Cloud Eye

User Guide

Issue	01
Date	2024-04-03

HUAWEI TECHNOLOGIES CO., LTD.

Copyright © Huawei Technologies Co., Ltd. 2024. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Technologies Co., Ltd.

Trademarks and Permissions

HUAWEI and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.
All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Huawei Technologies Co., Ltd.

Address: Huawei Industrial Base
Bantian, Longgang
Shenzhen 518129
People's Republic of China

Website: https://www.huawei.com

Email: support@huawei.com

Security Declaration

Vulnerability

Huawei's regulations on product vulnerability management are subject to the *Vul. Response Process.* For details about this process, visit the following web page:
https://www.huawei.com/en/psirt/vul-response-process
For vulnerability information, enterprise customers can visit the following web page:
https://securitybulletin.huawei.com/enterprise/en/security-advisory

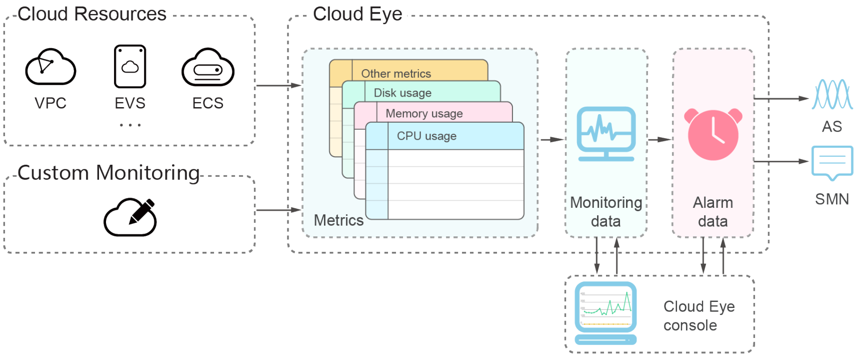
Contents

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 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.

- Server monitoring

  After you install the Agent (Telescope) on an ECS and Bare Metal Server (BMS), you can collect ECS and BMS monitoring data at a granularity of 60 seconds in real time. Cloud Eye provides 40 metrics, such as CPU, memory, and disk metrics. For details, see **6.1 Introduction to Server Monitoring**.

- 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.

- Real-time notification

  You can enable **Alarm Notification** when creating alarm rules. When the cloud service status changes and metrics reach the thresholds specified in alarm rules, 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.

- Dashboard

  A dashboard 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.

- Resource group

  A resource group allows you to add and monitor correlated resources and provides a collective health status for all resources that it contains.

1.2 Advantages

Automatic Provisioning

Cloud Eye is automatically provisioned for all users. You can use the Cloud Eye console or APIs to view cloud service statuses and set alarm rules.

Reliable Real-time 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.

Visualized Monitoring

You can create dashboards and graphs to compare multiple metrics. The graphs are refreshed automatically to always display the latest data.

Multiple Notification Types

You can enable **Alarm Notification** when creating alarm rules. When the metric reaches the threshold specified in an alarm rule, Cloud Eye notifies you by emails, or by sending HTTP/HTTPS messages to an IP address of your choice, allowing you to keep track of the statuses of cloud services and 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 cloud service status and metric data, and create alarm rules for metrics on the Cloud Eye console.

Server Monitoring

By monitoring the ECS or BMS metrics, such as CPU usage, memory usage, and disk usage, you can ensure that the ECS or BMS runs normally and prevent service interruptions caused by overuse of resources.

Performance Issues

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

Capacity Expansion

After you create alarm rules for metrics such as CPU usage, memory usage, and disk usage, you can track the statuses of cloud services. If the service volume increases, Cloud Eye sends you an alarm notification, enabling you to manually expand the capacity or configure AS policies 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.

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 Basic Concepts

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

- **Metrics**
- **Rollup**
- **Dashboards**

- 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 certain amount of monitoring data over time. It helps you understand the changes over a specific period.

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.

Dashboards

Dashboards allow you to view monitoring data of metrics of different services and dimensions. You can use dashboards to display metrics of key services in a centralized way, get an overview of the service 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 cloud service status in a timely manner.

Alarm Rules

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

1.5 Constraints

Table 1-1 lists Cloud Eye resource limits for a user. For details about how to adjust quotas, see **12 Quota Adjustment**.

Table 1-1 Resources and their default quotas

Resource	Default Quota
Alarm rules that can be created	100
Custom alarm templates that can be created	50
Alarm rules that can be added to an alarm template	20
Dashboards that can be created	20
Graphs that can be added to a dashboard	24
Objects that can be selected for monitoring when creating an alarm rule	50
Alarm rules that can be created at a time	1,000 **NOTE** If you select 50 monitored objects and 20 metrics, the number of alarm rules that can be created is 1,000.
Topics that can be selected for receiving notifications	5
Monitoring data records that can be exported at a time	400 **NOTE** If 400 monitored objects are to be exported, only records of one metric can be exported. If 80 monitored objects are to be exported, records of 5 metrics can be exported.

1.6 Region and AZ

Concept

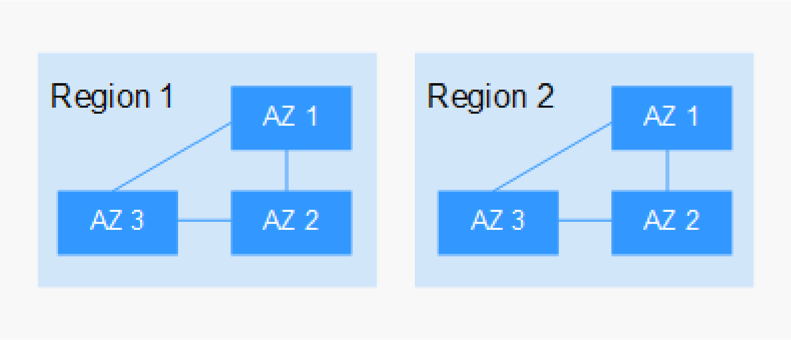
A region and availability zone (AZ) identify the location of a data center. You can create resources in a specific region and AZ.

- 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 Viewing the Overview

The **Overview** page provides the following modules, helping you track the resource usage and alarms in real time.

Resource Overview

Displays the total number of monitored cloud service resources and alarms generated for these resources in the current account.

Alarm Statistics

Displays the alarm trend for the last seven days and the number of alarms of each severity.

After you click an alarm severity, the **Alarm Rules** page is displayed, showing all alarm rules of the severity.

NOTE

On the **Alarm Rules** page, click **View Resource** in the **Operation** column. On the displayed window, you can copy the resource ID and go to the corresponding cloud service console to search for the specific resource.

ECS Monitoring

Displays the CPU usages of all monitored ECSs and a list of the top 5 ECSs, ranked by their CPU usage over the last 5 minutes.

Clicking an ECS takes you to the corresponding **Basic Monitoring** page.

Network Monitoring

Displays the outbound bandwidth and inbound bandwidth of the current EIP and bandwidth in the last 1 hour.

- Inbound bandwidth: indicates the network rate of inbound traffic.

- Outbound bandwidth: indicates the network rate of outbound traffic.

Storage Monitoring

Displays usages of all EVS disks in the last five minutes by listing the total read and write bandwidth in addition to the total quantity of read and write IOPS.

Full Screen

You can view various information, such as alarm statistics, event monitoring, and ECS monitoring on a full screen.

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 track the cloud service status by monitoring these metrics.

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

Procedure

1. Log in to the management console.
2. Click **Service List** in the upper left corner, and select **Cloud Eye**.
3. In the navigation pane on the left, choose **Cloud Service Monitoring**, and select a cloud service.

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

   The detailed monitoring page is displayed.

   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.

   NOTE

   - Metric units can be changed between byte or byte/s and GB or GB/s on graphs. When you are changing the unit, if the maximum value of a metric is smaller than 10^ (-5), both the maximum value and the minimum value of this metric are 0. In addition, all data displayed on the graph is 0.
   - If **Auto Refresh** is enabled, data is automatically refreshed every minute.
   - You can search for a specific metric in the search box.
   - Some cloud services allow you to view resource details. You can click **View Resource Details** in the upper part of the page to view details about monitored resources.
5. 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. Near the top left corner of the page, you can click **Settings** to change the rollup period of the monitoring data. For details about the rollup period, see **14.1.1 What Is Rollup?**.
- If you select **7d** or **30d**, aggregated data is displayed by default. Near the top left corner of the page, you can click **Settings** to change the rollup period of the monitoring data.

6. In the upper right corner of the monitoring view, click + to create an alarm rule for a metric.
7. To export data, click **Export Data** on the **Cloud Service Monitoring** page, configure parameters as prompted, and click **Export**. For details, see **14.1.4 How Can I Export Collected Data?**

2.3 Using Server Monitoring

Server monitoring includes basic monitoring, process monitoring, and OS monitoring for servers.

- Basic monitoring provides Agent-free monitoring for basic ECS or BMS metrics.
- OS monitoring provides proactive and fine-grained OS monitoring for servers, and it requires the Agent (a plug-in) to be installed on all servers that will be monitored.
- Process monitoring provides monitoring of active processes on hosts.

NOTE

Agent access statement: After the Agent is installed, it collects and reports server monitoring data to the Cloud Eye service. When you update the Agent software package, Cloud Eye accesses the software package repository address to update the software. In addition to the preceding behaviors, the Agent does not access any other addresses.

Functions

- Various Metrics

  Server monitoring provides more than 40 metrics, such as metrics for CPU, memory, disk, and network usage, meeting the basic monitoring and O&M requirements for servers.
- Fine-grained Monitoring

  After the Agent is installed, the metrics collected by the Agent are reported every minute.
- Process Monitoring

  CPU usage, memory usage, and number of opened files used by active processes are monitored to help you better understand the resource usages on ECSs and BMSs.

Using Server Monitoring

1. Log in to the management console.
2. Click **Service List** in the upper left corner, and select **Cloud Eye**.
3. In the navigation pane on the left, choose **Server Monitoring**.
4. Select the target ECS or BMS and install the Agent on it.
   a. Change the DNS server address of and add security group rules to the target ECS or BMS. For details, see **Modifying the DNS Server Address and Adding Security Group Rules (Linux)** or **Modifying the DNS Server Address and Adding Security Group Rules (Windows)**.
   b. Install the Agent. For details, see **Installing the Agent on a Linux Server** or **Installing and Configuring the Agent on a Windows Server**.
5. After 5 minutes, check whether the Agent status is **Running**.

   If yes, the Agent has been installed successfully.

   On the right of the ECS, click **View Metric** in the **Operation** column to view the monitoring data.

2.4 Using Custom Monitoring

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

For details about how to add monitoring data, see **Adding Monitoring Data**.

Viewing Custom Monitoring

1. Log in to the management console.
2. Click **Service List** in the upper left corner, and select **Cloud Eye**.
3. In the navigation pane on the left, choose **Custom Monitoring**.
4. On the **Custom Monitoring** page, view the data reported by yourself through API requests, including custom services and metrics.
5. Locate the row that contains the target cloud service resource and click **View Metric** in the **Operation** column.

   On the page displayed, 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.
6. If you want to view metric details, hover your mouse over a graph and click ⤡ in the upper right corner.

   In the upper left corner, you can see six default monitoring periods: **1h**, **3h**, **12h**, **1d**, **7d**, and **30d**. To view historical monitoring data for any period during the last six months, customize the monitoring period by setting **Select Range** in the upper right corner.

   In the upper left corner of the graph, click **Settings** to configure the rollup method.

Creating an Alarm Rule

1. Log in to the management console.
2. Click **Service List** in the upper left corner, and select **Cloud Eye**.
3. In the navigation pane on the left, choose **Custom Monitoring**.
4. Locate the target cloud service resource and click **Create Alarm Rule** in the **Operation** column.
5. Configure the alarm rule name, alarm policy, and alarm notification as prompted.

   After you create the alarm rule, if the custom metric data reaches the threshold, Cloud Eye immediately notifies you through SMN that an exception has occurred.

2.5 Using Event Monitoring

You can query system events 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.

Events are key operations on cloud service resources that are stored and monitored by Cloud Eye. You can view events to see operations performed by specific users on specific resources, such as deleting or rebooting an ECS.

Event monitoring is enabled by default. You can view monitoring details about system events and custom events. For details about the supported system events, see **Events Supported by Event Monitoring**.

Event monitoring provides an API for reporting custom events, which helps you collect and report abnormal events or important change events generated by services to Cloud Eye. For details about how to report custom events, see **Reporting Events**.

The differences between monitoring of custom events and **custom monitoring** are as follows:

- Monitoring of custom events is used to report and query monitoring data for non-consecutive events, and generate alarms in these scenarios.
- Custom monitoring is used to report and query periodically and continuously collected monitoring data, and generate alarms in these scenarios.

Viewing Event Monitoring Graphs

1. Log in to the management console.
2. Click **Service List** in the upper left corner, and select **Cloud Eye**.
3. In the navigation pane on the left, choose **Event Monitoring**.

   On the page displayed, all system events and custom events of the last 24 hours are displayed by default.
4. Select an event and click **View Graph** in the **Operation** column.

Creating an Alarm Rule

1. Log in to the management console.
2. Click **Service List** in the upper left corner, and select **Cloud Eye**.
3. In the navigation pane on the left, choose **Event Monitoring**.
4. In the event list, locate the event and click **Create Alarm Rule** in the **Operation** column.
5. Configure the alarm rule name, alarm policy, and alarm notification as prompted.

   After you create the alarm rule, if the metric data reaches the threshold, Cloud Eye immediately notifies you through SMN that an exception has occurred.

2.6 Using Resource Groups

Scenarios

- Resource Management

  If you use multiple cloud services, you can add all related resources, such as ECSs, BMSs, EVS disks, elastic IP addresses, bandwidths, and databases to the same resource group for easier management and O&M.
- Routine Inspection and Quick Fault Locating

  On the details page of a resource group, you can view the resource overview, unhealthy resources, alarm rules, and alarm records. This feature helps you view cloud resource usage and quickly locate faulty resources.

Functions

- Resource groups enable you to manage your cloud resources across products.
- The unhealthy resource list enables you to quickly locate faults.
- The alarm records help you track the overall service status.

Using Resource Groups

1. Log in to the management console.
2. Click **Service List** in the upper left corner, and select **Cloud Eye**.
3. In the navigation pane on the left, choose **Resource Groups**.
4. In the upper right corner, click **Create Resource Group**. On the page displayed, enter a group name as prompted.
5. Select the target cloud service resources.
6. Click **Create**.

   For details about how to create and manage resource groups, see **4.1 Introduction to Resource Groups**.

2.7 Creating an Alarm Rule

Scenarios

The alarm function provides the alarm service for monitoring data. By creating alarm rules, you define how the alarm system checks monitoring data and sends alarm notifications when metric data meets alarm policies.

After creating alarm rules for important metrics, you can timely know metric data exceptions and quickly rectify the faults.

Functions

- Alarm rules can be created for all monitoring items on Cloud Eye.
- Alarm rules can be created for all resources, resource groups, log monitoring, custom monitoring, event monitoring, and website monitoring.
- You can set validity periods of alarm rules, that is, customize the time when alarm rules take effect.
- Notifications can be sent by email, text message, or HTTP/HTTPS message.

Procedure

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

Table 2-1 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 configure alarm content parameters.

Table 2-2 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
Group	This parameter is mandatory when **Monitoring Scope** is set to **Resource groups**.	N/A
Method	There are two options: **Use template** or **Configure manually**.	Configure manually
Template	Specifies the template to be used. You can select a default alarm template or customize a template.	N/A
Alarm Policy	Specifies the policy for triggering an alarm. If you set **Resource Type** to **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. **NOTE** A maximum of 50 alarm policies can be added to an alarm rule. If any one of these alarm policies is met, an alarm is triggered.	N/A

Parameter	Description	Example Value
Mount Point or Disk	This parameter is mandatory when the metric is a fine-grained disk metric. For the Windows OS, enter a drive letter, such as **C**, **D**, or **E**. For the Linux OS, enter a mount point, such as **/dev** or **/opt**.	/dev
Alarm Severity	Specifies the alarm severity, which can be **Critical**, **Major**, **Minor**, or **Informational**.	Major

c. Configure the alarm notification.

Table 2-3 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.
Notification Object	Specifies the object to which alarm notifications will be sent. You can select the account contact or a topic. ● **Account contact** is the mobile 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 **5.2.1 Creating a Topic** and **5.2.2 Adding Subscriptions**.
Validity Period	Cloud Eye sends notifications only within the notification window 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.
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.

3 Dashboards

3.1 Introduction to Dashboards

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

3.2 Creating a Dashboard

You must create a dashboard before you add graphs. You can create a maximum of 20 dashboards.

Procedure

1. Log in to the management console.
2. Click **Service List** in the upper left corner, and select **Cloud Eye**.
3. In the navigation pane on the left, choose **Dashboard**. Click **Create Dashboard** in the upper right corner.

   The **Create Dashboard** dialog box is displayed.
4. Set the dashboard name.

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

3.3 Adding a Graph

After you create a dashboard, you can add graphs to the dashboard to monitor cloud services. Each dashboard supports up to 24 graphs.

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

Procedure

1. Log in to the management console.
2. Click **Service List** in the upper left corner, and select **Cloud Eye**.
3. In the navigation pane on the left, choose **Dashboard**. Switch to the dashboard to which you want to add a graph, and click **Add Graph**.

   The **Add Graph** dialog box is displayed.
4. 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 object. You can add up to 20 monitored objects. You can select a maximum of 20 monitored objects at a time.
Metric	Specifies the metric name. Example value: **CPU Usage**

5. Click **OK**.

   On the selected dashboard, 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 **Dashboards** page. The system provides you both default and customizable time ranges to view trends from last month. This topic describes how to view trends for a longer time range.

Procedure

1. Log in to the management console.
2. Click **Service List** in the upper left corner, and select **Cloud Eye**.

3. In the navigation pane on the left, choose **Dashboard**.

   You can view all monitoring graphs on the current dashboard.

   > **NOTE**
   >
   > - You can sort graphs by dragging them.
   > - You can click **1h**, **3h**, **12h**, **1d**, or **7d** in the upper part of monitoring graphs to switch the monitoring periods of all graphs on the dashboard. By default, raw metric data is displayed for **1h** , and the aggregated metric data is displayed for other periods.
   > - You can also go to the full screen to view the monitoring graphs. For details, see **Using the Full Screen**.

4. 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 or customize a time range to view the metric trend in a specific monitoring interval.

   Raw metric data is displayed for **1h**, **3h**, **12h**, and **1d** by default. For **7d** and **30d**, rolled-up data is displayed by default.

Using the Full Screen

The full screen displays metric data more clearly.

- To enter the full screen, click **Full Screen** in the upper right corner of the **Dashboard** page.
- To exit the full screen, click **Exit Full Screen** in the upper left corner of the page.

Customizing a Period to View the Monitoring Graph

By default, metrics in the last 1 hour, last 3 hours, last 12 hours, last 24 hours, and last 7 days are displayed. If you want to view metrics in the last 2 hours or a customized time period, you can drag the mouse to select the time range you want to view on the X axis.

- To view metric details in a customized time period, click the first icon on the right. Drag the mouse to select a customized time range. The system automatically displays the monitoring data in the selected time range.
- To go back to the default graph, click the third icon on the right.

Selecting Monitoring Objects and Viewing Metrics

To compare the same metric of multiple resources, you can combine the metrics of the resources into a graph. When there are a large number of resources, you can drag to select monitored objects if you want to compare the metric data of only some of the resources.

- To select a monitored object, click the second icon on the right. Drag the mouse on part of the curve of the target monitored objects. Then, the system automatically displays the data of the selected monitored objects and hides the monitoring data of other monitored objects.
- To go back to the default graph, click the third icon on the right.

📖 NOTE

In the lower part of an enlarged graph, you can select a monitored object as follows: Click a resource object to hide its trend chart, and click the monitored object again to display its trend chart.

3.5 Configuring a Graph

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

Procedure

1. Log in to the management console.
2. Click **Service List** in the upper left corner, and select **Cloud Eye**.
3. In the navigation pane on the left, choose **Dashboard**. 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 50 metrics to a graph.

3.6 Deleting a Graph

1. Log in to the management console.
2. Click **Service List** in the upper left corner, and select **Cloud Eye**.
3. In the navigation pane on the left, choose **Dashboard**.
4. Select the dashboard from which you want to delete a graph.
5. Hover your mouse on the target graph and click the trash icon in the upper right corner.
6. In the displayed **Delete Graph** dialog box, click **Yes**.

3.7 Deleting a Dashboard

To re-plan graphs on a dashboard, you can delete the dashboard. After that, all graphs on the dashboard will also be deleted.

Procedure

1. Log in to the management console.
2. Click **Service List** in the upper left corner, and select **Cloud Eye**.
3. In the navigation pane on the left, choose **Dashboard**.
4. Select the target dashboard.
5. Click **Delete**.
6. In the displayed **Delete Dashboard** dialog box, click **OK**.

4 Resource Groups

4.1 Introduction to Resource Groups

A resource group allows you to add and monitor correlated resources and provides a collective health status for all resources that it contains.

4.2 Creating a Resource Group

Scenarios

If you use multiple cloud services, you can add all related resources, such as ECSs, BMSs, EVS disks, elastic IP addresses, bandwidths, and databases to the same resource group for easier management and O&M.

Restrictions

- Each user can create up to 10 resource groups.
- A resource group must contain 1 to 1,000 cloud service resources.
- There are restrictions on the number of resources of different types that can be added to a resource group. For details, see the tips on the Cloud Eye console.

Procedure

1. Log in to the management console.
2. In the upper left corner, select a region and project.
3. Click **Service List** in the upper left corner, and select **Cloud Eye**.
4. In the navigation pane on the left, choose **Resource Groups**.
5. In the upper right corner, click **Create Resource Group**.
6. Enter the group name.
7. Select the target cloud service resources.

NOTE

You can search for ECSs and BMSs by name, ID, and private IP address. For other cloud services, you can search only by name and ID.

8. Click **Create**.

4.3 Viewing Resource Groups

4.3.1 Resource Group List

The resource group list displays all resource groups you have on Cloud Eye, the resources they contain, and the health status of each resource group.

Procedure

1. Log in to the management console.
2. In the upper left corner, select a region and project.
3. Click **Service List** in the upper left corner, and select **Cloud Eye**.
4. In the navigation pane on the left, choose **Resource Groups**.

   On the **Resource Groups** page, you can view all the resource groups that have been created.

Table 4-1 Parameters of the resource group list

Parameter	Description
Name/ID	Specifies the resource group name and ID. **NOTE** The group name can contain a maximum of 128 characters. Only letters, digits, hyphens (-), and underscores (_) are allowed.
Alarm Status	● No alarm: No alarm resource exists in the group. ● In alarm: An alarm is being generated for a resource in the group. ● No alarm rules set: No alarm rules have been created for any resource in the group.
Resources (Alarm/Total)	Total number of resources that are generating alarms in a group/Total number of resources in the group.
Resource Types	Specifies the number of different resource types in a group. For example, if there are two ECSs and one EVS disk in a resource group, then there are two types of resources and **Resource Types** is **2**.
Add Resources	Specifies how you add resources to a resource group. The value can be **Manually** or **Automatically**.
Synchronize Resources	You can add all resources in an enterprise project or resources with the same tags to a resource group.

Parameter	Description
Created	Specifies the time when the resource group was created.
Operation	Only the group deletion operation is supported.

4.3.2 Resource Overview

The **Resource Overview** page displays the resource types contained in the current group, as well as the total number of resources of each resource type, dimensions, and whether there are alarms generated for the resources.

Procedure

1. Log in to the management console.
2. In the upper left corner, select a region and project.
3. Click **Service List** in the upper left corner, and select **Cloud Eye**.
4. In the navigation pane on the left, choose **Resource Groups**.
5. Click a resource group name to go to the **Resource Overview** page.

4.3.3 Alarm Rules

The **Alarm Rules** page displays all alarm rules in a resource group. You can enable, disable, modify, or delete alarm rules.

Procedure

1. Log in to the management console.
2. In the upper left corner, select a region and project.
3. Click **Service List** in the upper left corner, and select **Cloud Eye**.
4. In the navigation pane on the left, choose **Resource Groups**.
5. Click a resource group name to go to the **Resource Overview** page.
6. In the navigation pane on the left, choose **Alarm Rules** to view all alarm rules in the resource group.

4.4 Managing Resource Groups

4.4.1 Deleting a Resource Group

Procedure

1. Log in to the management console.
2. In the upper left corner, select a region and project.
3. Click **Service List** in the upper left corner, and select **Cloud Eye**.
4. In the navigation pane on the left, choose **Resource Groups**.

5. Locate the row containing the target resource group and click **Delete** in the **Operation** column.
6. In the displayed **Delete Resource Group** dialog box, click **Yes**.

5 Using the Alarm Function

5.1 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 emails, or sends HTTP/HTTPS messages, enabling you to quickly respond to resource changes.

Cloud Eye invokes 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 subscription endpoints 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.

5.2 Creating Alarm Notification Topics

5.2.1 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. Log in to the management console.
2. In the upper left corner, select a region and project.
3. In the service list, select **Simple Message Notification**.

   The SMN console is displayed.

4. In the navigation pane on the left, choose **Topic Management** > **Topics**.

   The **Topics** page is displayed.

5. Click **Create Topic**.

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

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

Table 5-1 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 255 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 will be **username@example.com**.

7. 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.

8. 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.

5.2.2 Adding Subscriptions

A topic is a channel used by SMN to publish messages. Therefore, after you create a topic, add subscriptions. In this way, when the metric triggers an alarm, Cloud Eye sends the alarm information to subscription endpoints of the topic.

Adding Subscriptions

1. Log in to the management console.
2. Select **Simple Message Notification** under **Application**.

   The SMN console is displayed.

3. In the navigation pane on the left, choose **Topic Management** > **Topics**.

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

   The **Topics** page is displayed.

4. Locate the topic you want to add subscriptions to and click **Add Subscription** in the **Operation** column.

   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 subscription you added is displayed in the subscription list.

   NOTE

   After the subscription is added, the corresponding subscription endpoint will receive a subscription notification. You need to confirm the subscription so that the endpoint can receive alarm notifications.

5.3 Creating Alarm Rules

5.3.1 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.

5.3.2 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. Click **Service List** in the upper left corner, and 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 configure the parameters.
   a. Set the alarm rule name and description.

Table 5-2 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 configure alarm content parameters.

Table 5-3 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
Group	This parameter is mandatory when **Monitoring Scope** is set to **Resource groups**.	N/A
Method	There are two options: **Use template** or **Configure manually**.	Configure manually
Template	Specifies the template to be used. You can select a default alarm template or customize a template.	N/A

Parameter	Description	Example Value
Alarm Policy	Specifies the policy for triggering an alarm. If you set **Resource Type** to **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. **NOTE** A maximum of 50 alarm policies can be added to an alarm rule. If any one of these alarm policies is met, an alarm is triggered.	N/A
Mount Point or Disk	This parameter is mandatory when the metric is a fine-grained disk metric. For the Windows OS, enter a drive letter, such as **C**, **D**, or **E**. For the Linux OS, enter a mount point, such as **/dev** or **/opt**.	/dev
Alarm Severity	Specifies the alarm severity, which can be **Critical**, **Major**, **Minor**, or **Informational**.	Major

c. Configure the alarm notification.

Table 5-4 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.
Notification Object	Specifies the object to which alarm notifications will be sent. You can select the account contact or a topic. ● **Account contact** is the mobile 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 **5.2.1 Creating a Topic** and **5.2.2 Adding Subscriptions**.

Parameter	Description
Validity Period	Cloud Eye sends notifications only within the notification window 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.
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.

5.4 Viewing Alarm Records

The **Alarm Records** page displays the status changes of all alarm rules so that you can trace and view alarm records in a unified and convenient manner. By default, alarm records of the last seven days are displayed. You can customize the time range to display alarm records of the last 30 days.

When an alarm is generated, you can view the alarm records about the cloud resource.

Procedure

1. Log in to the management console.
2. Click **Service List** in the upper left corner, and select **Cloud Eye**.
3. Choose **Alarm Management** > **Alarm Records**.

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

   NOTE

   - You can select a time range within the past 30 days to view alarm records.
   - In the search bar of the **Alarm Records** page, you can search for alarm records by status, alarm severity, alarm rule name, resource type, resource ID, or alarm rule ID.
   - In the upper left of the alarm record list, you can click **Export** to export alarm records.

5.5 One-Click Monitoring

Scenarios

One-click monitoring enables you to quickly and easily enable or disable monitoring of common events for certain services. This topic describes how to use the one-click monitoring function to monitor key metrics.

Constraints

- One-click monitoring sends notifications only when alarms are generated and does not send notifications when alarms are cleared.
- Once the alarm threshold is reached, one-click monitoring will trigger alarms immediately.
- Alarm policies cannot be modified in one-click monitoring.

Procedure

1. Log in to the management console.
2. Click **Service List** in the upper left corner, and select **Cloud Eye**.
3. In the navigation pane on the left, choose **Alarm Management** > **One-Click Monitoring**.
4. Locate the cloud service you want to monitor, and enable **One-Click Monitoring**.
5. Click the arrow on the left of the cloud service name to view the built-in alarm rules.

   NOTE

   The notification object of the one-click monitoring rules is the account contact. Alarm notifications will be sent to the mobile number or email address provided during registration.

5.6 Alarm Rule Management

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

5.6.1 Modifying an Alarm Rule

Procedure

1. Log in to the management console.
2. Click **Service List** in the upper left corner, and select **Cloud Eye**.
3. Choose **Alarm Management** > **Alarm Rules**.
4. 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 **Modify** in the **Operation** column.
   - Click the name of the alarm rule you want to modify. On the page displayed, click **Modify** in the upper right corner.
5. On the **Modify Alarm Rule** page, modify alarm rule parameters as needed.

Table 5-5 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
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** When you set **Monitored Object** to **Specific resources**, you can add new monitored objects and remove the original monitored objects.	Specific resources
Alarm Policy	Specifies the policy for triggering an alarm. For example, an alarm is triggered if the average CPU usage of the monitored object is 80% or more for three consecutive 5-minute periods. Cloud Eye triggers an alarm every one hour again if the alarm persists. **NOTE** The last part of the alarm policy indicates how often to trigger an alarm again when the alarm has been triggered but the monitored object is still abnormal.	N/A
Mount Point or Disk	This parameter is mandatory when the metric is a fine-grained disk metric. For the Windows OS, enter a drive letter, such as **C**, **D**, or **E**. For the Linux OS, enter a mount point, such as **/dev** or **/opt**.	/dev
Alarm Severity	Specifies the alarm severity, which can be **Critical**, **Major**, **Minor**, or **Informational**.	Major
Alarm Notification	Specifies whether to notify users when alarms are triggered. Notifications can be sent by email, text message, or HTTP/HTTPS message.	N/A

Parameter	Description	Example Value
Notification Object	Specifies the object to which alarm notifications will be sent. You can select the account contact or a topic. ● **Account contact** is the mobile number and email address of the registered account. ● Topic: A topic is used to publish messages and subscribe to notifications. If the required topic is unavailable, create one and add subscriptions to it on the SMN console. For details, see **5.2.1 Creating a Topic** and **5.2.2 Adding Subscriptions**.	N/A
Validity Period	Cloud Eye sends notifications only within the notification window specified in the alarm rule. If **Notification Window** is set to **00:00-8:00**, Cloud Eye sends notifications only within 00:00-8:00.	N/A
Trigger Condition	Specifies the condition for triggering alarm notifications. You can select **Generated alarm** (when an alarm is generated), **Cleared alarm** (when an alarm is cleared), or both.	N/A
Enterprise Project	Specifies the enterprise project that the alarm rule belongs to. Only users with the enterprise project permissions can view and manage the alarm rule. For details about how to create an enterprise project, see .	default

6. Click **Modify**.

5.6.2 Disabling Alarm Rules

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

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 **Yes**.

5.6.3 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 **More** and **Enable** in the **Operation** column. In the displayed **Enable Alarm Rule** dialog box, click **Yes**.

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 **Yes**.

5.6.4 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 **Yes**.

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 **Yes**.

5.7 Alarm Templates

5.7.1 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. Log in to the management console.
2. Click **Service List** in the upper left corner, and select **Cloud Eye**.
3. Choose **Alarm Management** > **Alarm Templates**.

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

5.7.2 Creating a Custom Template

1. On the **Alarm Templates** page, click **Create Custom Template**.
2. On the **Create Custom Template** page, configure parameters by referring to **Table 5-6**.

Table 5-6 Parameters

Parameter	Description
Name	Specifies the alarm rule name. The system generates a random name, which you can modify. Example value: **alarmTemplate-c6ft**
Description	(Optional) Provides supplementary information about the custom template.
Method	You can select **Using existing template** or **Configure manually**. ● **Using existing template**: Select an existing template for **Template**. The default alarm rules in the template are automatically added. ● **Configure manually**: You can customize alarm policies as required.
Add Resource Type	Specifies the type of the resource the alarm rule is created for. Example value: **Elastic Cloud Server**
Metric Name	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	You can copy or delete an added alarm policy.

3. Click **Create**.

5.7.3 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 want to modify and click **Modify** in the **Operation** column.
2. On the **Modify Custom Template** page, modify the configured parameters by referring to **Table 5-6**.
3. Click **Modify**.

5.7.4 Deleting a Custom Template

In the navigation pane on the left, choose **Alarm Management** > **Alarm Templates** and click the **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**.

6 Server Monitoring

6.1 Introduction to Server Monitoring

Server monitoring includes basic monitoring, process monitoring, and OS monitoring for servers.

- Basic monitoring covers metrics automatically reported by ECSs. The data is collected every 5 minutes. For details, see **13 Services Interconnected with Cloud Eye**.
- OS monitoring provides proactive and fine-grained OS monitoring for ECSs or BMSs, and it requires the Agent to be installed on all servers that will be monitored. The data is collected every minute. OS monitoring supports metrics such as CPU usage and memory usage (Linux). For details, see **13 Services Interconnected with Cloud Eye**.
- Process monitoring provides monitoring of active processes on hosts. By default, Cloud Eye collects CPU usage, memory usage, and number of opened files of active processes.

NOTE

- Windows and Linux OSs are supported. For details, see **14.2.3 What OSs Does the Agent Support?**
- For the ECS specifications, use 2 vCPUs and 4 GB memory for a Linux ECS and 4 vCPUs and 8 GB memory or higher specifications for a Windows ECS.
- The Agent will use the system ports. For details, see descriptions of **ClientPort** and **PortNum** in **6.4.4 (Optional) Manually Configuring the Agent (Linux)**. If the Agent port conflicts with a service port, see **What Should I Do If the Service Port Is Used by the Agent?**
- To install the Agent in a Linux server, you must have the root permissions. For a Windows server, you must have the administrator permissions.

Scenarios

Whether you are using ECSs or BMSs, you can use server monitoring to track various OS metrics, monitor server resource usage, and query monitoring data when faults occur.

Monitoring Capabilities

Server monitoring provides multiple metrics, such as metrics for CPU, memory, disk, and network usage, meeting the basic monitoring and O&M requirements for servers. For details about metrics, see **13 Services Interconnected with Cloud Eye**.

Resource Usage

The Agent uses considerably less resources. When the Agent is installed on a server, it uses less than 5% of the CPU and less than 100 MB of memory.

6.2 Agent Installation and Configuration

Based on the OS you are going to use, server quantity, and personal habits, install the Agent by choosing one or more of the following scenarios:

Scenario	Supported Service	Reference
Installing the Agent on a Linux server	ECS and BMS	**6.4 Installing and Configuring the Agent on a Linux ECS or BMS**
Installing the Agent on a Windows server	ECS	**6.5 Installing and Configuring the Agent on a Windows ECS**

Agent installation and configuration description:

- To successfully install the Agent, ensure that both DNS and security group rules are correctly configured.
- After you install the Agent, you can click **Restore Agent Configurations** on the Cloud Eye console to complete the agency and Agent configuration.
- If the Agent fails to be configured by clicking **Restore Agent Configurations** or due to other reasons, manually configure it.
- It is recommended that you use an ECS or BMS with the Agent installed to create a private image, use the private image to create another ECS or BMS, and then configure the Agent for the new ECS or BMS by following the steps in **6.4.3 Restoring the Agent Configurations on a Linux Server**.

  NOTE

  A private image created in one region cannot be used in another region. Otherwise, no monitoring data will be generated for the ECSs created by using this private image.

  If you install the Agent on an ECS created using a private image, and any problem occurs during the Agent installation and usage, Cloud Eye does not provide technical support.

6.3 Agent Features per Version

Metrics or functions supported by the Agent vary depending on the Agent version. By default, the Agent is automatically upgraded, so that you can experience new functions as earlier as possible. The following describes features of each Agent version.

Version 1.2.3

The permission on the file generated after the Agent is installed is optimized.

Version 1.2.2

A 20-minute random hash is added when the Agent is started.

Version 1.1.9

Some metrics are optimized for better experience.

Version 1.1.2

The Agent performance is optimized. When the Agent does not report data, manually rectify it by referring to **What Should I Do If the Monitoring Period Is Interrupted or the Agent Status Keeps Changing?**

Version 1.0.14

CPU, CPU load, disk, and disk I/O metrics are added to **OS Monitoring**. For details, see **13 Services Interconnected with Cloud Eye**.

6.4 Installing and Configuring the Agent on a Linux ECS or BMS

6.4.1 Modifying the DNS Server Address and Adding Security Group Rules (Linux)

Scenarios

This topic describes how to add the DNS server address and security group rules to a Linux ECS or BMS to ensure successful downloading of the Agent installation package and successful monitoring data collection. This topic takes an ECS as an example. The operations for BMSs are similar.

You can modify the DNS server address of an ECS via command lines or the management console.

NOTE

DNS and security group configuration are intended for the primary NIC.

Modifying the DNS Server Address (Command Lines)

The following describes how to add the DNS server address to the **resolv.conf** file using command lines.

To use the management console, see **Modifying the DNS Server Address (Management Console)**.

1. Log in to an ECS as user **root**.
2. Run the **vi /etc/resolv.conf** command to open the file.
3. Add the DNS server address, for example, **nameserver 202.165.20.99** to the file. Enter **:wq** and press **Enter** to save the change.

   NOTE

   The value of **nameserver** varies depending on the region.

   my-kualalumpur-1: 202.165.20.99

Modifying the DNS Server Address (Management Console)

The following describes how to modify the DNS server address of an ECS on the management console. This topic takes an ECS as an example. The operations for BMSs are similar.

1. In the upper left corner, select a region and project.
2. Click **Service List** in the upper left corner. Under **Compute**, select **Elastic Cloud Server**.

   On the ECS console, click the name of the target ECS to view its details.
3. On the displayed **Summary** tab page, click the VPC name.

   The **Virtual Private Cloud** page is displayed.
4. Click the name of the target VPC.
5. In the **Networking Components** area, click the number following **Subnets**.

   The **Subnets** page is displayed.
6. In the subnet list, click the name of target subnet.
7. In the **Gateway and DNS Information** area, click ✎ following **DNS Server Address**.

   NOTE

   Set the DNS server address to the value of **nameserver** in **3**.
8. Click **OK**.

   NOTE

   The new DNS server address takes effect after the ECS or BMS is restarted.

Modifying the ECS Security Group Rules (Management Console)

The following describes how to modify security group rules for an ECS on the management console. This topic takes an ECS as an example. The operations for BMSs are similar.

1. On the ECS details page, click the **Security Groups** tab.

   The security group list is displayed.
2. Click the security group name.

3. Click **Modify Security Group Rule**.

   The security group details page is displayed.

   NOTE

   Procedure for BMS:

   1. Click the security group ID on the upper left.
   2. Click **Manage Rule** in the **Operation** column of the security group.

4. Click the **Outbound Rules** tab, and click **Add Rule**.
5. Add rules based on **Table 6-1**.

Table 6-1 Security group rules

Protocol	Port	Type	Destination	Description
TCP	80	IPv4	100.125.0.0/16	Used to download the Agent installation package from an OBS bucket to an ECS or BMS and obtain the ECS or BMS metadata and authentication information.
TCP and UDP	53	IPv4	100.125.0.0/16	Used by DNS to resolve domain names, for example, resolve the OBS domain name when you are downloading the Agent installation package, and resolve the Cloud Eye endpoint when the Agent is sending monitoring data to Cloud Eye.
TCP	443	IPv4	100.125.0.0/16	Used to collect monitoring data and send the data to Cloud Eye.

6.4.2 Installing the Agent on a Linux Server

Scenarios

This topic describes how to manually install the Agent on a Linux ECS or BMS.

Prerequisites

- You have the read and write permissions for the installation directories in **Procedure**. The Telescope process will not be stopped by other software after the installation.
- You have performed operations described in **6.4.1 Modifying the DNS Server Address and Adding Security Group Rules (Linux)**.

Procedure

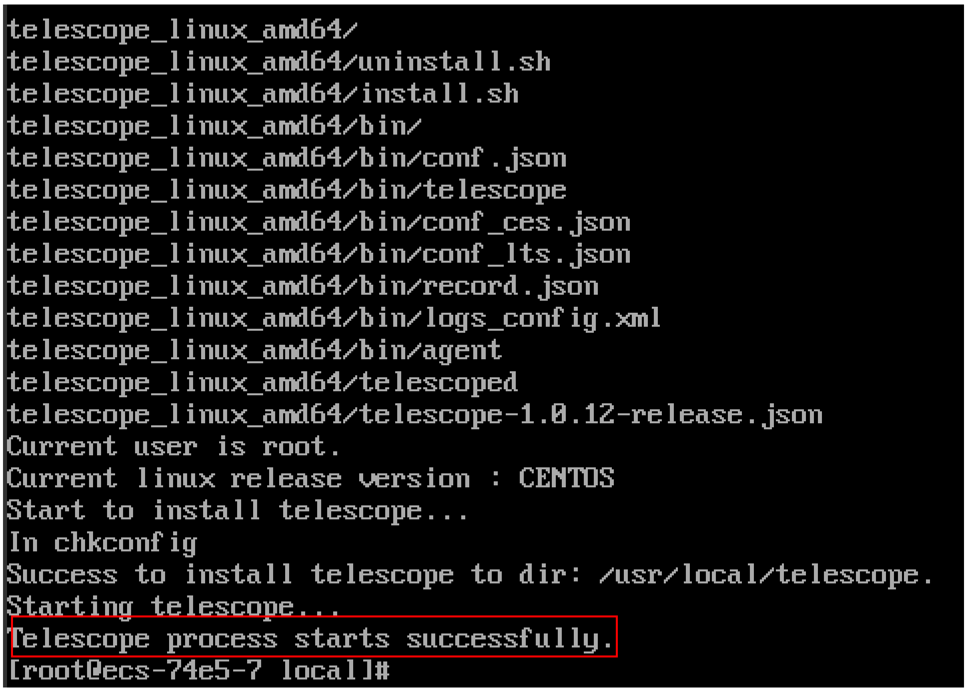
1. Log in to the ECS or BMS as user **root**.
2. Run the following command to install the Agent:

   my-kualalumpur-1:

   ```
   cd /usr/local && wget https://telescope-my-kualalumpur-1.obs.my-kualalumpur-1.alphaedge.tmone.com.my/scripts/agentInstall.sh && chmod 755 agentInstall.sh && ./agentInstall.sh
   ```

   The Agent is installed if the following command output is displayed.

   Figure 6-1 Successful installation

   ```
   telescope_linux_amd64/
   telescope_linux_amd64/uninstall.sh
   telescope_linux_amd64/install.sh
   telescope_linux_amd64/bin/
   telescope_linux_amd64/bin/conf.json
   telescope_linux_amd64/bin/telescope
   telescope_linux_amd64/bin/conf_ces.json
   telescope_linux_amd64/bin/conf_lts.json
   telescope_linux_amd64/bin/record.json
   telescope_linux_amd64/bin/logs_config.xml
   telescope_linux_amd64/bin/agent
   telescope_linux_amd64/telescoped
   telescope_linux_amd64/telescope-1.0.12-release.json
   Current user is root.
   Current linux release version : CENTOS
   Start to install telescope...
   In chkconfig
   Success to install telescope to dir: /usr/local/telescope.
   Starting telescope...
   Telescope process starts successfully.
   [root@ecs-74e5-7 local]#
   ```

3. Configure the Agent by referring to **6.4.3 Restoring the Agent Configurations on a Linux Server** or **6.4.4 (Optional) Manually Configuring the Agent (Linux)**.

   NOTE

   - **Restoring Agent Configurations** allows you to configure **AK/SK**, **RegionID**, and **ProjectId** in just a few clicks. You can also modify related configuration files by referring to **6.4.4 (Optional) Manually Configuring the Agent (Linux)**.
   - Agent configuration restoration cannot be performed on BMSs. For details about how to modify the Agent configuration file on a BMS, see **6.4.4 (Optional) Manually Configuring the Agent (Linux)**.

4. Run the following command to clear the installation script:

   if [[-f /usr/local/uniagent/extension/install/telescope/bin/telescope]]; then rm /usr/local/agent_install.sh; else rm /usr/local/agentInstall.sh; fi

6.4.3 Restoring the Agent Configurations on a Linux Server

Scenarios

This topic describes how to restore the Agent configurations on the Cloud Eye console (recommended).

NOTE

- The **Restore Agent Configurations** option is available for Agent 1.0.14 or later. If the Agent version is earlier than 1.0.14, upgrade the Agent first and then restore the Agent configurations or manually configure the Agent by following the instructions in **6.4.4 (Optional) Manually Configuring the Agent (Linux)**.
- The **Restore Agent Configurations** option is unavailable for BMSs. For details, see **6.4.4 (Optional) Manually Configuring the Agent (Linux)**.
- After you configure the Agent, its status is still displayed as **Not installed** because no monitoring data is reported yet. Wait 3 to 5 minutes and refresh the page.
- If the Agent is in the **Running** state and **Monitoring Status** is enabled, the Agent has been installed and has started to collect fine-grained metric data.

Restoring the Agent Configurations

1. Log in to the management console.
2. Click **Service List** in the upper left corner, and select **Cloud Eye**. In the navigation pane on the left, choose **Server Monitoring**.
3. On the **Server Monitoring** page, select a server that has the Agent installed.
4. Click **Restore Agent Configurations**.
5. In the displayed **Restore Agent Configurations** dialog box, click **One-Click Restore**.

   If the Agent status changes to **Running** and **Monitoring Status** is enabled, the Agent has been installed and has started to collect fine-grained metric data.

6.4.4 (Optional) Manually Configuring the Agent (Linux)

Scenarios

After you install the Agent, configure it by clicking **Restore Agent Configurations** on the Cloud Eye console. If the Agent fails to be configured by clicking **Restore Agent Configurations** or due to other reasons, manually configure it by following the instructions provided in this topic.

This topic takes an ECS as an example. The operations for BMSs are similar.

Prerequisites

The Agent has been installed.

Procedure

1. Log in to an ECS as user **root**.

2. Run the following command to go to the Agent installation path **bin**:

   cd /usr/local/uniagent/extension/install/telescope/bin

3. Modify configuration file **conf.json**.

   a. Run the following command to open **conf.json**:

      vi conf.json

   b. Modify the parameters in the file. For details, see **Table 6-2**.

      ECS parameters

NOTICE

Storing plaintext AKs and SKs poses great security risks. You are advised to delegate all ECS or BMS Agents in the region. For details, see **14.2.7 How Can I Create an Agency?**

```
{
    "InstanceId":"XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX",
    "ProjectId": "XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX",
    "AccessKey": "XXXXXXXXXXXXXXXXXXXX",
    "SecretKey": "XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX",
    "RegionId": "my-kualalumpur-1",
    "ClientPort": 0,
    "PortNum": 200
}
```

BMS parameters

```
{
    "InstanceId":"XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX",
    "ProjectId": "XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX",
    "AccessKey": "XXXXXXXXXXXXXXXXXXXX",
    "SecretKey": "XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX",
    "RegionId": "my-kualalumpur-1",
    "ClientPort": 0,
    "PortNum": 200,
    "BmsFlag": true
}
```

Table 6-2 Public parameters

Parameter	Description
InstanceId	(Optional) Specifies the ECS ID. You can log in to the management console and view the ECS ID in the ECS list. **NOTE** If you do not configure **InstanceId**, retain **"InstanceId":""**. If you configure it, ensure that the following two requirements are met: ● The ECS ID must be unique at all sites, that is, in the same region, **InstanceId** used by the Agent cannot be the same. Otherwise, errors may occur. ● The **InstanceId** value must be consistent with the actual ECS ID. Otherwise, you cannot see the OS monitoring data on Cloud Eye.

Paramete r	Description
ProjectId	(Optional) Specifies the project ID. If you do not configure **ProjectId**, retain **"ProjectId": ""**. If you configure it, perform the following operations: 1. Log in to the Cloud Eye console, click the username in the upper right corner, and choose **My Credentials**. 2. Under **Projects**, obtain the project ID for the region where the ECS is located.
AccessKey / SecretKey	To obtain the AK and SK, perform the following operations: Log in to the Cloud Eye console, click the username in the upper right corner, and choose **My Credentials**, and choose **Access Keys**. ● If you have obtained the access key, obtain the **AccessKey** value and the **SecretKey** value in the **credentials.csv** file saved when you create **Access Keys**. ● If no access keys are available, click **Create Access Key** to create one. Save the **credentials.csv** file and obtain the **AccessKey** value and the **SecretKey** value in it. **NOTICE** ● For the security purpose, use an IAM username with the **CES Administrator** and **LTS Administrator** permissions. ● The configured access key must be within the **Access Keys** list on the **My Credentials** page. Otherwise its authentication will fail and you cannot view OS monitoring data on Cloud Eye.
RegionId	Specifies the region ID. For example, the ECS or BMS region ID is **my-kualalumpur-1**. For IDs of other regions, see https://support.alphaedge.tmone.com.my/en-us/endpoint/index.html.
ClientPort	Specifies the start port number used by the Agent. **NOTE** The default value is **0,** indicating that the Agent will randomly use any port. Ports 1 to 1023 are reserved. You are advised not to specify a port in this range for the Agent.
PortNum	Specifies the number of ports configured for the Agent. **NOTE** The default value is **200**. If **ClientPort** is **5000**, the port range will be 5000 to 5199.
BmsFlag	Set this parameter to **true** for a BMS. This parameter is not required by an ECS. You do not need to set this parameter for the Windows OS.

4. Modify configuration file **conf_ces.json** for the Cloud Eye metric collection module.

   a. Run the following command to open public configuration file **conf_ces.json**:

      vi conf_ces.json

   b. Modify the endpoint in **conf_ces.json**, and save the **conf_ces.json** file. For details, see **Table 6-3**.

```
{
  "Endpoint": "https://ces.my-kualalumpur-1.alphaedge.tmone.com.my"
}
```

Table 6-3 Parameter setting of the metric collection module

Parameter	Description
Endpoint	Specifies the Cloud Eye endpoint URL in the region the ECS or BMS belongs to. For example, if the ECS or BMS is located in , **Endpoint** is .

NOTE

- After you configure the Agent, its status is still displayed as **Uninstalled** because no monitoring data is reported yet. Wait 3 to 5 minutes and refresh the page.
- If the Agent is in the **Running** state and **Monitoring Status** is enabled, the Agent has been installed and has started to collect fine-grained metric data.

6.5 Installing and Configuring the Agent on a Windows ECS

6.5.1 Modifying the DNS Server Address and Adding Security Group Rules (Windows)

Scenarios

This topic describes how to add the DNS server address and security group rules to a Windows ECS to ensure successful downloading of the Agent installation package and successful monitoring data collection.

The DNS server address of an ECS can be modified in either of the following ways: Windows GUI or management console. Choose a method based on your habits.

NOTE

DNS and security group configuration are intended for the primary NIC.

Modifying the DNS Server Address (Windows GUI)

The following describes how to use the Windows GUI to add the DNS server address.

1. Click **Service List** in the upper left corner. Under **Compute**, select **Elastic Cloud Server**. Use VNC to log in to the Windows ECS.
2. Choose **Control Panel** > **Network and Sharing Center**, and click **Change adapter settings**.
3. Right-click the used network, choose **Settings** from the shortcut menu, and configure the DNS.

   NOTE

   The DNS server address varies depending on the region.

   my-kualalumpur-1: 202.165.20.99

Modifying the ECS Security Group Rules (Management Console)

The following describes how to modify security group rules for an ECS on the management console. This topic takes an ECS as an example. The operations for BMSs are similar.

1. On the ECS details page, click the **Security Groups** tab.

   The security group list is displayed.
2. Click the security group name.
3. Click **Modify Security Group Rule**.

   The security group details page is displayed.

   NOTE

   Procedure for BMS:

   1. Click the security group ID on the upper left.
   2. Click **Manage Rule** in the **Operation** column of the security group.
4. Click the **Outbound Rules** tab, and click **Add Rule**.
5. Add rules based on **Table 6-4**.

Table 6-4 Security group rules

Protocol	Port	Type	Destination	Description
TCP	80	IPv4	100.125.0.0/16	Used to download the Agent installation package from an OBS bucket to an ECS or BMS and obtain the ECS or BMS metadata and authentication information.

Protocol	Port	Type	Destination	Description
TCP and UDP	53	IPv4	100.125.0.0/16	Used by DNS to resolve domain names, for example, resolve the OBS domain name when you are downloading the Agent installation package, and resolve the Cloud Eye endpoint when the Agent is sending monitoring data to Cloud Eye.
TCP	443	IPv4	100.125.0.0/16	Used to collect monitoring data and send the data to Cloud Eye.

6.5.2 Installing and Configuring the Agent on a Windows Server

Scenarios

This topic describes how to install the Agent on a Windows ECS.

Constraints

The Agent cannot be installed on Windows BMSs.

Prerequisites

- You have performed operations described in **6.5.1 Modifying the DNS Server Address and Adding Security Group Rules (Windows)**.
- Use an administrator account to install the Agent.
- Ensure that the Telescope process is not stopped by other processes after the installation.
- You have obtained the Agent installation package (Windows).

Table 6-5 Installation package path

Name	Format	Download Path
Installation package for 64-bit Windows	zip	my-kualalumpur-1: **https://telescope-my-kualalumpur-1.obs.my-kualalumpur-1.alphaedge.tmone.com.my/agent/telescope_windows_amd64.zip**

Procedure

1. Log in to the Windows ECS as an administrator.
2. Open a browser, and enter the address of the Agent installation package in the address box to download and save the installation package.
3. Create a directory for storing the installation package (for example, **D:\Agent**) and decompress the package to this directory.
4. Double-click the **install.bat** script to install and start the Agent.

   If **Install service success** is displayed, the Agent is successfully installed and started.

   NOTE

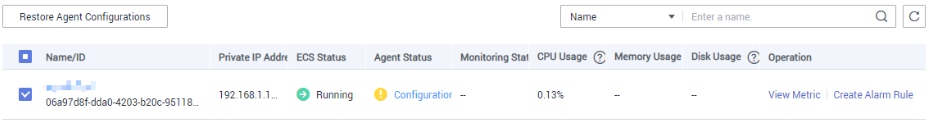
   > After you configure the Agent, its status is still displayed as **Uninstalled** because no monitoring data is reported yet. Wait 3 to 5 minutes and refresh the page.

5. On the **Server Monitoring** page, select the target ECS and click **Restore Agent Configurations**.
6. In the displayed **Restore Agent Configurations** dialog box, click **One-Click Restore**.

   The Agent configuration is completed.

   If the Agent is in the **Running** state and **Monitoring Status** is enabled, the Agent has been installed and has started to collect fine-grained metric data.

Figure 6-2 Restore Agent Configurations



■	Name/ID	Private IP Addre	ECS Status	Agent Status	Monitoring Stat	CPU Usage ⓘ	Memory Usage	Disk Usage ⓘ	Operation
☑	[redacted] 06a97d8f-dda0-4203-b20c-95118...	192.168.1.1...	Running	Configuratior	--	0.13%	--	--	View Metric | Create Alarm Rule

6.5.3 (Optional) Manually Configuring the Agent on a Windows Server

Scenarios

After you install the Agent, configure it by clicking **Restore Agent Configurations** on the Cloud Eye console. If the Agent fails to be configured by clicking **Restore Agent Configurations** or due to other reasons, manually configure it by following the instructions provided in this topic.

Constraints

The Agent cannot be installed on Windows BMSs.

Prerequisites

The Agent has been installed.

Procedure

1. Log in to the ECS.

2. Open the **conf.json** file in the **telescope_windows_amd64\bin** directory.
3. Configure the following parameters. For details, see **Table 6-6**.

NOTICE

Storing plaintext AKs and SKs poses great security risks. You are advised to delegate all ECS or BMS Agents in the region. For details, see **14.2.7 How Can I Create an Agency?**

```
{
    "InstanceId":"",
    "ProjectId": "",
    "AccessKey": "",
    "SecretKey": "",
    "RegionId": "my-kualalumpur-1",
    "ClientPort": 0,
    "PortNum": 200
}
```

Table 6-6 Public parameters

Parameter	Description
InstanceId	(Optional) Specifies the ECS ID. You can log in to the management console and view the ECS ID in the ECS list. **NOTE** If you do not configure **InstanceId**, retain **"InstanceId":""**. If you configure it, ensure that the following two requirements are met: ● The ECS ID must be unique at all sites, that is, in the same region, **InstanceId** used by the Agent cannot be the same. Otherwise, errors may occur. ● The **InstanceId** value must be consistent with the actual ECS or BMS ID. Otherwise, you cannot see the OS monitoring data on Cloud Eye.
ProjectId	Specifies the project ID. You do not need to configure **ProjectId**. Retain **"ProjectId": ""**. If you wish to configure it, perform the following operations: 1. Log in to the Cloud Eye console, click the username in the upper right corner, and choose **My Credentials**. 2. Under **Projects**, obtain the project ID for the region where the ECS or BMS is located.

Parameter	Description
AccessKey/ SecretKey	To obtain the AK and SK, perform the following operations: Log in to the Cloud Eye console, click the username in the upper right corner, and choose **My Credentials**, and choose **Access Keys**. ● If you have obtained the access key, obtain the **AccessKey** value and the **SecretKey** value in the **credentials.csv** file saved when you create **Access Keys**. ● If no access keys are available, click **Create Access Key** to create one. Save the **credentials.csv** file and obtain the **AccessKey** value and the **SecretKey** value in it. NOTICE ● For security purposes, it is recommended that the user be an IAM user with the **CES Administrator** and **LTS Administrator** permissions only.. ● The configured access key must be within the **Access Keys** list on the **My Credentials** page. Otherwise its authentication will fail and you cannot view OS monitoring data on Cloud Eye.
RegionId	Specifies the region ID. For example, the ECS or BMS region ID is **my-kualalumpur-1**. For IDs of other regions, see https://support.alphaedge.tmone.com.my/en-us/endpoint/index.html.
ClientPort	Specifies the start port number used by the Agent. **NOTE** The default value is **0,** indicating that the Agent will randomly use any port. Ports 1 to 1023 are reserved. You are advised not to specify a port in this range for the Agent.
PortNum	Specifies the number of ports configured for the Agent. **NOTE** The default value is **200**. If **ClientPort** is **5000**, the port range will be 5000 to 5199.

4. Wait for a few minutes.

   If **Agent Status** is **Running** and **Monitoring Status** is enabled, the Agent has been installed and starts to collect fine-grained metric data.

6.6 Installing the Agents in Batches on Linux ECSs

Scenarios

This topic describes how to install Agents in batches on Linux ECSs.

Operation

After binding an elastic IP address to an ECS, install and configure the Agent by following instructions in **6.4 Installing and Configuring the Agent on a Linux ECS or BMS** to ensure that data collection is normal. Use the ECS as a jump server and run scripts in batches to copy, decompress, and install the Agent package and configuration file to other ECSs.

NOTICE

- The ECSs where the Agent is to be installed in batches must belong to the same VPC.
- Agents cannot be installed on Windows servers in batches.

Prerequisites

- The IP addresses and password of user **root** of all ECSs for which the Agent is to be installed have been collected, sorted in the iplist.txt format, and uploaded to the **/usr/local** directory on the first ECS.

  NOTE

  In the **iplist.txt** file, each line contains only one IP address in the "IP address,Password of user **root**" format.

  In the following example, **abcd** is the password.

  ```
  192.168.1.1,abcd
  192.168.1.2,abcd
  ```

Procedure

1. Use PuTTY to log in to the ECS on which the Agent has been installed as user **root**.
2. Run the following command to download and run the batch installation script:

   MY-Kuala Lumpur

   ```
   cd /usr/local && wget https://telescope-my-kualalumpur-1.obs.my-kualalumpur-1.alphaedge.tmone.com.my/scripts/agentBatchPackage.sh && chmod 755 agentBatchPackage.sh && ./agentBatchPackage.sh
   ```

3. After the installation is complete, log in to the Cloud Eye console and choose **Server Monitoring** in the navigation pane on the left.

   View the list of ECSs on which the Agent has been installed.

   NOTE

   After you configure the Agent, its status is still displayed as **Uninstalled** because no monitoring data is reported yet. Wait 3 to 5 minutes and refresh the page.

4. On the **Server Monitoring** page, select all ECSs and click **Restore Agent Configurations**.
5. On the page that is displayed, click **One-Click Restore**.

6.7 Managing the Agent

This topic describes how to manage the Agent, including how to view, start, stop, and uninstall the Agent.

6.7.1 Managing the Agent (Linux)

NOTE

To view, start, stop, update, and uninstall the Agent, you must log in as user **root**.

Checking the Agent Status

Log in to an ECS or BMS as user **root** and run the following command to check the Agent status:

service telescoped status

The following message indicates that the Agent is running properly:

```
"Active (running) or "Telescope process is running well."
```

Starting the Agent

/usr/local/telescope/telescoped start

Restarting the Agent

/usr/local/telescope/telescoped restart

Stopping the Agent

Log in to an ECS or BMS and run the following command to stop the Agent:

service telescoped stop

NOTE

If the Agent installation fails, it may be impossible to stop the Agent normally. In this case, run the following command to stop the Agent:

/usr/local/telescope/telescoped stop

Uninstalling the Agent

Run the following command to uninstall the Agent:

/usr/local/telescope/uninstall.sh

NOTICE

You can manually uninstall the Agent. After the uninstallation, Cloud Eye does not collect the ECS or BMS monitoring data every one minute. To use the Agent again, reinstall it by referring to **6.4 Installing and Configuring the Agent on a Linux ECS or BMS**. Before reinstalling the Agent, manually delete the previous Agent installation package.

6.7.2 Managing the Agent (Windows)

The default installation path of the Agent is **C:\Program Files\telescope**.

Checking the Agent Status

In the task manager, check the status of the telescope process.

Starting the Agent

In the directory where the Agent installation package is stored, double-click the **start.bat** script.

Stopping the Agent

In the directory where the Agent installation package is stored, double-click the **shutdown.bat** script.

Uninstalling the Agent

In the directory where the Agent installation package is stored, double-click the **uninstall.bat** script.

NOTICE

Before reinstalling the Agent, manually delete the previous Agent installation package.

6.8 Process Monitoring

6.8.1 Viewing Process Monitoring

Process monitoring is used to monitor active processes on a host. By default, the Agent collects CPU usage, memory usage, and the number of opened files of the active processes. If you have customized process monitoring, the number of processes containing keywords is also monitored.

The Agent collects process CPU usages once every minute and displays the top 5 processes, ranked by the CPU usage over the last 24 hours.

NOTE

To view the process monitoring information, install the Agent.

Querying the System Processes

After the Agent is installed, you can check system processes on Cloud Eye.

To query the number of processes

1. Log in to the management console.
2. Click **Service List** in the upper left corner, and select **Cloud Eye**.
3. In the navigation pane on the left, choose **Server Monitoring**.
4. On the **Server Monitoring** page, locate the **Monitoring Status** column and enable the OS monitoring function.

NOTE

Ensure that **Monitoring Status** is enabled for all ECSs for which you want to monitor system processes, so that you can query monitoring data of the system processes in a timely manner.

5. On the **Server Monitoring** page, locate the row that contains the target ECS and click **View Metric** to go to the **OS Monitoring** page.
6. Select the **Process Monitoring** tab.

   In the **System Processes** area, the process information is displayed. **Table 6-7** describes the metrics of system processes.

Table 6-7 System process metrics

Metric	Description	Value Range	Collection Mode (Linux)	Collection Mode (Windows)
Running Processes	Number of processes that are running	≥ 0	Monitored object: ECS or BMS You can obtain the state of each process by checking the **Status** value in the **/proc/pid/status** file, and then collect the total number of processes in each state.	Not supported
Idle Processes	Number of processes that are idle	≥ 0	Monitored object: ECS or BMS You can obtain the state of each process by checking the **Status** value in the **/proc/pid/status** file, and then collect the total number of processes in each state.	Not supported
Zombie Processes	Number of zombie processes	≥ 0	Monitored object: ECS or BMS You can obtain the state of each process by checking the **Status** value in the **/proc/pid/status** file, and then collect the total number of processes in each state.	Not supported

Metric	Description	Value Range	Collection Mode (Linux)	Collection Mode (Windows)
Blocked Processes	Number of processes that are blocked	≥ 0	Monitored object: ECS or BMS You can obtain the state of each process by checking the **Status** value in the **/proc/pid/status** file, and then collect the total number of processes in each state.	Not supported
Sleeping Processes	Number of processes that are sleeping	≥ 0	Monitored object: ECS or BMS You can obtain the state of each process by checking the **Status** value in the **/proc/pid/status** file, and then collect the total number of processes in each state.	Not supported
Total Processes	Total number of processes	≥ 0	Monitored object: ECS or BMS You can obtain the state of each process by checking the **Status** value in the **/proc/pid/status** file, and then collect the total number of processes in each state.	Monitored object: ECS or BMS Obtain the total number of processes by using the system process status support module **psapi.dll**.

Viewing the Running Data of Top CPU Processes

- The Agent collects process CPU usages once every minute and displays the top 5 processes, ranked by the CPU usage over the last 24 hours.
- Run the **top** command to query the CPU usage and memory usage of a process.
- Run the **lsof** or **ls /proc/*pid*/fd |wc -l** command to query the number of files opened by the current process. In the command, replace *pid* with the ID of the process to be queried.

NOTE

- If a process occupies multiple CPUs, the CPU usage may exceed 100% because the collection result is the total usage of multiple CPUs.
- The top 5 processes are not fixed. The process list displays the top 5 processes that have entered the statistical period of 1 minute in the last 24 hours.
- The CPU usage, memory usage, and number of opened files are collected only for the top 5 processes for which monitoring has been enabled in the last 24 hours. If such a process has been stopped, its data will not be displayed.
- The time in the list indicates the time when the process is created.
- If the system time on the client browser is different from that on the monitored ECS, the graph may have no metric data. In this case, synchronize the local time with the ECS time.

To query information about top 5 processes with the highest CPU usages

1. Log in to the management console.
2. Click **Service List** in the upper left corner, and select **Cloud Eye**.
3. In the navigation pane on the left, choose **Server Monitoring**.
4. On the **Server Monitoring** page, locate the **Monitoring Status** column and enable the OS monitoring function.
5. On the **Server Monitoring** page, locate the row that contains the target ECS and click **View Metric** to go to the **OS Monitoring** page.
6. Select the **Process Monitoring** tab.
7. In the **Monitored Processes** area, click ⚙ in the upper right corner to view **Top 5 Processes with Highest CPU Usage**.
8. In the displayed **TOP 5 Processes with Highest CPU Usage** window, enable process monitoring for target processes, and click **OK**.

   In the **Monitored Processes** area, the system selects processes in the **Running** state by default and displays CPU usage curves of those processes in **1h**. The displayed data is raw data.

   You can also select the process to be displayed and view its CPU usage curve in **1h**.

   You can click **CPU Usage**, **Memory Usage**, or **Open Files** above the graph to view the curves of different metrics of the currently displayed process. **Table 6-8** lists **Process Monitoring** metrics.

Table 6-8 Process Monitoring metrics

Metric	Description	Value Range	Collection Mode (Linux)	Collection Mode (Windows)
CPU Usage	Specifies the usage of CPU consumed by a process. **pHashId** (process name and process ID) is the value of **md5**.	0–100 %	Monitored object: ECS or BMS Check the metric value changes in file **/proc/pid/stat**.	Monitored object: ECS or BMS Call Windows API GetProcessTimes to obtain the CPU usage of the process.
Memory Usage	Specifies the memory consumed by a process. **pHashId** (process name and process ID) is the value of **md5**.	0–100 %	Monitored object: ECS or BMS **Memory Usage** = **RSS***PAGESIZE**/**MemTotal** **RSS**: Obtain its value by checking the second column of file **/proc/pid/statm**. **PAGESIZE**: Obtain its value by running the **getconf PAGESIZE** command. **MemTotal**: Obtain its value by checking file **/proc/meminfo**.	Monitored object: ECS or BMS Invoke Windows API procGlobalMemoryStatusEx to obtain the total memory size. Invoke GetProcessMemoryInfo to obtain the used memory size. Use the used memory size to divide the total memory size to get the memory usage.
Open Files	Specifies the number of opened files consumed by the process. **pHashId** (process name and process ID) is the value of **md5**.	≥ 0	Monitored object: ECS or BMS You can run the **ls -l /proc/pid/fd** command to view the number.	Not supported

9. Hover your mouse over a graph. In the upper right corner, click ⤢ to enlarge the graph for viewing detailed data.

   In the upper left corner, you can see six default monitoring periods: **1h**, **3h**, **12h**, **1d**, **7d**, and **30d**. To view historical monitoring data for any period during the last six months, customize the monitoring period by setting **Select Range** in the upper right corner.

In the upper left corner of the graph, you can click **Settings** to configure the rollup method.

6.9 Viewing Server Monitoring Metrics

Scenarios

This topic describes how to view server monitoring metrics, including fine-grained OS metrics collected by the Agent and basic ECS metrics.

For details, see **13 Services Interconnected with Cloud Eye**.

Prerequisites

You have installed the Agent. For details, see **6.4 Installing and Configuring the Agent on a Linux ECS or BMS** and **6.5.2 Installing and Configuring the Agent on a Windows Server**.

Procedure

1. Log in to the management console.
2. Click **Service List** in the upper left corner, and select **Cloud Eye**.
3. View ECS or BMS metrics.
   - To view OS monitoring metrics of an ECS, in the left navigation pane, choose **Server Monitoring** > **Elastic Cloud Server**, locate the ECS, and click **View Metric** in the **Operation** column.
   - To view basic monitoring metrics of an ECS, in the left navigation pane, choose **Server Monitoring** > **Elastic Cloud Server**, locate the ECS, and click **View Metric** in the **Operation** column. Click the **Basic Monitoring** tab.
   - To view OS monitoring metrics of a BMS, in the left navigation pane, choose **Server Monitoring** > **Bare Metal Server**, locate the BMS, and click **View Metric** in the **Operation** column.
4. View metrics.

   In the upper part of the **OS Monitoring** page, different metric types, such as CPU, memory, and disk metrics are displayed.

   View metric graphs based on raw data from the last 1 hour, last 3 hours, last 12 hours, last 1 day, last 7 days, or last 30 days. Cloud Eye provides the **Auto Refresh** function at 60-second intervals.
5. Hover your mouse over a graph. In the upper right corner, click ⤡ to enlarge the graph for viewing detailed data.

   In the upper left corner, you can see six default monitoring periods: **1h**, **3h**, **12h**, **1d**, **7d**, and **30d**. To view historical monitoring data for any period during the last six months, customize the monitoring period by setting **Select Range** in the upper right corner.

6. In the upper left corner of the graph, click **Settings** to configure the rollup method.

6.10 Creating an Alarm Rule to Monitor a Server

Scenarios

This topic describes how to create an alarm rule for an ECS or BMS.

Procedure

1. Log in to the management console.
2. In the upper left corner, select a region and project.
3. Click **Service List** in the upper left corner, and select **Cloud Eye**.
4. In the navigation pane on the left, choose **Server Monitoring**.
5. Locate the target ECS or BMS, and click **Create Alarm Rule** in the **Operation** column.
6. On the **Create Alarm Rule** page, follow the prompts to configure the parameters.
   a. Set the alarm rule name, description, and associated enterprise project.

Table 6-9 Parameter description

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

   b. Select a monitored object and configure alarm content parameters.

Table 6-10 Parameter description

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.	Specific resources

Parameter	Description	Example Value
Monitored Object	You do not need to set the monitored object because it is the current ECS.	N/A
Method	There are three options: **Associate template**, **Use existing template**, and **Configure manually**. **NOTE** After an associated template is modified, the policies contained in this alarm rule to be created will be modified accordingly.	Configure manually
Template	Specifies the template to be used. You can select a default alarm template or **a custom template**.	N/A
Alarm Policy	Specifies the policy for triggering an alarm. For example, an alarm is triggered if the average CPU usage of the monitored object is 80% or more for three consecutive 5-minute periods. Cloud Eye triggers an alarm every one hour again if the alarm persists. For details about basic and OS monitoring metrics, see **13 Services Interconnected with Cloud Eye**. **NOTE** ● That is, if the alarm is not cleared after it is generated, an alarm notification is sent, once every hour. ● A maximum of 50 alarm policies can be added to an alarm rule. If any one of these alarm policies is met, an alarm is triggered.	N/A
Mount Point or Disk	This parameter is mandatory when the metric is a fine-grained disk metric. For the Windows OS, enter a drive letter, such as **C**, **D**, or **E**. For the Linux OS, enter a mount point, such as **/dev** or **/opt**.	/dev
Alarm Severity	Specifies the alarm severity, which can be **Critical**, **Major**, **Minor**, or **Informational**.	Major

c. Configure the alarm notification.

Table 6-11 Parameter description

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.
Notification Object	Specifies the object to which alarm notifications will be sent. You can select the account contact or a topic. ● **Account contact** is the mobile number and email address of the registered account. ● Topic: A topic is used to publish messages and subscribe to notifications. If the required topic is unavailable, create one and add subscriptions to it on the SMN console. For details, see **5.2.1 Creating a Topic** and **5.2.2 Adding Subscriptions**. For the HTTP(S) messages, see the *Simple Message Notification User Guide*.
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.
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.

7 Custom Monitoring

The **Custom Monitoring** page displays all custom metrics reported by users. 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. Log in to the management console.
2. Click **Service List** in the upper left corner, and select **Cloud Eye**.
3. In the navigation pane on the left, choose **Custom Monitoring**.
4. 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 section "Adding Monitoring Data" in the *Cloud Eye API Reference*.
5. Locate the row that contains the cloud resource to be viewed, and click **View Metric**.

   On the page displayed, you can view graphs based on raw data collected in **1h**, **3h**, **12h**, **1d**, and **7d**. 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. Log in to the management console.
2. Click **Service List** in the upper left corner, and select **Cloud Eye**.
3. In the navigation pane on the left, choose **Custom Monitoring**.
4. On the **Custom Monitoring** page, locate the target resource and click **Create Alarm Rule** in the **Operation** column.
5. On the **Create Alarm Rule** page, follow the prompts to configure the parameters. For details, see **Table 5-2** and **Table 5-4**.
6. Click **Create**.

8 Event Monitoring

8.1 Introduction to 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. Event monitoring does not depend on the Agent.

Events are key operations on cloud service resources that are stored and monitored by Cloud Eye. You can view events to see operations performed by specific users on specific resources, such as deleting or rebooting an ECS.

Event monitoring is enabled by default. For details, see **8.4 Events Supported by Event Monitoring**.

Event monitoring provides an API for reporting custom events, which helps you collect and report abnormal events or important change events generated by services to Cloud Eye.

For details about how to report custom events, see **Reporting Events**.

8.2 Viewing Event Monitoring Data

Scenarios

This topic describes how to view the event monitoring data.

Procedure

1. Log in to the management console.
2. Click **Service List** in the upper left corner, and select **Cloud Eye**.
3. In the navigation pane on the left, choose **Event Monitoring**.

   On the displayed **Event Monitoring** page, all system events generated in the last 24 hours are displayed by default.

You can also click **1h**, **3h**, **12h**, **1d**, **7d**, or **30d** to view the events generated in different periods.

4. Expand an event, and click **View Event** in the **Operation** column to view details about a specific event.

8.3 Creating an Alarm Rule to Monitor an Event

Scenarios

This topic describes how to create an alarm rule to monitor an event.

Procedure

1. Log in to the management console.
2. Click **Service List** in the upper left corner, and select **Cloud Eye**.
3. In the navigation pane on the left, choose **Event Monitoring**.
4. On the event list page, click **Create Alarm Rule** in the upper right corner.
5. On the **Create Alarm Rule** page, configure the parameters.
   a. Set the alarm rule name and description.

Table 8-1 Parameters for configuring alarm rules

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

   b. Select a monitored object and configure alarm content parameters.

Table 8-2 Parameters for configuring alarm content

Parameter	Description
Resource Type	Specifies the type of the resource the alarm rule is created for.
Dimension	Specifies the metric dimension of the selected resource type. Example value: **System event**
Event Source	Specifies the service the event is generated for. Example value: **Elastic Cloud Server** For a custom event, set **Event Source** to the value of **event_source**.

Parameter	Description
Monitoring Scope	Specifies the monitoring scope for event monitoring. Example value: **All resources**
Method	Specifies the means you use to create the alarm rule.
Event Name	Specifies the instantaneous operations users performed on resources, such as login and logout. For events supported by event monitoring, see **8.4 Events Supported by Event Monitoring**. Example value: **Delete ECS**
Monitored Object	Specifies the object to be monitored. This parameter is mandatory if you set **Monitoring Scope** to **Specific resources**.
Trigger Mode	You can select immediate trigger or accumulative trigger based on the operation severity. Example value: **Immediate trigger**
Alarm Severity	Specifies the alarm severity, which can be **Critical**, **Major**, **Minor**, or **Informational**. Example value: **Major**

c. Configure the alarm notification.

Table 8-3 Parameters for configuring alarm notifications

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.
Notification Object	Specifies the object to which alarm notifications will be sent. You can select the account contact or a topic. ● **Account contact** is the mobile number and email address of the registered account. ● **Topic**: 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 **5.2.1 Creating a Topic** and **5.2.2 Adding Subscriptions**.
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.

Parameter	Description
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**.

8.4 Events Supported by Event Monitoring

Table 8-4 Elastic Cloud Server (ECS)

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
ECS	Restart triggered due to hardware fault	startAutoRecovery	Major	ECSs on a faulty host would be automatically migrated to another properly-running host. During the migration, the ECSs was restarted.	Wait for the event to end and check whether services are affected.	Services may be interrupted.
	Restart completed due to hardware failure	endAutoRecovery	Major	The ECS was recovered after the automatic migration.	This event indicates that the ECS has recovered and been working properly.	None
	Auto recovery timeout (being processed on the backend)	faultAutoRecovery	Major	Migrating the ECS to a normal host timed out.	Migrate services to other ECSs.	Services are interrupted.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	GPU link fault	GPULinkFault	Critical	The GPU of the host on which the ECS is located was faulty or was recovering from a fault.	Deploy service applications in HA mode. After the GPU fault is rectified, check whether services are restored.	Services are interrupted.
	ECS deleted	deleteServer	Major	The ECS was deleted ● on the management console. ● by calling APIs.	Check whether the deletion was performed intentionally by a user.	Services are interrupted.
	ECS restarted	rebootServer	Minor	The ECS was restarted ● on the management console. ● by calling APIs.	Check whether the restart was performed intentionally by a user. ● Deploy service applications in HA mode. ● After the ECS starts up, check whether services recover.	Services are interrupted.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	ECS stopped	stopServer	Minor	The ECS was stopped ● on the management console. ● by calling APIs. **NOTE** The ECS is stopped only after CTS is enabled. For details, see *Cloud Trace Service User Guide*.	● Check whether the restart was performed intentionally by a user. ● Deploy service applications in HA mode. ● After the ECS starts up, check whether services recover.	Services are interrupted.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	NIC deleted	deleteNic	Major	The ECS NIC was deleted ● on the management console. ● by calling APIs.	● Check whether the deletion was performed intentionally by a user. ● Deploy service applications in HA mode. ● After the NIC is deleted, check whether services recover.	Services may be interrupted.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	ECS resized	resizeServer	Minor	The ECS specifications were resized ● on the management console. ● by calling APIs.	● Check whether the operation was performed by a user. ● Deploy service applications in HA mode. ● After the ECS is resized, check whether services have recovered.	Services are interrupted.
	GuestOS restarted	RestartGuestOS	Minor	The guest OS was restarted.	Contact O&M personnel.	Services may be interrupted.
	ECS failure due to abnormal host processes	VMFaultsByHostProcessExceptions	Critical	The processes of the host accommodating the ECS were abnormal.	Contact O&M personnel.	The ECS is faulty.
	Startup failure	faultPowerOn	Major	The ECS failed to start.	Start the ECS again. If the problem persists, contact O&M personnel.	The ECS cannot start.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Host breakdown risk	hostMayCrash	Major	The host where the ECS resides may break down, and the risk cannot be prevented through live migration due to some reasons.	Migrate services running on the ECS first and delete or stop the ECS. Start the ECS only after the O&M personnel eliminate the risk.	The host may break down, causing service interruption.
	Scheduled migration completed	instance_migrate_completed	Major	Scheduled ECS migration is completed.	Wait until the ECSs become available and check whether services are affected.	Services may be interrupted.
	Scheduled migration being executed	instance_migrate_executing	Major	ECSs are being migrated as scheduled.	Wait until the event is complete and check whether services are affected.	Services may be interrupted.
	Scheduled migration canceled	instance_migrate_canceled	Major	Scheduled ECS migration is canceled.	None	None
	Scheduled migration failed	instance_migrate_failed	Major	ECSs failed to be migrated as scheduled.	Contact O&M personnel.	Services are interrupted.
	Scheduled migration to be executed	instance_migrate_scheduled	Major	ECSs will be migrated as scheduled.	Check the impact on services during the execution window.	None

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Scheduled specification modification failed	instance_resize_failed	Major	Specifications failed to be modified as scheduled.	Contact O&M personnel.	Services are interrupted.
	Scheduled specification modification completed	instance_resize_completed	Major	Scheduled specifications modification is completed.	None	None
	Scheduled specification modification being executed	instance_resize_executing	Major	Specifications are being modified as scheduled.	Wait until the event is completed and check whether services are affected.	Services are interrupted.
	Scheduled specification modification canceled	instance_resize_canceled	Major	Scheduled specifications modification is canceled.	None	None
	Scheduled specification modification to be executed	instance_resize_scheduled	Major	Specifications will be modified as scheduled.	Check the impact on services during the execution window.	None
	Scheduled redeployment to be executed	instance_redeploy_scheduled	Major	ECSs will be redeployed on new hosts as scheduled.	Check the impact on services during the execution window.	None
	Scheduled restart to be executed	instance_reboot_scheduled	Major	ECSs will be restarted as scheduled.	Check the impact on services during the execution window.	None

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Scheduled stop to be executed	instance_stop_scheduled	Major	ECSs will be stopped as scheduled as they are affected by underlying hardware or system O&M.	Check the impact on services during the execution window.	None
	Live migration started	liveMigrationStarted	Major	The host where the ECS is located may be faulty. Live migrate the ECS in advance to prevent service interruptions caused by host breakdown.	Wait for the event to end and check whether services are affected.	Services may be interrupted for less than 1s.
	Live migration completed	liveMigrationCompleted	Major	The live migration is complete, and the ECS is running properly.	Check whether services are running properly.	None
	Live migration failure	liveMigrationFailed	Major	An error occurred during the live migration of an ECS.	Check whether services are running properly.	There is a low probability that services are interrupted.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	ECC uncorrectable error alarm generated on GPU SRAM	SRAMUncorrectableEccError	Major	There are ECC uncorrectable errors generated on GPU SRAM.	If services are affected, submit a service ticket.	The GPU hardware may be faulty. As a result, the GPU memory is faulty, and services exit abnormally.
	FPGA link fault	FPGALinkFault	Critical	The FPGA of the host on which the ECS is located was ● faulty. ● recovering from a fault.	Deploy service applications in HA mode. After the FPGA fault is rectified, check whether services are restored.	Services are interrupted.

NOTE

Once a physical host running ECSs breaks down, the ECSs are automatically migrated to a functional physical host. During the migration, the ECSs will be restarted.

Table 8-5 Elastic IP (EIP)

Event Source	Event Name	Event ID	Event Severity
EIP	EIP released	deleteEip	Minor

Table 8-6 Elastic IP and bandwidth

Event Source	Event Name	Event ID	Event Severity
Elastic IP and bandwidth	VPC deleted	deleteVpc	Major
	VPC modified	modifyVpc	Minor
	Subnet deleted	deleteSubnet	Minor
	Subnet modified	modifySubnet	Minor
	Bandwidth modified	modifyBandwidth	Minor
	VPN deleted	deleteVpn	Major
	VPN modified	modifyVpn	Minor

Table 8-7 Elastic Volume Service (EVS)

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
EVS	Update disk	updateVolume	Minor	Update the name and description of an EVS disk.	No further action is required.	None
	Expand disk	extendVolume	Minor	Expand an EVS disk.	No further action is required.	None
	Delete disk	deleteVolume	Major	Delete an EVS disk.	No further action is required.	Deleted disks cannot be recovered.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	QoS upper limit reached	reachQoS	Major	The I/O latency increases as the QoS upper limits of the disk are frequently reached and flow control triggered.	Change the disk type to one with a higher specification.	The current disk may fail to meet service requirements.

Table 8-8 Identity and Access Management (IAM)

Event Source	Event Name	Event ID	Event Severity
IAM	Login	login	Minor
	Logout	logout	Minor
	Password changed	changePassword	Major
	User created	createUser	Minor
	User deleted	deleteUser	Major
	User updated	updateUser	Minor
	User group created	createUserGroup	Minor
	User group deleted	deleteUserGroup	Major
	User group updated	updateUserGroup	Minor
	Identity provider created	createIdentityProvider	Minor
	Identity provider deleted	deleteIdentityProvider	Major
	Identity provider updated	updateIdentityProvider	Minor
	Metadata updated	updateMetadata	Minor
	Security policy updated	updateSecurityPolicies	Major

Event Source	Event Name	Event ID	Event Severity
	Credential added	addCredential	Major
	Credential deleted	deleteCredential	Major
	Project created	createProject	Minor
	Project updated	updateProject	Minor
	Project suspended	suspendProject	Major

Table 8-9 Key Management Service (KMS)

Event Source	Event Name	Event ID	Event Severity
KMS	Key disabled	disableKey	Major
	Key deletion scheduled	scheduleKeyDeletion	Minor
	Grant retired	retireGrant	Major
	Grant revoked	revokeGrant	Major

Table 8-10 Object Storage Service (OBS)

Event Source	Event Name	Event ID	Event Severity
OBS	Bucket deleted	deleteBucket	Major
	Bucket policy deleted	deleteBucketPolicy	Major
	Bucket ACL configured	setBucketAcl	Minor
	Bucket policy configured	setBucketPolicy	Minor

9 Data Dump

9.1 Adding a Dump Task

Scenarios

You can dump cloud service monitoring data to DMS for Kafka in real time and query the metrics on the DMS for Kafka console or using an open-source Kafka client.

NOTE

An account can create a maximum of 20 data dump tasks.

Procedure

1. Log in to the management console.
2. Click **Service List** in the upper left corner, and select **Cloud Eye**.
3. In the navigation pane on the left, choose **Data Dump**.
4. Click **Add Dump Task**.
5. In the **Add Dump Task** dialog box, configure parameters as prompted.

Table 9-1 Dump task parameters

Parameter	Description
Name	Specifies the dump task name. The name can contain 1 to 64 characters and consist of only letters, digits, underscores (_), and hyphens (-). Example value: **dataShareJob-ECSMetric**
Resource Type	Specifies the type of resources monitored by Cloud Eye. Example value: **Elastic Cloud Server**

Parameter	Description
Dimension	Specifies the dimension of the monitored object. For details, see **Metrics** and **Dimension** on the monitoring metric description page. If **All** is selected, all monitored objects of the selected service will be dumped to Kafka. If **ECSs** is selected, metrics of this dimension will be dumped to Kafka. Example value: **All**
Monitoring Scope	The scope can only be **All resources**, indicating that all metrics of the specified monitored object will be dumped to DMS for Kafka.
Resource Type	The type can only be **Distributed Message Service for Kafka**.
Destination	Specifies the Kafka instance and topic where the data is to be dumped. If no Kafka instance or topic is available, see **Buying an Instance** and **Creating a Topic**.

6. Click **Add** after the configuration is complete.

NOTE

You can query the dumped data in Kafka. For details, see **Querying Messages**.

9.2 Modifying, Deleting, Enabling, or Disabling a Dump Task

Scenarios

This topic describes how to modify, disable, enable, or delete dump tasks.

Modifying a Dump Task

1. Log in to the management console.
2. Click **Service List** in the upper left corner, and select **Cloud Eye**.
3. In the navigation pane, choose **Data Dump**.
4. Click **Modify** in the **Operation** column.

   The **Modify Dump Task** page is displayed.
5. Modify the task settings.
6. Click **Modify**.

Disabling a Dump Task

Locate the dump task and click **Disable** in the **Operation** column. In the displayed **Disable Data Dump** dialog box, click **Yes**.

Enabling a Dump Task

Locate a dump task whose status is **Disabled** and click **Enable** in the **Operation** column. In the displayed **Enable Data Dump** dialog box, click **Yes**.

Deleting a Dump Task

Locate the dump task and click **Delete** in the **Operation** column. In the displayed **Delete Data Dump** dialog box, click **Yes**.

10 Auditing Operation Records on Cloud Eye

Cloud Trace Service (CTS) records Cloud Eye operation requests initiated from the cloud service management console or open APIs and responses to the requests. You can query, audit, and trace back the operation records.

10.1 Key Cloud Eye Operations

Table 10-1 Cloud Eye operations that can be recorded by CTS

Operation	Resource Type	Trace Name
Creating an alarm rule	alarm_rule	createAlarmRule
Deleting an alarm rule	alarm_rule	deleteAlarmRule
Disabling an alarm rule	alarm_rule	disableAlarmRule
Enabling an alarm rule	alarm_rule	enableAlarmRule
Modifying an alarm rule	alarm_rule	updateAlarmRule
Updating the alarm status to Alarm	alarm_rule	alarmStatusChangeToAlarm
Updating the alarm status to Insufficient data	alarm_rule	alarmStatusChangeToInsufficientData
Updating the alarm status to OK	alarm_rule	alarmStatusChangeToOk
Creating a custom template	alarm_template	createAlarmTemplate
Deleting a custom template	alarm_template	deleteAlarmTemplate
Modifying a custom template	alarm_template	updateAlarmTemplate

Operation	Resource Type	Trace Name
Creating a dashboard	dashboard	createDashboard
Deleting a dashboard	dashboard	deleteDashboard
Modifying a dashboard	dashboard	updateDashboard
Exporting monitoring data	metric	downloadMetricsReport

10.2 Viewing Cloud Eye Logs

Scenarios

After CTS is enabled, CTS starts recording operations on cloud resources. The CTS management console stores the operation records of the last 7 days.

This section describes how to query or export the last seven days of operation records on the management console.

Procedure

1. Log in to the management console.
2. In the upper left corner, select a region and project.
3. Click **Service List** and choose **Management & Deployment** > **Cloud Trace Service**.
4. In the left navigation pane, choose **Trace List**.
5. Click **Filter** and specify filters as needed. You can query traces by combining the following filters:
   - **Trace Source**, **Resource Type**, and **Search By**

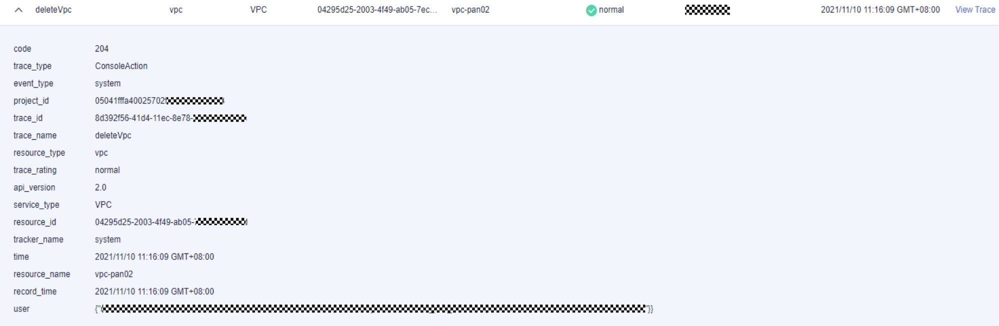
     Select a filter from the drop-down list.

     After you select **Trace name** for **Search By**, you also need to select a trace name.

     After you select **Resource ID** for **Search By**, you also need to select or enter a resource ID.

     After you select **Resource name** for **Search By**, you also need to select or enter a resource name.
   - **Operator**: Select a specific operator.
   - **Trace Status**: Select one of **All trace statuses**, **Normal**, **Warning**, and **Incident**.
   - Time range: You can select start and end time to query traces generated during a time range of the last seven days.
6. Click ⌄ on the left of a trace to expand its details.

Figure 10-1 Expanding trace details

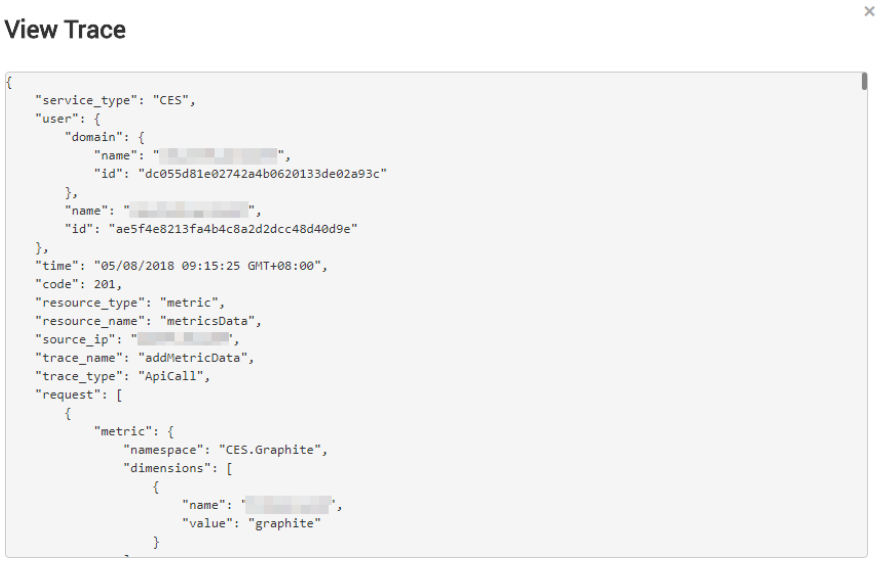


^ deleteVpc vpc VPC 04295d25-2003-4f49-ab05-7ec... vpc-pan02 normal [redacted] 2021/11/10 11:16:09 GMT+08:00 View Trace

code	204
trace_type	ConsoleAction
event_type	system
project_id	05041fffa40025702[redacted]
trace_id	8d392f56-41d4-11ec-8e78-[redacted]
trace_name	deleteVpc
resource_type	vpc
trace_rating	normal
api_version	2.0
service_type	VPC
resource_id	04295d25-2003-4f49-ab05-[redacted]
tracker_name	system
time	2021/11/10 11:16:09 GMT+08:00
resource_name	vpc-pan02
record_time	2021/11/10 11:16:09 GMT+08:00
user	{"[redacted]"}}

7. Click **View Trace** in the **Operation** column. On the displayed **View Trace** dialog box, view details of the trace.

Figure 10-2 View Trace



View Trace

×

```
{
    "service_type": "CES",
    "user": {
        "domain": {
            "name": "[redacted]",
            "id": "dc055d81e02742a4b0620133de02a93c"
        },
        "name": "[redacted]",
        "id": "ae5f4e8213fa4b4c8a2d2dcc48d40d9e"
    },
    "time": "05/08/2018 09:15:25 GMT+08:00",
    "code": 201,
    "resource_type": "metric",
    "resource_name": "metricsData",
    "source_ip": "[redacted]",
    "trace_name": "addMetricData",
    "trace_type": "ApiCall",
    "request": [
        {
            "metric": {
                "namespace": "CES.Graphite",
                "dimensions": [
                    {
                        "name": "[redacted]",
                        "value": "graphite"
                    }
```

11 Permissions Management

11.1 Creating a User and Granting Permissions

IAM enables you to perform a refined management on your Cloud Eye service. It allows you to:

- Create IAM users for employees based on your enterprise's organizational structure. Each IAM user will have their own security credentials for accessing Cloud Eye resources.
- Grant different permissions to IAM users based on their job responsibilities.
- Entrust a account or cloud service to perform efficient O&M on your Cloud Eye resources.

If your account does not require individual IAM users, skip this topic.

This topic describes the procedure for granting permissions (see **Figure 11-1**).

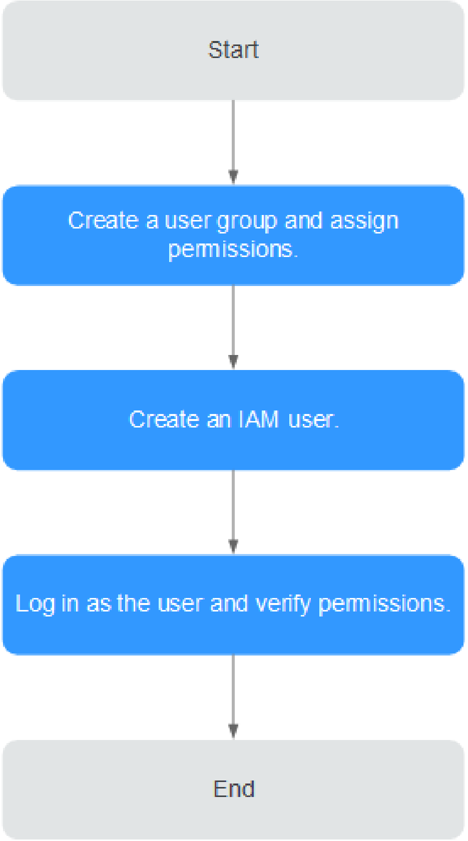
Prerequisites

Before assigning permissions to a user group, you need to understand the Cloud Eye system policies that can be added to the user group and select a policy as required.

For details about the system policies supported by Cloud Eye and the comparison between these policies, see Permissions.

Process Flow

Figure 11-1 Process for granting Cloud Eye permissions


Start
Create a user group and assign permissions.
Create an IAM user.
Log in as the user and verify permissions.
End

1. **Create a user group and assign permissions**.

   Create a user group on the IAM console, and attach the **CES Administrator**, **Tenant Guest**, and **Server Administrator** policies to the group.

   NOTE

   - Cloud Eye is a region-specific service and must be deployed in specific physical regions. Cloud Eye permissions can be assigned and take effect only in specific regions. If you want a permission to take effect for all regions, assign it in all these regions. The global permission does not take effect.
   - The preceding permissions are all Cloud Eye permissions. For more refined Cloud Eye permissions, see Permissions Management.

2. **Create a user and add it to a user group**.

   Create a user on the IAM console and add the user to the group created in **1**.

3. and verify permissions.

   Log in to the Cloud Eye console as the created user, and verify that the user only has the **CES Administrator** permissions.

11.2 Cloud Eye Custom Policies

Custom policies can be created to supplement the system-defined policies of Cloud Eye. For the actions that can be added to custom policies, see Permissions Policies and Supported Actions.

You can create custom policies in either of the following two ways:

- Visual editor: Select cloud services, actions, resources, and request conditions. This does not require knowledge of policy syntax.
- JSON: Edit JSON policies from scratch or based on an existing policy.

For details, see **Creating a Custom Policy**. This topic contains examples of common Cloud Eye custom policies.

Example Custom Policies

- Example 1: Allowing users to modify alarm rules

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Action": [
                "ces:alarms:put"
            ],
            "Effect": "Allow"
        }
    ]
}
```

- Example 2: Denying alarm rule deletion

  A policy with only "Deny" permissions must be used in conjunction with other policies to take effect. If the permissions assigned to a user contain both "Allow" and "Deny", the "Deny" permissions take precedence over the "Allow" permissions.

  The following method can be used if you need to assign permissions of the **CES FullAccess** policy to a user but you want to prevent the user from deleting alarm rules. Create a custom policy for denying alarm rule deletion, and attach both policies to the group the user belongs. Then the user can perform all operations on alarm rules except deleting alarm rules. The following is an example of a deny policy:

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Action": [
                "ces:alarms:delete"
            ],
            "Effect": "Deny"
        }
    ]
}
```

- Example 3: Allowing users to have all operation permissions on alarm rules, including creating, modifying, querying, and deleting alarm rules

  A custom policy can contain the actions of multiple services that are of the global or project-level type. The following is a policy with multiple actions:

```
{
      "Version": "1.1",
      "Statement": [
            {
                  "Action": [
                        "ces:alarms:put",
                        "ces:alarms:create",
                        "ces:alarms:delete"
                  ],
                  "Effect": "Allow"
            }
      ]
}
```

12 Quota Adjustment

What Is Quota?

Quotas can limit the number or amount of resources available to users, such as the maximum number of ECSs or EVS disks that can be created.

If the existing resource quota cannot meet your service requirements, you can apply for a higher quota.

How Do I View My Quotas?

1. Log in to the management console.
2. Click 📍 in the upper left corner and select the desired region and project.
3. In the upper right corner of the page, click 📊 .

   The **Service Quota** page is displayed.
4. View the used and total quota of each type of resources on the displayed page.

   If a quota cannot meet service requirements, apply for a higher quota.

13 Services Interconnected with Cloud Eye

Category	Service	Namespace	Reference
Compute	Elastic Cloud Server	SYS.ECS	**Basic ECS metrics**
	ECS (OS monitoring)	AGT.ECS	**OS monitoring metrics supported by ECSs with the Agent installed**
	Auto Scaling	SYS.AS	**AS metrics**
Storage	Elastic Volume Service	SYS.EVS	**EVS metrics**
	Object Storage Service	SYS.OBS	**OBS metrics**
	Scalable File Service	SYS.SFS	**SFS metrics**
Networking	Elastic IP and bandwidth	SYS.VPC	**VPC metrics**
	Elastic Load Balance	SYS.ELB	**ELB metrics**
	NAT Gateway	SYS.NAT	**NAT Gateway metrics**
Middleware	Distributed Message Service	SYS.DMS	**DMS metrics (Kafka)** **DMS metrics (RabbitMQ)**
	Distributed Cache Service	SYS.DCS	**DCS metrics**

Category	Service	Namespace	Reference
Database	Relational Database Service	SYS.RDS	**RDS for MySQL metrics** **RDS for PostgreSQL metrics** **RDS for SQL Server metrics**
	Document Database Service	SYS.DDS	**DDS metrics**

14 FAQs

14.1 General Consulting

14.1.1 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. Configure a longer rollup period if you want more smoothing to be performed. If more smoothing is performed, the generated data will be more precise, enabling you to predict trends more precisely. Configure 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.

14.1.2 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 14-1 Retention periods for rolled-up data

Rollup Period	Retention Period
5 minutes	6
20 minutes	20 days
1 hour	155 days

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.

14.1.3 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.

14.1.4 How Can I Export Collected Data?

1. On the Cloud Eye console, choose **Cloud Service Monitoring** or **Server Monitoring**.
2. Click **Export Data**.
3. Configure the time range, resource type, dimension, monitored object, and metric.
4. Click **Export**.

NOTE

You can export data for multiple metrics at a time to a CSV file.

- The first row in the exported CSV file displays the username, region, service, instance name, instance ID, metric name, metric data, time, and timestamp. You can view historical monitoring data.
- 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**.

14.2 Server Monitoring

14.2.1 How Can I Quickly Restore the Agent Configuration?

After the Agent is installed, you can configure **AK/SK**, **RegionID**, and **ProjectId** in one-click mode. This saves manual configuration and improves configuration efficiency.

If you are in a region that does not support one-click configuration restoration of the Agent, on the **Server Monitoring** page, select the target ECS and click **Restore Agent Configurations**. In the displayed **Restore Agent Configurations** dialog box, click **One-Click Restore**.

14.2.2 Why Is a BMS with the Agent Installed Displayed in the ECS List on the Server Monitoring Page?

Symptoms

The Agent was installed on a BMS, but the BMS is listed on the **Server Monitoring** > **Elastic Cloud Server** page on the Cloud Eye console.

Possible Causes

The Agent determines whether a server is an ECS or BMS based on the services provided by IP address 169.254.169.254. If the route for this address is changed, the Agent will consider the server to be an ECS by default.

Solution

Manually modify the Agent configuration file by adding BMS identifier **BmsFlag** and setting it to **true**.

- Linux OS: See **6.4.4 (Optional) Manually Configuring the Agent (Linux)**.
- Windows OS: See **6.5.3 (Optional) Manually Configuring the Agent on a Windows Server**.

14.2.3 What OSs Does the Agent Support?

The following table lists OSs compatible with the Agent. More OSs will be supported soon.

NOTICE

Using the OSs or versions that have not been verified may adversely affect your services. Exercise caution when using them.

Table 14-2 and **Table 14-3** lists the supported OSs.

Table 14-2 OS versions supported for ECS

OS (64 bit)	Version
CentOS	6.3, 6.5, 6.8, 6.9, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6
OpenSUSE	13.2, 42.2
Debian	7.5.0, 8.2.0, 8.8.0, 9.0.0
Ubuntu	14.04 server, 16.04 server
EulerOS	2.2, 2.3
SUSE	Enterprise11 SP4, Enterprise12 SP1, Enterprise12 SP2
Fedora	24, 25
Oracle Linux	6.9, 7.4
CoreOS	10.10.5 **NOTE** Cloud-Init cannot be installed automatically. Install it manually in the **/** directory. To query the Agent status, run **systemctl telescoped status**.
Other	Gentoo Linux 13.0, Gentoo Linux 17.0 **NOTE** To query the Agent status, run **rc-service telescoped status**.
Windows	Windows Server 2016 Standard 64-bit Windows Server 2016 Datacenter 64-bit Windows Server 2012 R2 Standard 64-bit Windows Server 2012 R2 Datacenter 64-bit Windows Server 2008 R2 Standard 64-bit Windows Server 2008 R2 Datacenter 64-bit Windows Server 2008 R2 Enterprise 64-bit Windows Server 2008 R2 Web 64-bit

OS (64 bit)	Version
Arm general-computing	CentOS 7.4 64bit with ARM (40 GB) CentOS 7.5 64bit with ARM (40 GB) CentOS 7.6 64bit with ARM (40 GB) EulerOS 2.8 64bit with ARM (40 GB) Fedora 29 64bit with ARM (40 GB) Ubuntu 18.04 64bit with ARM (40 GB)

Table 14-3 OS versions for BMS

OS (64 bit)	Version
SUSE	Enterprise11 SP4, Enterprise12 SP1
CentOS	6.9, 7.2, and 7.3

NOTE

The GPU plug-in supports only Ubuntu 14.04 server, EulerOS 2.2, and CentOS 7.3.

14.2.4 What Statuses Does the Agent Have?

The Agent has the following statuses:

- **Not installed or started**: The Agent is not installed on an ECS or BMS or has been manually stopped.
- **Running**: The Agent is running and can report monitoring data.
- **Faulty**: The Agent failed to send a heartbeat message to Cloud Eye for three consecutive minutes. In this case,
  - The account is in arrears.
  - If the Agent process is faulty, restart it by following the instructions provided in **6.7 Managing the Agent**. If the restart fails, related files have been deleted by mistake. In this case, reinstall the Agent.
  - It may be that the Agent is incorrectly configured. Check whether the DNS server address is correct. If it is, check the Agent configurations by referring to **6.4.1 Modifying the DNS Server Address and Adding Security Group Rules (Linux)** and **6.4.4 (Optional) Manually Configuring the Agent (Linux)**.
  - Locate the cause in log **/usr/local/telescope/log/common.log**.
- **Configuration error**
  - No agency has been configured for the ECS or BMS.
  - Permissions of the current agency are abnormal.
  - The current agency is invalid.
  - Security group rules of the default NIC are incorrectly configured.

  - The DNS is incorrectly configured.

- **Stopped**: The Agent has been manually stopped. For details about how to start the Agent, see **6.7 Managing the Agent**.

14.2.5 What Should I Do If the Monitoring Period Is Interrupted or the Agent Status Keeps Changing?

Symptoms

The Agent is overloaded if you see either of the following symptoms:

- On the **Server Monitoring** page of the Cloud Eye console, the Agent status frequently toggles between **Running** and **Faulty**.
- The time period in the monitoring panel is discontinuous.

Possible Causes

To prevent other services from being affected, Cloud Eye uses a circuit-breaker to automatically stop the Agent process if it is consuming too many CPU or memory resources on the server. After the Agent process is stopped, no monitoring data is reported.

Circuit-Breaker Principles

By default, once per minute, the system checks whether the CPU usage of the Agent process is exceeding 30% or whether the memory usage is exceeding 700 MB (the tier-2 threshold) every minute. If the tier-2 threshold is exceeded, the Agent process exits. If the tier-2 threshold is not exceeded, Cloud Eye checks whether the CPU usage is exceeding 10% or whether the memory usage is exceeding 200 MB (the tier-1 threshold). If the tier-1 threshold is exceeded for three consecutive times, the Agent process exits, and the exit is logged.

After the Agent exits, the daemon process automatically starts the Agent process and checks the exit record. If there are three consecutive exit records, the Agent will hibernate for 20 minutes, during which monitoring data will not be collected.

When too many disks are attached to a server, the CPU or memory usage of the Agent process will become high. You can configure the tier-1 and tier-2 thresholds referring to **Procedure** to trigger circuit-breaker according to actual resource usages.

Procedure

1. Use the **root** account to log in to the ECS or BMS for which the Agent does not report data.
2. Go to the Agent installation path **bin**:

   cd /usr/local/telescope/bin

   NOTE

   In a Windows OS, the directory is **telescope_windows_amd64\bin**.
3. Modify configuration file **conf.json**.

a. Open **conf.json**:

   vi conf.json

b. Add the parameters listed in **Table 14-4** to the **conf.json** file.

Table 14-4 Parameters

Parameter	Description
cpu_first_pct_threshold	Specifies the tier-1 threshold for CPU usage. If the CPU usage of the Agent process is about 20%, set this parameter to **35**. Unit: percent (%) **NOTE** To query the CPU usage and memory usage of the Agent process, use the following method: ● Linux **top -p** *telescope PID* ● Windows View the details of the Agent process in **Task Manager**.
memory_first_threshold	Specifies the tier-1 threshold for memory usage. If the Agent used up about 100 MB of memory, set this parameter to **314572800** (300 MB). Unit: bytes
cpu_second_pct_threshold	Specifies the tier-2 threshold for CPU usage. If the CPU usage of the Agent process is about 20%, set this parameter to **55**. Unit: percent (%)
memory_second_threshold	Specifies the tier-2 threshold for memory usage. If the Agent process used up about 100 MB memory, set this parameter to **734003200** (700 MB). Unit: bytes

c. Run the following command to save and exit the **conf.json** file:

   :wq

4. Run the following command to restart the Agent:

   /usr/local/telescope/telescoped restart

   NOTE

   For Windows, in the directory where the Agent installation package is stored, double-click the **shutdown.bat** script to stop the Agent, and execute the **start.bat** script to start the Agent.

14.2.6 What Should I Do If the Service Port Is Used by the Agent?

Cloud Eye Agent uses HTTP requests to report data. Any port in the range obtained from path **/proc/sys/net/ipv4/ip_local_port_range** may be occupied. If any service port is used by the Agent, you can modify path **/proc/sys/net/ipv4/ip_local_port_range** and restart the Agent to solve the problem.

Procedure

1. Log in an ECS or BMS as user **root**.
2. Open the **sysctl.conf** file:

   vim /etc/sysctl.conf
3. (Permanent change) Add new ports to the **sysctl.conf** file:

   net.ipv4.ip_local_port_range=49152 65536
4. Make the modification take effect:

   sysctl -p /etc/sysctl.conf

   NOTE

   - The permanent change still takes effect after the ECS or BMS is restarted.
   - For temporary modification (which expires after the ECS or BMS is restarted), run **# echo 49152 65536 > /proc/sys/net/ipv4/ip_local_port_range**.
5. Run the following command to restart the Agent:

   /usr/local/telescope/telescoped restart

   NOTE

   For Windows, in the directory where the Agent installation package is stored, double-click the **shutdown.bat** script to stop the Agent, and execute the **start.bat** script to start the Agent.

14.2.7 How Can I Create an Agency?

Scenarios

Create an agency so that the Agent can automatically obtain the AK and SK. This frees you from exposing the AK or SK in the configuration file.

Procedure

1. Log in to the management console.
2. Click 📍 in the upper left to select a region and project.
3. Click **Service List** in the upper left corner, and select **Identity and Access Management**.
4. In the navigation pane on the left, choose **Agencies**. In the upper right corner, click **Create Agency**.
5. Configure the parameters by referring to **Table 14-5**.

Table 14-5 Creating an agency

Parameter	Description
Agency Name	Specifies the name of the agency. Example: **CESAgentAutoConfigAgency**

Parameter	Description
Agency Type	Select **Cloud service**.
Cloud Service	Select **Elastic Cloud Server (ECS) and Bare Metal Server (BMS)** from the drop-down list.
Validity Period	Select **Unlimited**.
Description	(Optional) Provides supplementary information about the agency.

6. Click **OK**.

Agency Configuration

If no agency is configured for a server, perform the following operations to configure an agency:

1. Log in to the management console.
2. Choose **Service List** > **Computing** > **Elastic Cloud Server**.

   NOTE

   If you purchase a BMS, choose **Computing** > **Bare Metal Server**.
3. Click the name of the target ECS on which the Agent is installed.
4. For **Agency**, select the agency created in 5 and click the green tick to make the agency take effect.

14.2.8 What Can't I Create Another Agency?

It may be that your quota is used up. If this is the case, you can delete unneeded agencies first or increase the agency quota. Then you can use the agency to restore the Agent configuration.

14.2.9 What Should I Do If Agency CESAgentAutoConfigAgency Failed to Be Automatically Created?

When the Agent configuration is being restored, agency **CESAgentAutoConfigAgency** will be automatically created, but if you have created such an agency but not for the ECS or BMS service, agency **CESAgentAutoConfigAgency** will fail to be automatically created.

You can delete the agency you created and then restore the Agent configuration, or manually configure the agency based on **14.2.7 How Can I Create an Agency?**

14.2.10 What Can I Do If Agency CESAgentAutoConfigAgency Is Invalid?

An invalid agency is an agency that has expired. If you set the agency **Validity Period** to **Unlimited**, the agency will become valid again. For details, see **14.2.7 How Can I Create an Agency?**

14.2.11 Will the Agent Affect the Server Performance?

The Agent uses very minimal system resources and it has almost no impact on the server performance.

- On an ECS, the Agent uses less than 5% of the CPU capacity and less than 100 MB of memory.
- On a BMS, the Agent uses less than 5% of the CPU capacity and less than 100 MB of memory.

14.2.12 What Should I Do If the Agent Status Is Faulty?

The OS monitoring Agent sends a heartbeat message to Cloud Eye every minute. If Cloud Eye does not receive any heartbeat messages for three consecutive minutes, **Agent Status** is **Faulty**.

It may because:

- Your account is in arrears.
- If the Agent process is faulty, restart it by following the instructions provided in **6.7 Managing the Agent**. If the restart fails, related files have been deleted accidentally. In this case, reinstall the Agent.
- The server time is inconsistent with the local standard time.
- The log path varies depending on the Agent version.

  The log paths are as follows:

  - Linux:

    New Agent version: **/usr/local/uniagent/extension/install/telescope/log/ces.log**

    Early Agent version: **/usr/local/telescope/log/ces.log**

  - Windows:

    New version: **C:\Program Files\uniagent\extension\install\telescope\log\ces.log**

    Earlier version: **C:\Program Files\telescope\log\ces.log**

It may be that the Agent is incorrectly configured. Check whether the DNS server address is correct. If it is, check the Agent configurations by referring to **6.4.1 Modifying the DNS Server Address and Adding Security Group Rules (Linux)** and **6.4.4 (Optional) Manually Configuring the Agent (Linux)**.

Locate the cause in log **/usr/local/telescope/log/common.log**.

14.3 Alarm Notifications or False Alarms

14.3.1 What Is an Alarm Notification? How Many Types of Alarm Notifications Are There?

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

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

Cloud Eye can:

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

14.3.2 What Alarm Status Does Cloud Eye Support?

Alarm, **Resolved**, **Insufficient data**, **Triggered**, and **Expired** are supported.

- Alarm: The metric value reached the alarm threshold, and an alarm has been triggered but not cleared for the resource.
- Resolved: The metric value went back to the normal range, and the resource alarm was cleared.
- 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.
- Triggered: An event configured in the alarm policy triggered an alarm.
- Expired: The monitored resources or alarm policies in the alarm rule were adjusted, so the original alarm record status expired.

14.3.3 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.

14.3.4 When Will an "Insufficient data" Alarm Be Triggered?

When monitoring data of a metric is not reported to Cloud Eye for three consecutive hours, the alarm rule status changes to **Insufficient data**.

In special cases, if monitoring data of a metric is reported at an interval longer than three hours and no monitoring data is reported for three consecutive intervals, the alarm rule status also changes to **Insufficient data**.

14.3.5 How Can I Change the Mobile Number and Email Address for Receiving Alarm Notifications?

Alarm notifications can be sent to the account contact or SMN topic subscribers configured in alarm rules.

You can change mobile numbers and email addresses of the account contact or SMN topic subscribers.

Account Contact

If you set **Notification Object** to **Account contact**, alarm notifications will be sent to the mobile number and email address registered for your account.

You can update them on the **My Account** page by performing the following steps:

1. Log in to the management console.
2. Hover your mouse over the username in the upper right corner and select **Basic Information**.

   The **My Account** page is displayed.
3. Click **Edit** next to the mobile number or email address.
4. Change the mobile number or email address as prompted.

SMN Topic Subscribers

If you set **Notification Object** to an SMN topic, perform the following steps to change the mobile numbers:

1. Log in to the management console.
2. In the service list, select **Simple Message Notification**.
3. In the navigation pane on the left, choose **Topics**.
4. Click the name of the target topic.
5. Add subscription endpoints to or delete subscription endpoints from the topic.

14.3.6 How Can an IAM User Receive Alarm Notifications?

To send alarm notifications to an IAM user of your account, subscribe the contact information to an SMN topic and select the topic when you create alarm rules. For details, see **5.2.1 Creating a Topic** and **5.2.2 Adding Subscriptions**.

14.3.7 Why Did I Receive a Bandwidth Overflow Notification While There Being No Bandwidth Overflow Record in the Monitoring Data?

You may have configured Cloud Eye to trigger alarm notifications immediately when the bandwidth overflow occurs. However, if the average value for the last 5 minutes falls under the preset threshold, no alarm will be recorded in the system.

14.4 Monitored Data Exceptions

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

Possible causes are as follows:

- The cloud service is not interconnected with Cloud Eye. To check whether a cloud service has been interconnected with Cloud Eye, see **13 Services Interconnected with Cloud Eye**.

- The collection and monitoring frequency for each service that has been interconnected with Cloud Eye is not the same. 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 stopped.
- It has been less than 10 minutes since the resource was purchased.

14.4.2 Why I Cannot See the Monitoring Data on the Cloud Eye Console After Purchasing Cloud Service Resources?

The cloud platform is working to interconnect Cloud Eye with more cloud services. Before the interconnection is complete, you cannot view the resource monitoring data of the cloud services that have not been interconnected with Cloud Eye. If you want to check the resource monitoring data of the cloud services you purchased, you need to first check whether the cloud services have been interconnected with Cloud Eye.

If the services have been interconnected with Cloud Eye, wait for a period of time, because the frequencies of each service to collect and report data to Cloud Eye are different. You can view the resource monitoring graph after Cloud Eye collects the first piece of monitoring data.

14.4.3 Why Is OS Monitoring Data Not Displayed or Not Displayed Immediately After the Agent Is Installed and Configured on a server?

After you install the Agent successfully, choose **Server Monitoring**, and enable **Monitoring Status**, you need to wait for 2 minutes before you can see the monitoring data on the Cloud Eye console.

If **Agent Status** is **Running**, **Monitoring Status** is enabled, and you cannot see the OS monitoring data after waiting for 5 minutes, check whether the ECS or BMS time and the console client time are consistent.

The Agent reports data at the ECS or BMS local time. The management console delivers requests at the browser time of the user client. If the local time of the OS is inconsistent with the browser time, no OS monitoring data will be displayed on the Cloud Eye console.

14.4.4 Why Is Basic Monitoring Data Inconsistent with the Data Monitored by the OS?

Symptoms

CPU Usage under **Basic Monitoring** is close to 100%, which is different from the CPU usage monitored by the OS (50%).

Possible Causes

1. If you set **idle** to **poll** in the guest operating system (guest OS), the guest OS will enter the **polling** state when idling. In this case, the guest OS consumes compute resources and does not proactively release CPU resources. As a result, the CPU usage is abnormal.
2. If you set **idle** to **mwait** in the guest OS for a HANA ECS, the guest OS will enter the **mwait** state when idling. In this case, the guest OS consumes fewer compute resources compared with it does when **idle** is **set** to **poll**. In addition, it still does not proactively release CPU resources. As a result, the CPU usage is abnormal.

NOTE

- You can run the **cat /proc/cmdline** command to check whether **idle** is set to **poll** for your guest OS.
- If you want to check whether **idle** is set to **mwait** for your guest OS, contact technical support.
- SAP High-Performance Analytic Appliance (HANA) is a high-performance real-time data computing platform based on memory computing technologies. The cloud platform provides high-performance IaaS services that comply with SAP HANA requirements. These services help you rapidly request for SAP HANA resources (such as applying for HANA ECSs and public IP addresses) and install and configure SAP HANA, therefore improving your operation efficiency, reducing operation costs, and enhancing your experience.

  HANA ECSs are dedicated for SAP HANA. If you have deployed SAP HANA on cloud servers, you can purchase HANA ECSs.

Solution

Install and configure the Agent to view OS metrics.

14.4.5 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.

14.4.6 Why Is the Metric Collection Point Lost During a Certain Period of Time?

There may be no monitoring data for a certain period of time, which can be perfectly normal. The Agent collects metrics based on the time for the server OS, and sometimes time synchronization leads to server time changes, which can result in the appearance of periods of time when no data was collected.

14.4.7 Why Are Memory Usage, Disk Usage, Inband Incoming Rate, and Inband Outgoing Rate Not Displayed for an ECS?

Your ECS may run a Linux which does not support the four metrics by default.

To learn more about basic metrics supported by different OSs, see **Basic ECS Metrics**.

To monitor the memory usage, disk usage, inband incoming rate, and inband outgoing rate, see **6.2 Agent Installation and Configuration**.

14.4.8 What Are the Impacts on ECS Metrics If UVP VMTools Is Not Installed on ECSs?

If UVP VMTools is 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 lowers the CPU monitoring accuracy.

To learn more about ECS metrics supported by Cloud Eye, see **Basic ECS Metrics**.

14.5 User Permissions

14.5.1 What Should I Do If the IAM User Permissions Are Abnormal?

To use server monitoring, IAM users in a user group must have the **Security Administrator** permissions. If they do not have the permissions, a message indicating abnormal permissions is displayed. Contact the account administrator to grant the permissions.

A Change History

Released On	Description
2022-04-12	This issue is the first official release.