on activities that have a high number of executions compared to the total number of executions in the instance. This might help you point out abnormal activities, wrong use of the system, and so on.
- **Frequent Activators.** Reports on originators that have a high number of executions compared to the total number of executions in the instance. This might help you point out abnormal originators; for example, SAP users running many transactions.
- **High I/O activity.** Reports on I/O objects that have high access hits compared to the total number of accesses in the instance. This might help you point out objects that were accessed many times compared to all other objects in the system.
- **Internal load metrics.** Indicates the internal load. This might help you point out times when instance resources are exceeded. For example, when the number of logged-in users approaches, reaches, or transgresses the allowed maximum, and so on.

Service set

The Service set includes SLA metrics. The SLA metrics indicates the actual service level compared to the predefined SLAs. These metrics help to identify a decrease in response time.

 Alerts samples the data for the Service metrics from Insight and not from the “Precise for” products (except for SAP and Web Tiers, which retrieve their Service data from their “Precise for” products and not from Insight).

The following SLA metrics are included:

- **Overall SLA Compliance.** Reports on the total instance performance not conforming to the defined SLA.
- **SLA Breaching Activities.** Reports on activities that exceeded their defined SLA, for example, programs taking longer than defined.
- **SLA Breaching Activators.** Reports on activators that get bad response times, for example, users suffering from SLA breaches.

Performance trending set

The Performance Trending set helps you point out problematic performance aspects that cannot be pinpointed in the short term. The performance trending set holds the following metrics that measure the performance of the instance over a longer period of time:

- **Instance Performance (Exceptions).** Based on daily and/or monthly Report Manager reports that compare the instance performance to a baseline.
- **Activity Performance (Exceptions).** Based on daily and/or monthly Report Manager reports for the different activities that:
 - Compare the average performance of each activity to its baseline.
 - Compare the average time of all the activities to a baseline.

- **Internal performance trending metrics.** Includes metrics based on daily and/or monthly Report Manager reports that compare the performance of internal instance components to their baseline.

The metrics in this set are sampled by Report Manager.

Load trending set

The Load Trending set helps you identify a change in the load levels of the system that cannot be pinpointed in the short term.


It holds the following metrics that measure the load of the instance over a longer period of time.

- **Activity Volume (Exceptions).** Based on daily and/or monthly Report Manager reports that compare:
 - The number of executions of an activity in relation to its baseline.
 - The percentage of executions of an activity to the total of executions of all the activities in relation to a baseline.
- **Activator Volume (Exceptions).** Based on daily and/or monthly Report Manager reports that compare:
 - The number of executions by each activator in relation to the relevant baseline.
 - The percentage of executions by activator to the total of executions by all activators in relation to a baseline.

The metrics in this set are sampled by Report Manager.

Precise status set

The Precise status set is available in the Precise Status application for Cross-Tiers.

 Metrics for the i3 Status application do not appear in the alerts report on screen, and are indicated by the action items defined in the metric properties only. See the [Precise Administration Guide](#) for details.

- **FocalPoints.** Indicates the FocalPoint agents' status.
- **Agents.** Indicates the agents' status, excluding FocalPoint agents.
- **Licenses.** Indicates the license status of Precise components.
- **Processes.** Indicates the status of PMDB processes.

Customized set

The Customized set holds all user-defined metrics. You can create customized metrics to sample any system data. You can create customized metrics in AdminPoint. See the [Precise Administration Guide](#) for details.