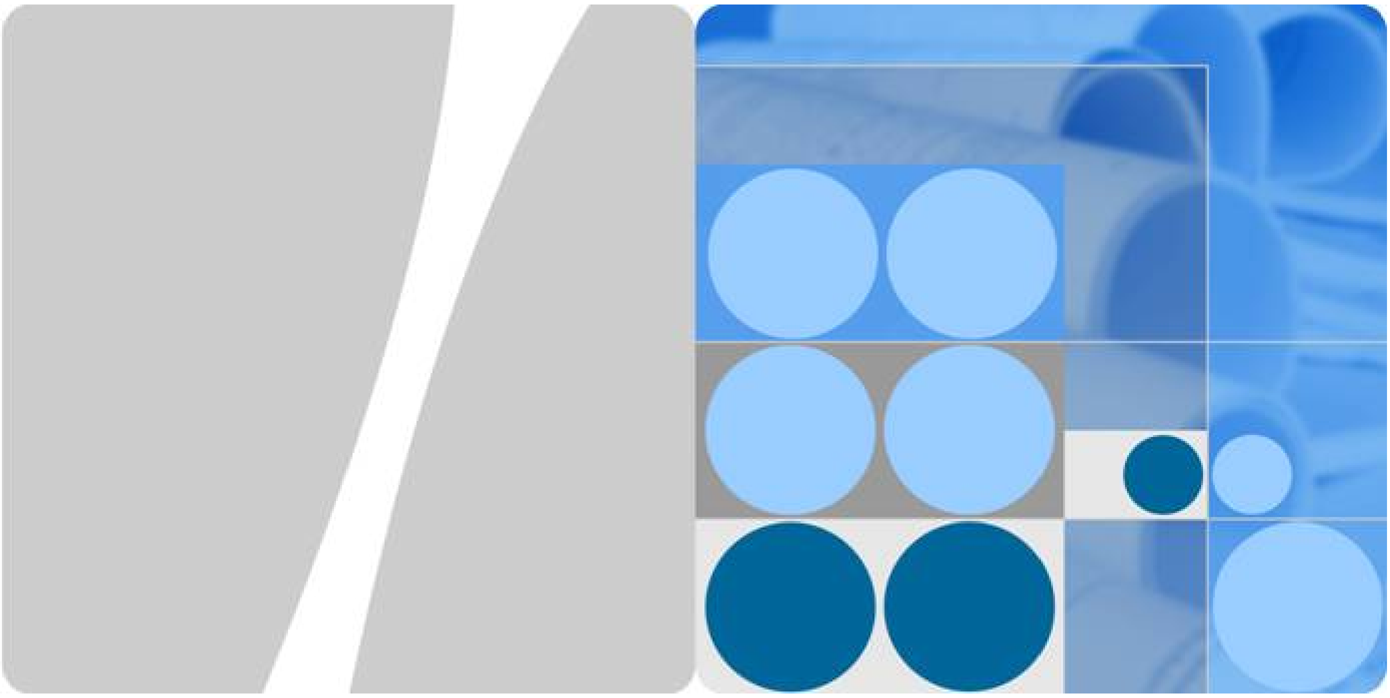


Cloud Eye

User Guide

Date **2018-05-30**

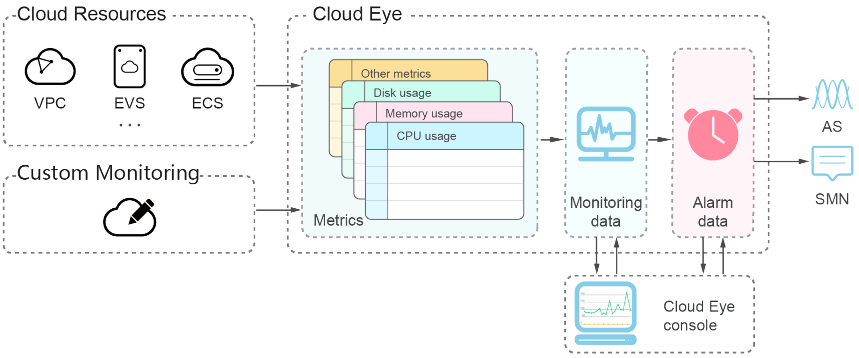
Contents

1 Product Introduction

1.1 What Is Cloud Eye?

Cloud Eye is a multi-dimensional resource monitoring service. You can use Cloud Eye to monitor resources, set alarm rules, identify resource exceptions, and quickly respond to resource changes. **Figure 1-1** shows the Cloud Eye architecture.

Figure 1-1 Cloud Eye architecture



Cloud Eye provides the following functions:

- Automatic monitoring

  Monitoring starts automatically after you have enabled cloud services and created resources such as Elastic Cloud Servers (ECSs). On the Cloud Eye console, you can view the service status and set alarm rules for these resources.

- Flexible alarm rule configuration

  You can create alarm rules for multiple resources at the same time. After you create an alarm rule, you can modify, enable, disable, or delete it at any time. For more information, see **4.5 Alarm Rule Management**.

- Real-time notification

  You can enable Simple Message Notification (SMN) when creating alarm rules. When the cloud service status changes and the monitoring data of the metric reaches the threshold specified in an alarm rule, Cloud Eye notifies you by emails, or by sending messages to server addresses, allowing you to monitor the cloud resource status and changes in real time.

- Monitoring panel

  The panel enables you to view cross-service and cross-dimension monitoring data. It displays key metrics, providing an overview of the service status and monitoring details that you can use for troubleshooting. For more information, see **3.1 Introduction to Monitoring Panels**.

1.2 Advantages

Automatic Provisioning

Cloud Eye is automatically enabled for all users. You can use the Cloud Eye console or APIs to view the service running status and set alarm rules.

Real-time and Reliable Monitoring

Raw data is reported to Cloud Eye in real time for monitoring of cloud services.

Alarms are generated and notifications are sent to you in real time.

Monitoring Visualization

You can create monitoring panels and graphs to compare multiple metrics. The graphs automatically refresh to display the latest data.

Multiple Notification Types

You can enable the SMN service when creating alarm rules. When the metric data reaches the threshold specified in an alarm rule, Cloud Eye notifies you by emails, allowing you to keep track of the running status of cloud services. Cloud Eye can also send HTTP/HTTPS messages to an IP address of your choice, enabling you to build smart alarm handling programs.

Batch Creation of Alarm Rules

Alarm templates allow you to create alarm rules in batches for multiple cloud services.

1.3 Application Scenarios

Cloud Service Monitoring

After enabling a cloud service supported by Cloud Eye, you can view the running status of the cloud service and the usage of each metric, and create alarm rules for metrics on the Cloud Eye console.

Performance Issues

When an alarm rule's conditions are met, Cloud Eye generates an alarm and invokes the SMN API to send the notifications, allowing you to understand the root cause of performance issues.

Capacity Expansion

After creating alarm rules for metrics such as CPU usage, memory usage, and disk usage, you can track the running status of a cloud service. If the service volume increases, Cloud Eye sends you an alarm notification, enabling you to manually expand the capacity or configure AS to automatically increase capacity.

Custom Monitoring

Custom monitoring supplements cloud service monitoring. If Cloud Eye does not provide the required metrics, you can use custom monitoring and report the collected monitoring data to Cloud Eye. Cloud Eye helps to display those monitoring data in graphs and allows you to create alarm rules for those custom metrics.

Log Monitoring

The log monitoring function enables you to monitor log content in real time. You can set alarm rules on Cloud Eye to monitor the logs collected by Log Tank Service (LTS), thus to reduce your O&M cost for log monitoring and simplify the log monitoring process.

Event Monitoring

In event monitoring, you can query system events that are automatically reported to Cloud Eye and custom events reported to Cloud Eye through the API. You can create alarm rules for both system events and custom events. When specific events occur, Cloud Eye generates alarms for you.

1.4 Related Services

Once you start to use Cloud Eye, the system automatically identifies cloud services enabled on the current cloud platform, captures their key metrics, and reports monitoring data of these metrics to Cloud Eye.

At present, Cloud Eye supports automatic monitoring of the following metrics:

Computing

- **6.1.1 ECS Metrics**
- BMS Metrics Under OS Monitoring
- **6.1.2 AS Metrics**

Storage

- **6.2.1 EVS Metrics**

- **6.2.2 SFS Metrics**

Network

- **6.3.1 EIP and Bandwidth Metrics**
- **6.3.2 ELB Metrics**

1.5 Basic Concepts

The following concepts are central to your understanding and use of Cloud Eye:

- **Metrics**
- **Rollup**
- **Monitoring Panels**
- **Topics**
- **Alarm Rules**
- **Alarm Templates**
- **Projects**

Metrics

A metric refers to a quantized value of a resource dimension on the cloud platform, such as the ECS CPU usage and memory usage. A metric is a time-dependent variable that generates a series of monitoring data over time. It helps you understand the metric changes over a specified period of time.

Rollup

Rollup is the process in which Cloud Eye calculates the average, maximum, minimum, sum, or variance value based on sample raw data reported by each cloud service in specific periods. The calculation period is called rollup period. Cloud Eye supports the following rollup periods: 5 minutes, 20 minutes, 1 hour, 4 hours, and 24 hours.

Monitoring Panels

Monitoring panels allow you to view monitoring data of metrics of different services and dimensions. You can use monitoring panels to display metrics of key services in a centralized way, get an overview of the service running status, and use monitoring data for troubleshooting.

Topics

A topic is used to publish messages and subscribe to notifications. Topics provide you with one-to-many publish subscription and message notification functions. You can send messages to different types of endpoints with just one message request. Cloud Eye uses SMN to notify you of cloud service resource changes, enabling you to track the running status of cloud services in a timely manner.

Alarm Rules

You can create alarm rules to set thresholds for cloud service metrics. When the status (such as **Alarm** and **OK**) of the alarm rule changes, Cloud Eye notifies you by sending emails, or by sending HTTP/HTTPS messages to servers.

Alarm Templates

Alarm templates contain one or more alarm rules for specific services. The templates help you create alarm rules for multiple cloud services, improving O&M efficiency.

Projects

A project is used to group and isolate OpenStack resources, such as the compute, storage, and network resources. A project can either be a department or a project team. You can use an account to create multiple projects.

1.6 Constraints

Table 1-1 lists Cloud Eye resource limits for a user.

Table 1-1 User resource limits

Quota Type	Default Limit
Number of alarm rules that can be created	100
Number of custom alarm templates that can be created	50
Number of alarm rules that can be added to an alarm template	20
Number of monitoring panels that can be created	20
Number of graphs that can be added to a monitoring panel	24
Number of topics that can be selected	5

1.7 Region and AZ

Concept

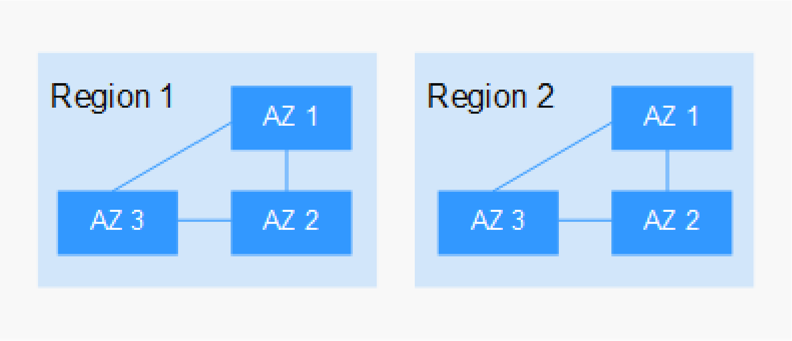
A region and availability zone (AZ) identify the location of a data center. You can create resources in a specific region and AZ.

- A region is a physical data center, which is completely isolated to improve fault tolerance and stability. The region that is selected during resource creation cannot be changed after the resource is created.

- An AZ is a physical location where resources use independent power supplies and networks. A region contains one or more AZs that are physically isolated but interconnected through internal networks. Because AZs are isolated from each other, any fault that occurs in one AZ will not affect others.

Figure 1-2 shows the relationship between regions and AZs.

Figure 1-2 Regions and AZs



Selecting a Region

Select a region closest to your target users for lower network latency and quick access.

Selecting an AZ

When deploying resources, consider your applications' requirements on disaster recovery (DR) and network latency.

- For high DR capability, deploy resources in different AZs within the same region.
- For lower network latency, deploy resources in the same AZ.

Regions and Endpoints

Before you use an API to call resources, specify its region and endpoint. For more details, see **Regions and Endpoints**.

2 Getting Started

2.1 Checking the Overall Status of a Cloud Platform

On the **Monitoring Overview** page, you can view information about **Monitored Object Statistics**, **Alarm Rule Statistics**, and **Resource Monitoring Preview (in the Alarm State)** to quickly track the overall status of the cloud platform.

Viewing Monitored Object Statistics

1. Under **Management & Deployment**, select **Cloud Eye**.
2. In the navigation pane on the left, choose **Dashboard** > **Monitoring Overview**, and you can view the service resource quantity in the **Monitored Object Statistics** area.

Resource Monitoring Preview (in the Alarm State)

Graphs are used to display the metric status of service resources in the **Alarm** status, helping you to know the resource running status and handle exceptions in a timely manner. Click the resource name, and you can go to the page displaying alarm rule details configured for this resource.

Alarm Rule Statistics

In the **Alarm Rule Statistics** area, numbers of alarm rules in the **Alarm**, **OK**, **Disabled**, and **Insufficient data** status are displayed one by one. Click the number of one type of alarm rules, and you can directly go to the **Alarm Rules** page displaying the alarm rule list of this type.

2.2 Querying Metrics of a Cloud Service

Cloud Eye provides multiple built-in metrics based on the characteristics of each service. After you enable one cloud service on the cloud platform, Cloud Eye automatically associates its built-in metrics. You can monitor these metrics to know the service running status.

This topic describes how to view monitoring data of cloud service resources.

Procedure

1. Under **Management & Deployment**, select **Cloud Eye**.
2. In the navigation pane on the left, choose **Cloud Service Monitoring**, and select a cloud service.

   The cloud service page is displayed.
3. Locate the row that contains the cloud service resource you want to monitor and click **View Graph** in the **Operation** column.

   On the displayed page, you can view graphs based on raw data collected in the last **1h**, **3h**, **12h**, **1d**, and **7d**. In the upper right corner of the graph, the maximum and minimum values of the metric in the corresponding time periods are dynamically displayed. You can also enable **Auto Refresh** to view the real-time data refreshed every minute.
4. Hover your mouse over a graph and click ⤢ in the upper right corner.

   An enlarged graph of the metric is displayed, on which you can view the metric monitoring details for longer time ranges. In the upper left corner, you can see six default monitoring periods: **1h**, **3h**, **12h**, **1d**, **7d**, and **30d**. You can also view historical monitoring data for any period during the last six months by customizing the monitoring period in the upper right corner of the graph.

   NOTE

   - If you select **1h**, **3h**, **12h**, or **1d**, raw data is displayed by default. You can click **Settings** in the upper left corner of the graph to change the rollup method of the monitoring data.
   - If you select **7d** or **30d**, aggregated data is displayed by default. You can click **Settings** in the upper left corner of the graph to change the rollup method of the monitoring data.
5. To export data, click **Export Data** on the **Cloud Service Monitoring** page, set parameters as prompted, and click **Export**.

3 Monitoring Panels

3.1 Introduction to Monitoring Panels

Panels serve as custom monitoring platforms and allow you to view core metrics and compare the performance data of different services.

3.2 Creating a Monitoring Panel

You must create a monitoring panel before you add graphs. You can create a maximum of 20 monitoring panels.

Procedure

1. Under **Management & Deployment**, select **Cloud Eye**.
2. In the navigation pane on the left, choose **Dashboard** > **Monitoring Panels** and click **Create Panel**.

   The **Create Panel** dialog box is displayed.
3. Set the panel name.

   Enter a maximum of 128 characters. Only letters, digits, hyphens (-), and underscores (_) are allowed.
4. Click **OK**.

3.3 Adding a Graph

After you create a panel, you can add graphs to the panel to monitor cloud services. Each panel supports a maximum of 24 graphs.

You can add a maximum of 20 metrics to one graph. Monitoring comparison between different services, dimensions, and metrics is supported.

Procedure

1. Under **Management & Deployment**, select **Cloud Eye**.

2. Choose **Dashboard** > **Monitoring Panels**, switch to the desired panel, and click **Add Graph**.

   The **Add Graph** dialog box is displayed.

3. Set parameters based on **Table 3-1**.

Table 3-1 Parameters

Parameter	Description
Title	Specifies the title of the graph to be added. Only letters, digits, underscores (_), and hyphens (-) are allowed. Enter a maximum of 128 characters. Example value: **widget-axaj**
Resource Type	Specifies the type of the resource to be monitored. Example value: **Elastic Cloud Server**
Dimension	Specifies the metric dimension. Example value: **ECSs**
Monitored Object	Specifies the monitored objects of the metric. You can select a maximum of 20 monitored objects at a time.
Metric	Specifies the metric name. Example value: **CPU Usage**

4. Click **OK**.

   On the selected panel, you can view the trends of the new graph. If you hover your mouse on the graph and click ⤢, you can view detailed metric data comparison.

3.4 Viewing a Graph

After you add a graph, you can view the metric trends on the **Monitoring Panels** page. The system provides you both default time ranges to view trends from last month. This topic describes how to view trends for a longer time range.

Procedure

1. Under **Management & Deployment**, select **Cloud Eye**.
2. Choose **Dashboard** > **Monitoring Panels**.

   You can view all monitoring graphs on the current monitoring panel.

   NOTE

   - You can sort graphs by dragging them.
   - Click **1h**, **3h**, **12h**, **1d**, **7d**, or **30d** in the upper left to switch the monitoring periods of all graphs on the panel.

3. Hover your mouse over a graph. In the upper right corner, click ⤡ to view monitoring details on an enlarged graph. You can select a time period to view the metric trend in a specific monitoring interval.

   If you select **1h**, Cloud Eye displays raw data from the last hour by default; if you select any of the other time periods, Cloud Eye displays rolled-up data.

3.5 Configuring a Graph

This topic describes how to add, modify, and delete metrics on graphs.

Procedure

1. Under **Management & Deployment**, select **Cloud Eye**.
2. In the navigation pane on the left, choose **Dashboard** > **Monitoring Panels**, select the target panel and graph, and click the configure icon.

   On the displayed **Configure Graph** dialog box, you can edit the graph title and add new metrics. You can also delete or modify the current metrics.

   NOTE

   You can add up to 20 metrics to a single monitoring graph.

3.6 Deleting a Graph

1. Under **Management & Deployment**, select **Cloud Eye**.
2. In the navigation pane on the left, choose **Dashboard** > **Monitoring Panels**.
3. Select the monitoring panel from which you want to delete a graph.
4. Hover your mouse on the target graph and click the trash icon in the upper right corner.
5. In the displayed **Delete Graph** dialog box, click **Yes**.

3.7 Deleting a Panel

If you need to re-plan graphs on a panel, you can delete the existing panel. After you delete a panel, all graphs associated with it will be deleted.

Procedure

1. Under **Management & Deployment**, select **Cloud Eye**.
2. In the navigation pane on the left, choose **Dashboard** > **Monitoring Panels**.
3. Select the monitoring panel to be deleted.
4. Click **Delete**.
5. In the displayed **Delete Monitoring Panel** dialog box, click **Yes**.

4 Using the Alarm Function

4.1 Introduction to the Alarm Function

You can set alarm rules for key metrics of cloud services. When the conditions in the alarm rule are met, Cloud Eye sends email, or sends HTTP/HTTPS messages, enabling you to quickly respond to resource changes.

Cloud Eye invokes the SMN APIs to send notifications. This requires you to create a topic and add subscriptions to this topic on the SMN console. Then, when you create alarm rules on Cloud Eye, you can enable the alarm notification function and select the topic. When alarm rule conditions are met, Cloud Eye sends the alarm information to the subscriptions in real time.

NOTE

If no alarm notification topic is created, alarm notifications will be sent to the default email address of the login account.

4.2 Creating Alarm Notification Topics

4.2.1 Creating a Topic

Scenarios

A topic serves as a message sending channel, where publishers and subscribers can interact with each other.

You can create your own topic.

Creating a Topic

1. Choose **Service List** > **Application** > **Simple Message Notification**.

   The SMN console is displayed.

2. In the navigation pane on the left, choose **Topics**.

   The **Topics** page is displayed.

3. Click **Create Topic**.

   The **Create Topic** dialog box is displayed.

4. Enter a topic name and display name (topic description).

Table 4-1 Parameters required for creating a topic

Parameter	Description
Topic Name	Specifies the topic name, which ● Contains only letters, digits, hyphens (-), and underscores (_) and must start with a letter or a digit. ● Must contain 1 to 256 characters. ● Must be unique and cannot be modified after the topic is created.
Display Name	Specifies the message sender name, which must be less than 192 characters. **NOTE** After you specify a display name in *Display name***<username@example.com>** format, the name you specify will be displayed as the email sender. Otherwise, the sender name will be displayed as **username@example.com**.

5. Click **OK.**

   The topic you created is displayed in the topic list.

   After you create a topic, the system generates a uniform resource name (URN) for the topic, which uniquely identifies the topic and cannot be changed.

6. Click a topic name to view the topic details and the total number of topic subscriptions.

Follow-up Operations

After you create a topic, **add subscriptions**. After the subscriptions have been confirmed, alarm notifications will be sent to the subscription endpoints via SMN.

4.2.2 Adding Subscriptions

A topic is a channel used by SMN to broadcast messages. Therefore, after the topic is created, you need to add related subscriptions. In this way, when the metric triggers an alarm, Cloud Eye sends the alarm information to subscribers of the topic.

Adding Subscriptions

1. Log in to the management console.
2. In the **Application** category, select **Simple Message Notification**.

   The SMN console is displayed.

3. In the navigation pane, choose **Topics**.

   The **Topics** page is displayed.

4. Locate the topic you want to add subscriptions to, click **More** under **Operation**, and select **Add Subscription**.

   The **Add Subscription** dialog box is displayed.

5. Specify the subscription protocol and endpoints.

   If you enter multiple endpoints, enter each endpoint on a separate line.

6. Click **OK**.

   The subscriptions you added are displayed in the subscription list.

4.3 Creating Alarm Rules

4.3.1 Introduction to Alarm Rules

You can flexibly create alarm rules on the Cloud Eye console. You can create an alarm rule for a specific metric or use the alarm template to create alarm rules in batches for multiple cloud service resources.

Cloud Eye provides you with default alarm templates tailored to each service. In addition, you can also create custom alarm templates by modifying the default alarm template or by specifying every required field.

4.3.2 Creating an Alarm Rule

This topic describes how to create an alarm rule.

Creating an Alarm Rule

1. Log in to the management console.
2. Under **Management & Deployment**, select **Cloud Eye**.
3. In the navigation pane on the left, choose **Alarm Management** > **Alarm Rules**.
4. Click **Create Alarm Rule** in the upper right corner.
5. On the **Create Alarm Rule** page, follow the prompts to set the parameters.
   a. Set the alarm rule name and description.

   Table 4-2 Name and **Description**

Parameter	Description
Name	Specifies the alarm rule name. The system generates a random name, which you can modify. Example value: **alarm-b6al**
Description	(Optional) Provides supplementary information about the alarm rule.

   b. Select a monitored object and set alarm rule parameters.

Table 4-3 Parameters

Parameter	Description	Example Value
Resource Type	Specifies the type of the resource the alarm rule is created for.	Elastic Cloud Server
Dimension	Specifies the metric dimension of the selected resource type.	ECSs
Monitoring Scope	Specifies the monitoring scope the alarm rule applies to. You can select **Resource groups** or **Specific resources**. **NOTE** ● If **Resource groups** is selected and any resource in the group meets the alarm policy, an alarm is triggered. ● If you select **Specific resources**, select one or more resources and click » to add them to the box on the right.	Specific resources
Select Group	This parameter is mandatory when **Monitoring Scope** is set to **Resource groups**.	-
Method	There are two options: **Use template** or **Create manually**.	Create manually
Template	Specifies the template to be used. You can select a default alarm template or **a custom template**.	-
Alarm Policy	Specifies the policy for triggering an alarm. If you set **Resource Type** to **Website Monitoring**, **Log Monitoring**, **Custom Monitoring**, or a specific cloud service, whether to trigger an alarm depends on whether the metric data in consecutive periods reaches the threshold. For example, Cloud Eye triggers an alarm if the average CPU usage of the monitored object is 80% or more for three consecutive 5-minute periods. If you set **Resource Type** is to **Event Monitoring**, the event that triggers the alarm is an instant event. For example, if event improper ECS running occurs, Cloud Eye triggers an alarm.	-
Alarm Severity	Specifies the alarm severity. Valid values are **Critical**, **Major**, **Minor**, and **Informational**.	Major

c. Set **Alarm Notification** parameters.

Table 4-4 Alarm Notification parameters

Parameter	Description
Alarm Notification	Specifies whether to notify users when alarms are triggered. Notifications can be sent by email, text message, or HTTP/HTTPS message.
Validity Period	Cloud Eye sends notifications only within the validity period specified in the alarm rule. If **Validity Period** is set to **08:00-20:00**, Cloud Eye sends notifications only within 08:00-20:00.
Notification Object	Specifies the object that receives alarm notifications. You can select the account contact or a topic. ● **Account contact** is the mobile phone number and email address of the registered account. ● A topic is used to publish messages and subscribe to notifications. If the required topic is unavailable, create one first and add subscriptions to it. For details, see **4.2.1 Creating a Topic** and **4.2.2 Adding Subscriptions**.
Trigger Condition	Specifies the condition for triggering the alarm notification. You can select **Generated alarm** (when an alarm is generated), **Cleared alarm** (when an alarm is cleared), or both.

d. Click **Create**.

After the alarm rule is created, if the metric data reaches the specified threshold, Cloud Eye immediately informs you that an exception has occurred.

4.4 Viewing the Alarm History

The alarm history displays the status changes of all alarm rules in the last 30 days.

When an alarm is generated, you can view the historical alarm details of the cloud resource.

Procedure

1. Log in to the management console.
2. Under **Management & Deployment**, select **Cloud Eye**.
3. Choose **Alarm Management** > **Alarm History**.

   On the **Alarm History** page, you can view the status changes of all alarm rules from the last 7 days.

NOTE

You can select a time range to search for the alarm history.

You can also view the alarm history by clicking **All resource types**, **All severities**, or **All statuses**.

4. Click the target alarm rule to go to the **Alarm Rules** page. In the lower part of the **Alarm History** area, you can view the history of the selected alarm rule from the last 30 days.

   In the alarm history list, you can check whether resources are abnormal and handle the exceptions, if any.

NOTE

- Typically, alarms are triggered based on calculation. Therefore, the alarm triggering time may be a few seconds later than the time the threshold was reached.
- If you have created or modified an alarm rule after obtaining the monitoring data and an alarm is triggered, the alarm triggering time is the time when you created or modified the alarm rule.

4.5 Alarm Rule Management

This topic describes how to manage alarm rules as your system grows.

4.5.1 Modifying an Alarm Rule

Procedure

1. Under **Management & Deployment**, select **Cloud Eye**.
2. Choose **Alarm Management** > **Alarm Rules**.
3. On the displayed **Alarm Rules** page, use either of the following two methods to modify an alarm rule:
   - Locate the row containing the alarm rule you want to modify, click **More** in the **Operation** column, and choose **Modify**.
   - Click the name of the alarm rule you want to modify. On the displayed page, click **Modify** in the upper right corner.
4. On the **Modify Alarm Rule** page, modify alarm rule parameters as needed.

Table 4-5 Parameters

Parameter	Description	Example Value
Name	Specifies the alarm rule name. The system generates a random name, which you can modify.	alarm-b6al
Description	(Optional) Provides supplementary information about the alarm rule.	N/A
Resource Type	Specifies the type of the resource the alarm rule is created for.	Elastic Cloud Server

Parameter	Description	Example Value
Dimension	Specifies the metric dimension of the selected resource type.	ECSs
Monitored Object	Specifies the resource the alarm rule is created for. You can specify one or more resources.	N/A
Monitored Object ID	Specifies the resource ID.	N/A
Metric	For example: ● CPU Usage Indicates the CPU usage of the monitored object in percent. ● Memory Usage Indicates the memory usage of the monitored object in percent.	CPU Usage
Alarm Policy	Specifies the policy for triggering an alarm. For example, an alarm is triggered if the average value of the monitored metric is 80% or more for three consecutive 5-minute periods.	N/A
Alarm Severity	Specifies the alarm severity, which can be **Critical**, **Major**, **Minor**, or **Informational**.	Major
Alarm Notification	Specifies whether to notify users by sending emails, or by sending HTTP/ HTTPS messages to servers.	N/A
Trigger Condition	Specifies the condition for triggering the alarm notification. You can select **Generated alarm** (when an alarm is generated), **Cleared alarm** (when an alarm is cleared), or both.	N/A

5. Click **OK**.

4.5.2 Disabling Alarm Rules

To disable a single alarm rule, go to the **Alarm Rules** page, locate the row containing the alarm rule you want to disable, and click **Disable** in the **Operation** column. In the displayed **Disable Alarm Rule** dialog box, click **OK**.

To disable multiple alarm rules, go to the **Alarm Rules** page, select multiple alarm rules, and click **Disable** in the upper left of the alarm rule list. In the displayed **Disable Alarm Rule** dialog box, click **OK**.

4.5.3 Enabling Alarm Rules

To enable a single alarm rule, go to the **Alarm Rules** page, locate the row containing the alarm rule you want to enable, and click **Enable** in the **Operation** column. In the displayed **Enable Alarm Rule** dialog box, click **OK**.

To enable multiple alarm rules, go to the **Alarm Rules** page, select multiple alarm rules, and click **Enable** in the upper left of the alarm rule list. In the displayed **Enable Alarm Rule** dialog box, click **OK**.

4.5.4 Deleting Alarm Rules

To delete a single alarm rule, go to the **Alarm Rules** page, locate the row containing the alarm rule you want to delete, click **More** in the **Operation** column, and choose **Delete**. In the displayed **Delete Alarm Rule** dialog box, click **OK**.

To delete multiple alarm rules, go to the **Alarm Rules** page, select multiple alarm rules, and click **Delete** in the upper left of the alarm rule list. In the displayed **Delete Alarm Rule** dialog box, click **OK**.

4.6 Alarm Templates

4.6.1 Viewing Alarm Templates

An alarm template contains a group of alarm rules for a specific service. You can use it to quickly create alarm rules for multiple resources of a cloud service. Cloud Eye recommends alarm templates based on the attributes of each cloud service. It also allows you to create custom templates as needed.

Procedure

1. Under **Management & Deployment**, select **Cloud Eye**.
2. Choose **Alarm Management** > **Alarm Templates**.

On the **Alarm Templates** page, you can create, view, modify, or delete custom templates.

4.6.2 Creating a Custom Template

1. On the **Alarm Templates** page, click **Create Custom Template**.
2. In the **Configure Template** step, specify the parameters listed in **Table 4-6**.

Table 4-6 Parameters

Parameter	Description
Resource Type	Specifies the type of the resource the alarm rule is created for. Example value: **Elastic Cloud Server**

Parameter	Description
Dimension	Specifies the metric dimension of the selected resource type. Example value: **ECSs**
Import Template	● Enable Select an existing template, then you can use or modify default alarm rules contained in the selected alarm template. ● Disable Manually add one or more alarm rules.

3. Click **Next** to go to the **Add Alarm Rule** step. Specify parameters listed in **Table 4-7**. You can add one or more rules to the alarm template.

Table 4-7 Parameters

Parameter	Description
Metric	For example: ● CPU Usage Indicates the CPU usage of the monitored object in percent. ● Memory Usage Indicates the memory usage of the monitored object in percent.
Alarm Policy	Specifies the policy for triggering an alarm. For example, an alarm is triggered if the average value of the monitored metric is 80% or more for three consecutive 5-minute periods.
Alarm Severity	Specifies the alarm severity, which can be **Critical**, **Major**, **Minor**, or **Informational**.
Operation	When the number of the alarm policies is two or more, you can delete alarm policies.

4. Click **Next** to go to the **Specify Template Details** step. Specify parameters listed in **Table 4-8**.

Table 4-8 Parameters

Parameter	Description
Name	Specifies the custom template name. The system generates a random name, which you can modify. Example value: **alarmTemplate-ku0x**

Parameter	Description
Description	(Optional) Provides supplementary information about the alarm template.

5. Click **Finish**.

4.6.3 Modifying a Custom Template

1. In the navigation pane on the left, choose **Alarm Management** > **Alarm Templates** and click **Custom Templates**. Locate the template you wan to modify and click **Modify** in the **Operation** column.
2. In the displayed **Modify Custom Template** dialog box, modify the parameter settings based on **Table 4-7** and click **Next**.
3. Specify the template name and description based on **Table 4-8**, and click **OK**.

4.6.4 Deleting a Custom Template

In the navigation pane on the left, choose **Alarm Management** > **Alarm Templates** and click **Custom Templates**. Locate the template you want to delete and click **Delete** in the **Operation** column. In the displayed **Delete Custom Template** dialog box, click **OK**.

5 Custom Monitoring

The **Custom Monitoring** page displays all custom metrics reported by you. You can use simple API requests to report collected monitoring data of those metrics to Cloud Eye for processing and display.

Viewing Custom Monitoring

1. Under **Management & Deployment**, select **Cloud Eye**.
2. In the navigation pane on the left, choose **Custom Monitoring**.
3. On the **Custom Monitoring** page, view the data reported by yourself through API requests, including custom services and metrics.

   NOTE

   - Only after you add monitoring data through APIs, will those data be displayed on the Cloud Eye console.
   - For details about how to add monitoring data, see "Adding Monitoring Data" in the *Cloud Eye API Reference*.
4. Locate the row that contains the cloud service resource to be viewed, and click **View Graph**.

   On the displayed page, you can view graphs based on raw data collected in **1h**, **3h**, and **12h**. In the upper right corner of each graph, the maximum and minimum values of the metric in the corresponding time periods are dynamically displayed.

Creating an Alarm Rule

1. Under **Management & Deployment**, select **Cloud Eye**.
2. In the navigation pane on the left, choose **Custom Monitoring**.
3. On the **Custom Monitoring** page, locate the target resource and click **Create Alarm Rule** in the **Operation** column.
4. On the **Create Alarm Rule** page, follow the prompts to set the parameters. For details, see **Table 4-2** and **Table 4-4**.
5. Click **Create**.

6 Services Interconnected with Cloud Eye

6.1 Computing

6.1.1 ECS Metrics

You do not need to install the Agent on an ECS to check basic monitoring metrics. The monitoring data is available in minutes after an ECS starts running.

Basic monitoring metric data is reported every 5 minutes.

ECS metrics vary depending on ECS OSs and types. For details, see **Table 6-1**. √ indicates that the metric is supported, and x indicates that the metric is not supported.

Table 6-1 Supported ECS metrics

Metric	Windows ECS		Linux ECS	
N/A	Xen	KVM	Xen	KVM
CPU Usage	√	√	√	√
Memory Usage	√	√	√ (VMTools must be installed on the image. Otherwise, this metric is unavailable.)	x (Not supported)
Disk Usage	√	√	√ (VMTools must be installed on the image. Otherwise, this metric is unavailable.)	x (Not supported)

Metric	Windows ECS		Linux ECS	
Disks Read Rate	√	√	√	√
Disks Write Rate	√	√	√	√
Disks Read Requests	√	√	√	√
Disks Write Requests	√	√	√	√
Inband Incoming Rate	√	√	√ (VMTools must be installed on the image. Otherwise, this metric is unavailable.)	x (Not supported)
Inband Outgoing Rate	√	√	√ (VMTools must be installed on the image. Otherwise, this metric is unavailable.)	x (Not supported)
Outband Incoming Rate	√	√	√	√
Outband Outgoing Rate	√	√	√	√
System Status Check Failed	√	×	√	×

NOTE

Certain ECS metrics require the installation of VMTools on the image, based on which the ECS is created. For instructions about how to install VMTools, see **https://github.com/UVP-Tools/UVP-Tools/**.

Table 6-2 describes these ECS metrics.

Table 6-2 Metric description

Metric	Parameter	Description	Value Range	Monitored Object	Monitoring Interval (Raw Metrics and KVM Only)
cpu_util	CPU Usage	CPU usage of an ECS Unit: Percent Formula: CPU usage of an ECS/Number of vCPUs in the ECS	≥ 0	ECS	5 minutes
mem_util	Memory Usage	Memory usage of an ECS This metric is unavailable if the image has no VMTools installed. Unit: Percent Formula: Used memory of an ECS/ Total memory of the ECS	≥ 0	ECS	5 minutes
disk_util_inband	Disk Usage	Disk usage of an ECS This metric is unavailable if the image has no VMTools installed. Unit: Percent Formula: Used capacity of an ECS disk/Total capacity of the ECS disk	≥ 0	ECS	5 minutes
disk_read_bytes_rate	Disk Read Bandwidth	Number of bytes read from an ECS disk per second Unit: byte/s Formula: Total number of bytes read from an ECS disk/ Monitoring interval byte_out = (rd_bytes - last_rd_bytes)/Time difference	≥ 0	ECS	5 minutes

Metric	Parameter	Description	Value Range	Monitored Object	Monitoring Interval (Raw Metrics and KVM Only)
disk_write_bytes_rate	Disk Write Bandwidth	Number of bytes written to an ECS disk per second Unit: byte/s Formula: Total number of bytes written to an ECS disk/Monitoring interval	≥ 0	ECS	5 minutes
disk_read_requests_rate	Disk Read IOPS	Number of read requests sent to an ECS disk per second Unit: request/s Formula: Total number of read requests sent to an ECS disk/Monitoring interval req_out = (rd_req - last_rd_req)/Time difference	≥ 0	ECS	5 minutes
disk_write_requests_rate	Disk Write IOPS	Number of write requests sent to an ECS disk per second Unit: request/s Formula: Total number of write requests sent to an ECS disk/Monitoring interval req_in = (wr_req - last_wr_req)/Time difference	≥ 0	ECS	5 minutes

Metric	Parameter	Description	Value Range	Monitored Object	Monitoring Interval (Raw Metrics and KVM Only)
network_incoming_bytes_rate_inband	Inband Incoming Rate	Number of incoming bytes on an ECS per second Unit: byte/s Formula: Total number of inband incoming bytes on an ECS/Monitoring interval	≥ 0	ECS	5 minutes
network_outgoing_bytes_rate_inband	Inband Outgoing Rate	Number of outgoing bytes on an ECS per second Unit: byte/s Formula: Total number of inband outgoing bytes on an ECS/Monitoring interval	≥ 0	ECS	5 minutes
network_incoming_bytes_aggregate_rate	Outband Incoming Rate	Number of incoming bytes on an ECS per second on the hypervisor Unit: byte/s Formula: Total number of outband incoming bytes on an ECS/Monitoring interval This metric is unavailable if SR-IOV is enabled.	≥ 0	ECS	5 minutes

Metric	Parameter	Description	Value Range	Monitored Object	Monitoring Interval (Raw Metrics and KVM Only)
network_outgoing_bytes_aggregate_rate	Outband Outgoing Rate	Number of outgoing bytes on an ECS per second on the hypervisor Unit: byte/s Formula: Total number of outband outgoing bytes on an ECS/Monitoring interval This metric is unavailable if SR-IOV is enabled.	≥ 0	ECS	5 minutes

Metric	Parameter	Description	Value Range	Monitored Object	Monitoring Interval (Raw Metrics and KVM Only)
inst_sys_status_error	System Status Check Failed	Status of the cloud platform for running ECSs, which can be **0** or **1** ● **0**: The system is running properly. All check items are normal. ● **1**: The system is not running properly. At least one check item failed. When the power source of the physical server fails or the hardware/ software becomes faulty, the check result is **1**. The system periodically checks the status and returns check results using value **0** or **1**. ● If the detected fault does not affect ECS functions, certain management operations performed on the ECS, such as starting, stopping, or specifications modifications, may be affected. ● If the detected fault affects ECS functions, such as a server power supply failure, the system will	**0** or **1**	ECS	5 minutes

Metric	Parameter	Description	Value Range	Monitored Object	Monitoring Interval (Raw Metrics and KVM Only)
		recover the ECS as soon as possible.			

6.1.2 AS Metrics

This section describes the monitoring metrics reported by AS to Cloud Eye and defines the namespace for the metrics. You can use Cloud Eye to query metrics and alarms generated by AS.

Table 6-3 AS metrics

Metric ID	Metric	Description	Value Range	Monitored Object & Dimension	Monitoring Interval (Raw Data)
cpu_util	CPU Usage	CPU usage of an AS group Formula: Total CPU usage of all ECSs in an AS group/Number of ECSs in the AS group Unit: Percent	≥0%	Object: AS group Dimension: AutoScalingGroup	5 minutes
mem_util	Memory Usage	Memory usage of an AS group Formula: Total memory usage of all ECSs in an AS group/Number of ECSs in the AS group Unit: Percent **NOTE** This metric is unavailable if the image has no VM Tools installed.	≥0%	Object: AS group Dimension: AutoScalingGroup	5 minutes

Metric ID	Metric	Description	Value Range	Monitored Object & Dimension	Monitoring Interval (Raw Data)
network_outgoing_bytes_rate_inband	Inband Incoming Rate	Number of incoming bytes per second on an ECS in an AS group Formula: Total inband incoming rates of all ECSs in an AS group/ Number of ECSs in the AS group Unit: Byte/s	≥0 Byte/s	Object: AS group Dimension: AutoScalingGroup	5 minutes
instance_num	Inband Outgoing Rate	Number of outgoing bytes per second on an ECS in an AS group Formula: Total inband outgoing rates of all ECSs in an AS group/ Number of ECSs in the AS group Unit: Byte/s	≥0	Object: AS group Dimension: AutoScalingGroup	5 minutes
disk_read_bytes_rate	Disks Read Rate	Number of bytes read from an AS group per second Formula: Total disks read rates of all ECSs in an AS group/Number of ECSs in the AS group Unit: Byte/s	≥0 Byte/s	Object: AS group Dimension: AutoScalingGroup	5 minutes
disk_write_bytes_rate	Disks Write Rate	Number of bytes written to an AS group per second Formula: Total disks write rates of all ECSs in an AS group/Number of ECSs in the AS group Unit: Byte/s	≥0 Byte/s	Object: AS group Dimension: AutoScalingGroup	5 minutes

Metric ID	Metric	Description	Value Range	Monitored Object & Dimension	Monitoring Interval (Raw Data)
disk_read_requests_rate	Disks Read Requests	Number of read requests per second sent to an ECS disk in an AS group Formula: Total disks read rates of all ECSs in an AS group/Number of ECSs in the AS group Unit: Request/s	≥0 request/s	Object: AS group Dimension: AutoScalingGroup	5 minutes
disk_write_requests_rate	Disks Write Requests	Number of write requests per second sent to an ECS disk in an AS group Formula: Total disks write rates of all ECSs in an AS group/Number of ECSs in the AS group Unit: Request/s	≥0 request/s	Object: AS group Dimension: AutoScalingGroup	5 minutes

NOTE

For details about whether your OS supports the **Memory Usage**, **Inband Outgoing Rate**, and **Inband Incoming Rate** metrics, see 6.1.1 ECS Metrics.

6.2 Storage

6.2.1 EVS Metrics

Metric ID	Metric Name	Meaning	Value Range	Monitored Object	Monitoring Period (Raw Data)
disk_device_read_bytes_rate	Disk Read Rate	Number of bytes read from the monitored disk per second Unit: Bytes/s	≥ 0 bytes/s	EVS disk	5 minutes

Metric ID	Metric Name	Meaning	Value Range	Monitored Object	Monitoring Period (Raw Data)
disk_device_write_bytes_rate	Disk Write Rate	Number of bytes written to the monitored disk per second Unit: Bytes/s	≥ 0 bytes/s	EVS disk	5 minutes
disk_device_read_requests_rate	Disk Read Requests	Number of read requests sent to the monitored disk per second Unit: Requests/s	≥ 0 Requests/s	EVS disk	5 minutes
disk_device_write_requests_rate	Disk Write Requests	Number of write requests sent to the monitored disk per second Unit: Requests/s	≥ 0 Requests/s	EVS disk	5 minutes

6.2.2 SFS Metrics

Table 6-4 SFS metrics

Metric ID	Metric	Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
read_bandwidth	Read Bandwidth	Read bandwidth of the file system within a monitoring period Unit: byte/s	≥ 0 bytes/s	File sharing	4 minutes
write_bandwidth	Write Bandwidth	Write bandwidth of the file system within a monitoring period Unit: byte/s	≥ 0 bytes/s	File sharing	4 minutes
rw_bandwidth	Read Write Bandwidth	Read and write bandwidth of the file system within a monitoring period Unit: byte/s	≥ 0 bytes/s	File sharing	4 minutes

6.3 Network

6.3.1 EIP and Bandwidth Metrics

Table 6-5 EIP and Bandwidth metrics

Metric ID	Metric	Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
downstream_bandwidth	Upstream Bandwidth	Outbound network rate of the monitored object	≥ 0 bits/s	Bandwidth or EIP	1 minute
upstream_bandwidth_usage	Downstream Bandwidth	Inbound network rate of the monitored object	≥ 0 bits/s	Bandwidth or EIP	1 minute

6.3.2 ELB Metrics

Classic Load Balancer Metrics

Metric ID	Metric	Description	Monitored Object & Dimension	Monitoring Period (Raw Data)
m1_cps	Concurrent Connections	Number of TCP and UDP connections between the monitored object and backend servers Unit: Count	Monitored object: classic load balancer Dimension: lb_instance_id	1 minute
m2_act_conn	Active Connections	Number of TCP or UDP connections in the **ESTABLISHED** state between the monitored object and backend servers You can run the following command to view the connections (both Windows and Linux servers): Unit: Count		1 minute

Metric ID	Metric	Description	Monitored Object & Dimension	Monitoring Period (Raw Data)
m3_inact_conn	Inactive Connections	Number of TCP connections between the monitored object and backend servers except those in the **ESTABLISHED** state You can run the following command to view the connections (both Windows and Linux servers): Unit: Count		1 minute
m4_ncps	New Connections	Number of TCP and UDP connections established between clients and the monitored object per second Unit: Count/s		1 minute
m5_in_pps	Incoming Packets	Number of packets received by the monitored object per second Unit: Packet/s		1 minute
m6_out_pps	Outgoing Packets	Number of packets sent from the monitored object per second Unit: Packet/s		1 minute
m7_in_Bps	Inbound Rate	Traffic used for accessing the monitored object from the Internet Unit: byte/s		1 minute
m8_out_Bps	Outbound Rate	Traffic used by the monitored object to access the Internet Unit: byte/s		1 minute
m9_abnormal_servers	Unhealthy Servers	Number of unhealthy backend servers associated with the monitored object Unit: Count		1 minute
ma_normal_servers	Healthy Servers	Number of healthy backend servers associated with the monitored object Unit: Count		1 minute

Metrics of Shared Load Balancers and Shared Load Balancer Listeners

Metric ID	Metric	Description	Monitored Object & Dimension	Monitoring Period (Raw Data)
m1_cps	Concurrent Connections	Number of TCP and UDP connections between the monitored object and backend servers Unit: Count	Monitored object: shared load balancer and shared load balancer listener Dimensions [a]: lbaas_instance_id and lbaas_listener_id	1 minute
m2_act_conn	Active Connections	Number of TCP or UDP connections in the **ESTABLISHED** state between the monitored object and backend servers You can run the following command to view the connections (both Windows and Linux servers): Unit: Count		1 minute
m3_inact_conn	Inactive Connections	Number of TCP connections between the monitored object and backend servers except those in the **ESTABLISHED** state You can run the following command to view the connections (both Windows and Linux servers): Unit: Count		1 minute
m4_ncps	New Connections	Number of TCP and UDP connections established between clients and the monitored object per second Unit: Count/s		1 minute
m5_in_pps	Incoming Packets	Number of packets received by the monitored object per second Unit: Packet/s		1 minute
m6_out_pps	Outgoing Packets	Number of data packets sent from the monitored object per second Unit: Packet/s		1 minute
m7_in_Bps	Inbound Rate	Traffic used for accessing the monitored object from the Internet Unit: byte/s		1 minute
m8_out_Bps	Outbound Rate	Traffic used by the monitored object to access the Internet Unit: byte/s		1 minute

Metric ID	Metric	Description	Monitored Object & Dimension	Monitoring Period (Raw Data)
m9_abnormal_servers	Unhealthy Servers	Number of unhealthy backend servers associated with the monitored object Unit: Count		1 minute
ma_normal_servers	Healthy Servers	Number of healthy backend servers associated with the monitored object Unit: Count		1 minute

a: If a service has multiple dimensions, all dimensions are mandatory when you use APIs to query the metrics.

- Example of querying a single metric from both dimensions: dim.0=lbaas_instance_id,223e9eed-2b02-4ed2-a126-7e806a6fee1f&dim.1=lbaas_listener_id,3baa7335-8886-4867-8481-7cbba967a917
- Example of querying metrics in batches from both dimensions:

```
"dimensions": [
{
"name": "lbaas_instance_id",
"value": "223e9eed-2b02-4ed2-a126-7e806a6fee1f"
}
{
"name": "lbaas_listener_id",
"value": "3baa7335-8886-4867-8481-7cbba967a917"
}
],
```

7 FAQs

7.1 Product Consultation

7.1.1 What Is Rollup?

Rollup is a process where Cloud Eye calculates the maximum, minimum, average, sum, or variance value of raw data sampled for different periods and repeats the process for each subsequent period. A calculation period is called a rollup period.

The rollup process involves the smoothing of data sets. Set a longer rollup period if you want more smoothing to be performed. If more smoothing is performed, the generated data will be more accurate, enabling you to more accurately predict trends. Set a shorter rollup period if you want more accurate alarm reporting.

The rollup period can be 5 minutes, 20 minutes, 1 hour, 4 hours, or 1 day.

During the rollup, Cloud Eye processes data sampled based on the data type.

- If the data sampled is integers, Cloud Eye rounds off the rollup results.
- If the data includes decimal values (floating point number), Cloud Eye truncates the data after the second decimal place.

For example, if the instance quantity in Auto Scaling is an integer value, the rollup period is 5 minutes, and the current time is 10:35, Cloud Eye rolls up the raw data generated between 10:30 and 10:35 to the time point of 10:30. If the sampled metrics are 1 and 4 respectively, after rollup, the maximum value is 4, the minimum value is 1, and the average value is [(1 + 4)/2] = 2, instead of 2.5.

Choose whichever rollup method best meets your service requirements.

7.1.2 How Long Is Metric Data Retained?

Metric data includes raw data and rolled-up data.

- Raw data is retained for two days.
- Rolled-up data is data aggregated based on raw data. The retention period for rolled-up data depends on the rollup period.

Table 7-1 Retention periods for rolled-up data

Rollup Period	Retention Period
5 minutes	10 days
20 minutes	20 days
1 hour	155 days
4 hours	300 days
1 day	5 years

If an instance is disabled, stopped, or deleted, its metrics will be deleted one hour after the raw data reporting of those metrics stops. When the instance is enabled or restarted, raw data reporting of its metrics will resume. If the instance has been disabled or stopped for less than two days or for less time than the previous rolled-up data retention period, you can view the historical data of its metrics generated before these metrics were deleted.

7.1.3 How Many Rollup Methods Does Cloud Eye Support?

Cloud Eye supports the following rollup methods:

- Average

  If **Avg.** is selected for **Statistic**, Cloud Eye calculates the average value of metrics collected within a rollup period.
- Maximum

  If **Max.** is selected for **Statistic**, Cloud Eye calculates the maximum value of metrics collected within a rollup period.
- Minimum

  If **Min.** is selected for **Statistic**, Cloud Eye calculates the minimum value of metrics collected within a rollup period.
- Sum

  If **Sum** is selected for **Statistic**, Cloud Eye calculates the sum of metrics collected within a rollup period.
- Variance

  If **Variance** is selected for **Statistic**, Cloud Eye calculates the variance value of metrics collected within a rollup period.

NOTE

Take a 5-minute period as an example. If it is 10:35 now and the rollup period starts at 10:30, the raw data generated between 10:30 and 10:35 is rolled up.

7.1.4 How Can I Export Collected Data?

1. On the Cloud Eye console, choose **Cloud Service Monitoring** or **Server Monitoring**.
2. Click **Export Data**.

3. Set the time range, resource type, dimension, monitored object, and metric.
4. Click **Export**.

- The first row in the exported monitoring report displays the username, region, service, instance name, instance ID, metric name, metric data, time, and timestamp.
- To convert the time using a Unix timestamp to the time of the target time zone, perform the following steps:
  a. Use Excel to open a .csv file.
  b. Use the following formula to convert the time:

     Target time = [Unix timestamp/1000 + (Target time zone) x 3600]/86400 + 70 x 365 + 19

  c. Set cell format to **Date**.

     To convert a Unix timestamp of 1475918112000 to Shanghai time (UTC +8), using the formula from step b:

     Target time = [1475918112000/1000 + (+8) x 3600]/86400 + 70 x 365 + 19

     Set the cell format to date and select a presentation format such as 2016/3/14 13:30. Then, the target time obtained will be presented as 2016/10/8 17:15.

7.2 Alarm Notification and False Alarm

7.2.1 What Is an Alarm Notification? How Many Types of Alarm Notifications Are There? How Can I Configure an Alarm Notification?

Alarm notifications are email or SMS messages that are sent out when an alarm status is **Alarm**.

You can configure Cloud Eye to send or not send alarm notifications when you create or modify an alarm rule.

Cloud Eye can:

- Send you email notifications, or send HTTP/HTTPS messages to servers.
- Work with Auto Scaling to trigger the system to automatically add or remove servers.

7.2.2 What Alarm Status Does Cloud Eye Support?

There are three Cloud Eye alarm statuses: **Alarm**, **OK**, and **Insufficient data**. If an alarm rule is disabled, its status is considered as invalid, and **Disabled** is displayed.

- **Alarm**: The monitoring data meets the preset alarm policy.
- **OK**: The monitoring data is reported but does not meet the preset alarm policy.

- **Insufficient data**: No monitoring data has been reported for three consecutive hours, and this is generally because the instance has been deleted or is abnormal.

7.2.3 What Alarm Severities Does Cloud Eye Support?

There are four levels of alarm severity: critical, major, minor, and informational.

- **Critical**: An emergency fault has occurred and services are affected.
- **Major**: A relatively serious problem has occurred and may hinder the use of resources.
- **Minor**: A less serious problem has occurred but will not hinder the use of resources.
- **Informational**: A potential error exists and may affect services.

7.3 Abnormal Monitoring Data

7.3.1 Why Is the Monitoring Data Not Displayed on the Cloud Eye Console?

Possible causes are as follows:

- The service is not interconnected with Cloud Eye. To check whether a service has been interconnected with Cloud Eye, see Services Interconnected with Cloud Eye.
- The service has been interconnected with Cloud Eye. However, the collection and monitoring frequency for each service varies. The data may have just not been collected yet.
- The ECS or BMS has been stopped for more than 1 hour.
- The EVS disk has not been attached to an ECS or BMS.
- No backend server is bound to the elastic load balancer or all of the backend servers are shut down.
- It has been less than 10 minutes since the resource was created.

7.3.2 Why Are the Network Traffic Metric Values in Cloud Eye Different from Those Detected in ECS?

Because the sampling period in Cloud Eye is different from that of the metric monitoring tool in ECS.

Cloud Eye collects ECS and EVS disk data every 4 minutes (5 minutes for KVM ECSs). In contrast, the metric monitoring tool in ECS collects data every second.

The larger the sampling period, the greater the data distortion in the short term. Cloud Eye is more suitable for long-term monitoring for websites and applications running on ECSs.

Furthermore, to improve reliability, you can configure alarm thresholds to enable Cloud Eye to generate alarms where there are resource exceptions or insufficiencies.

7.3.3 What Are the Impacts on ECS Metrics If VM Tools Are Not Installed on ECSs?

If VM Tools are not installed on your ECSs, Cloud Eye can still monitor the outband incoming rate and outband outgoing rate. However, it cannot monitor memory usage, disk usage, inband incoming rate, or inband outgoing rate, which reduces the CPU monitoring accuracy.

For details about ECS metrics supported by Cloud Eye, see **Basic ECS Metrics**.

A Change History

Released On	Description
2020-03-24	This release incorporates the following changes: Added Event Monitoring.
2019-08-31	This release incorporates the following changes: Added Server Monitoring and related FAQs.
2018-09-30	This release incorporates the following changes: Optimized the **Create Alarm Rule** window.
2018-06-30	This release incorporates the following changes: ● Users can sort graphs by dragging them. ● Users can view graphs directly from the alarm rule list on the **Alarm Rules** page. ● Added the automatic refresh function to both standard and expanded graphs.
2018-05-30	This release incorporates the following changes: ● Added the auto refresh button to the monitoring panels. ● Added metrics for the enhanced load balancer and enhanced load balancer listener.
2018-04-30	This release incorporates the following changes: ● Interconnected with Document Database Service (DDS). ● Added Relational Database Service (RDS) metrics. ● Interconnected with NAT Gateway. ● Optimized the strings for alarm rule creation.

Released On	Description
2018-03-30	This release incorporates the following changes: ● Added the **Alarm History** page. ● Optimized the monitoring data export function, in which users can select the time for the data to be exported.
2018-02-28	This release incorporates the following changes: Updated Virtual Private Cloud (VPC) metrics.
2018-01-30	This release incorporates the following changes: Launched the **Custom Monitoring** function.
2017-11-30	This release incorporates the following changes: ● Interconnected with Machine Learning Service (MLS). ● Added Auto Scaling (AS) metrics.
2017-10-30	This release incorporates the following changes: ● Added Scalable File Service (SFS) metrics. ● Added Relational Database Service (RDS) metrics.
2017-09-30	This release incorporates the following changes: ● Added the **Custom Alarm Templates** function. ● Added **Monitoring Overview**.
2017-08-30	This release incorporates the following changes: ● Added the alarm template. ● Updated the process of adding alarm rules.
2017-07-30	This release incorporates the following changes: ● Deleted an Elastic Cloud Server (ECS) metric that can recover ECSs. ● Added an FAQ: Under What Circumstances Will an Alarm Rule Trigger "Insufficient data"?
2017-06-30	This release incorporates the following change: Optimized the **Instance Monitoring** page and supported tiled display of multiple metrics.
2017-05-26	This release incorporates the following changes: ● Added **Metric Quantity** description. ● Added **Sum.** as a rollup method.
2017-04-28	This release incorporates the following changes: Added an Elastic Cloud Server (ECS) metric that can recover ECSs.

Released On	Description
2017-02-27	This release incorporates the following changes: ● Added the operation of creating a monitoring panel. ● Added the Cloud Eye data rollup mechanism.
2017-01-19	This release incorporates the following changes: Added the rollup methods supported by Cloud Eye.
2016-12-30	This issue is the first official release.