Cloud Eye

User Guide

Issue	01
Date	2024-04-03

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

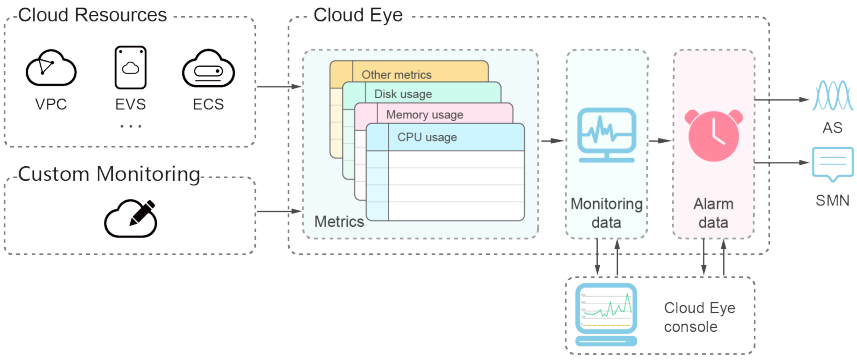
Contents

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 **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 SMS messages, 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.
- 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.

1.2 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 SMS messages, 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 Service Pricing

Cloud Eye basic functions, such as viewing dashboards, creating alarm rules, and adding monitoring items, are free of charge. Cloud Eye may interconnect with other cloud services to provide you with value-added services such as monitoring data file dump and alarm notification. These value-added services may incur extra fees, which are settled by services that provide such functions.

Generally, the value-added service fee is low. Therefore, you are advised to use them as required.

The following are some value-added services:

- Sending alarm notifications: Simple Message Notification (SMN) is required. When the status change of the cloud service triggers the threshold set in the alarm rule, Cloud Eye sends emails or text messages to users, or HTTP/HTTPS messages to servers.

Value-added services are charged as follows:

- Simple Message Notification (SMN)

  SMN is billed based on the usage of SMS, emails, or HTTP/HTTPS requests.

1.5 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, SMS messages, 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.

1.6 Constraints

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

Table 1-1 Resources and their default quotas

Resource	Default Quota
Alarm rules that can be created	1,000
Custom alarm templates that can be created	200
Alarm rules that can be added to an alarm template	20
Dashboards that can be created	10
Graphs that can be added to a dashboard	50
Time that the alarm history can be kept	7 days
Objects that can be selected for monitoring when creating an alarm rule	5,000

Resource	Default Quota
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.
Resource groups that can be created	1,000

1.7 Region and AZ

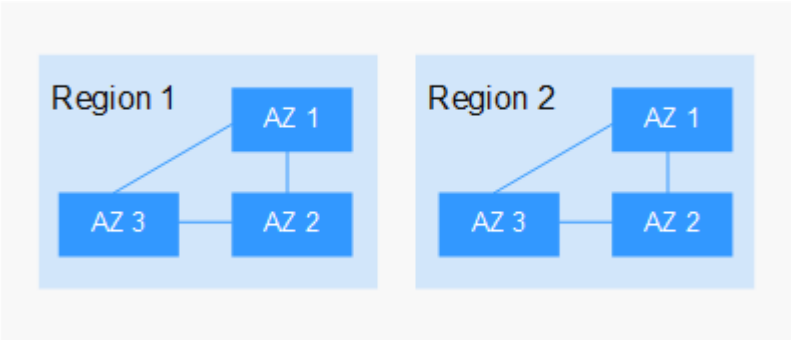
Concept

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

- A region is a physical data center, which is completely isolated to improve fault tolerance and stability. The region that is selected during resource creation cannot be changed after the resource is created.
- An AZ is a physical location where resources use independent power supplies and networks. A region contains one or more AZs that are physically isolated but interconnected through internal networks. Because AZs are isolated from each other, any fault that occurs in one AZ will not affect others.

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

Figure 1-2 Regions and AZs



Selecting a Region

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

Selecting an AZ

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

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

Regions and Endpoints

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

1.8 Permissions

If you need to assign different permissions to employees in your enterprise to access your Cloud Eye resources, you can use IAM to manage fine-grained permissions. IAM provides identity authentication, permissions management, and access control, helping you secure access to your cloud service resources.

With IAM, you can use your account to create IAM users, and assign permissions to the users to control their access to specific resources. For example, some software developers in your enterprise need to use Cloud Eye resources but should not be allowed to delete the resources or perform any other high-risk operations. In this scenario, you can create IAM users for the software developers and grant them only the permissions required for using Cloud Eye resources.

If your account does not require individual IAM users for permissions management, skip this section.

IAM is a free service. You pay only for the resources in your account. For more information about IAM, see **IAM Service Overview**.

Cloud Eye Permissions

By default, IAM users do not have permissions. To assign permissions to IAM users, add them to one or more groups, and attach policies or roles to these groups. The users then inherit permissions from the groups to which the users belong, and can perform specific operations on cloud services.

Cloud Eye is a project-level service deployed and accessed in specific physical regions. Therefore, Cloud Eye permissions are assigned to users in specific regions (such as) and only take effect in these regions. If you want the permissions to take effect in all regions, you need to assign the permissions to users in each region. When users access Cloud Eye, they need to switch to a region where they have been authorized to use this service.

You can grant users permissions by using roles and policies.

- Roles: A type of coarse-grained authorization mechanism that defines permissions related to user responsibilities. This mechanism provides only a limited number of service-level roles for authorization. When using roles to grant permissions, you also need to assign other roles on which the permissions depend to take effect. However, roles are not an ideal choice for fine-grained authorization and secure access control.
- Policies: A type of fine-grained authorization mechanism that defines permissions required to perform operations on specific cloud resources under certain conditions. This mechanism allows for more flexible policy-based authorization, meeting requirements for secure access control. For example, you can grant ECS users only the permissions for managing a certain type of ECSs.

  Most policies define permissions based on APIs. For the API actions supported by Cloud Eye, see **Permissions Policies and Supported Actions**.

Table 1-2 lists the system-defined policies supported by Cloud Eye.

Table 1-2 System policies

Policy Name	Description	Dependency	Type
CES Administrator	Administrator permissions for Cloud Eye	Dependent on the **Tenant Guest** and **Server Administrator** policies. **Tenant Guest**: a global policy, which must be assigned in the Global project	System-defined policy
CES FullAccess	Administrator permissions for Cloud Eye. Users granted these permissions can perform all operations on Cloud Eye.	The Cloud Eye monitoring function involves querying resources of other cloud services, which requires the cloud services to support fine-grained authorization. .	System-defined policy
CES ReadOnlyAccess	Read-only permissions for Cloud Eye. Users granted these permissions can only view Cloud Eye data.	The Cloud Eye monitoring function involves querying resources of other cloud services, which requires the cloud services to support fine-grained authorization. .	System-defined policy

Table 1-3 lists common operations supported by the Cloud Eye system policy.

Table 1-3 Common operations supported by the Cloud Eye system policy

Feature	Operation	CES Administrator (The Tenant Guest policy must be added at the same time.)	Tenant Guest	CES FullAccess	CES ReadOnlyAccess
Monitoring Overview	Viewing monitoring overview	√	√	√	√
	Viewing full screen monitoring	√	√	√	√
Dashboards	Creating a dashboard	√	×	√	×
	Viewing full screen monitoring	√	√	√	√
	Querying a dashboard	√	√	√	√
	Deleting a dashboard	√	×	√	×
	Adding a graph	√	×	√	×
	Viewing a graph	√	√	√	√
	Modifying a graph	√	×	√	×
	Deleting a graph	√	×	√	×
	Adjusting the position of a graph	√	×	√	×
Resource Groups	Creating a resource group	√	×	√	×
	Viewing the resource group list	√	√	√	√
	Viewing resource groups (Resource Overview)	√	√	√	√

Feature	Operation	CES Administrator (The Tenant Guest policy must be added at the same time.)	Tenant Guest	CES FullAccess	CES ReadOnlyAccess
	Viewing resource groups (Alarm Rules)	√	√	√	√
	Viewing resource groups (Alarm Records)	√	√	√	√
	Modifying a resource group	√	×	√	×
	Deleting a resource group	√	×	√	×
Alarm Rules	Creating an alarm rule	√	×	√	×
	Modifying an alarm rule	√	×	√	×
	Enabling an alarm rule	√	×	√	×
	Disabling an alarm rule	√	×	√	×
	Deleting an alarm rule	√	×	√	×
	Querying the alarm rule list	√	√	√	√
	Viewing details of an alarm rule	√	√	√	√
	Viewing a graph	√	√	√	√
Alarm Records	Viewing alarm records	√	√	√	√
Alarm Templates	Viewing a default template	√	√	√	√
	Viewing a custom template	√	√	√	√
	Creating a custom template	√	×	√	×

Feature	Operation	CES Administrator (The Tenant Guest policy must be added at the same time.)	Tenant Guest	CES FullAccess	CES ReadOnlyAccess
	Modifying a custom template	√	×	√	×
	Deleting a custom template	√	×	√	×
Server Monitoring	Viewing the server list	√	√	√	√
	Viewing server monitoring metrics	√	√	√	√
	Installing the Agent	√ (You must have the **ECS FullAccess** permission.)	×	√ (You must have the **ECS FullAccess** permission.)	×
	Restoring the Agent configurations	√ (You must have the **Security Administrator** and **ECS FullAccess** permissions.)	×	√ (You must have the **Security Administrator** and **ECS FullAccess** permissions.)	×

Feature	Operation	CES Administrator (The Tenant Guest policy must be added at the same time.)	Tenant Guest	CES FullAccess	CES ReadOnlyAccess
	Uninstalling the Agent	√ (You must have the **ECS FullAccess** permission.)	×	√ (You must have the **ECS FullAccess** permission.)	×
	Configuring process monitoring	√	×	√	×
	Configuring monitoring for a process	√	×	√	×
Cloud Service Monitoring	Viewing the cloud service list	√	√	√ (Cloud services need to support fine-grained authorization.)	√ (Cloud services need to support fine-grained authorization.)
	Querying cloud service metrics	√	√	√	√
Custom Monitoring	Adding custom monitoring data	√	×	√	×
	Viewing the custom monitoring list	√	√	√	√
	Viewing custom monitoring data	√	√	√	√
Event Monitoring	Adding a custom event	√	×	√	×

Feature	Operation	CES Administrator (The Tenant Guest policy must be added at the same time.)	Tenant Guest	CES FullAccess	CES ReadOnlyAccess
	Viewing the event list	√	√	√	√
	Viewing details of an event	√	√	√	√
Data Dumping to DMS Kafka	Creating a dump task	√	×	√	×
	Querying data dumping tasks	√	√	√	√
	Querying a specified data dump task	√	√	√	√
	Modifying a data dump task	√	×	√	×
	Starting a data dump task	√	×	√	×
	Stopping a data dump task	√	×	√	×
	Deleting a data dump task	√	×	√	×
Others	Configuring data storage	√ (You must have the **Tenant Administrator** permission.)	×	√ (You must have the **OBS Bucket Viewer** permission.)	×
	Exporting monitoring data	√	×	√	×
	Sending an alarm notification	√	×	√	×

Helpful Links

- **IAM Service Overview**
- For details about how to create a user group and user and grant the **CES Administrator** permissions, see **Creating a User and Granting Permissions**.
- For the actions supported by fine-grained policies, see section "Permissions Policies and Supported Actions" in *Cloud Eye API Reference*.

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.

NOTE

To view ECS monitoring data, you need to purchase an ECS. For details, see **Creating an ECS**.

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.

NOTE

To view network monitoring data, you need to apply for a VPC and bind an EIP or bandwidth. For details, see **Creating a VPC**.

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.

NOTE

To view storage monitoring data, you need to purchase an EVS disk. For details, see **Create an EVS Disk**.

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.

NOTE

For services that support enterprise projects, the system displays, by default, the host list of the enterprise projects on which you have permissions.

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.

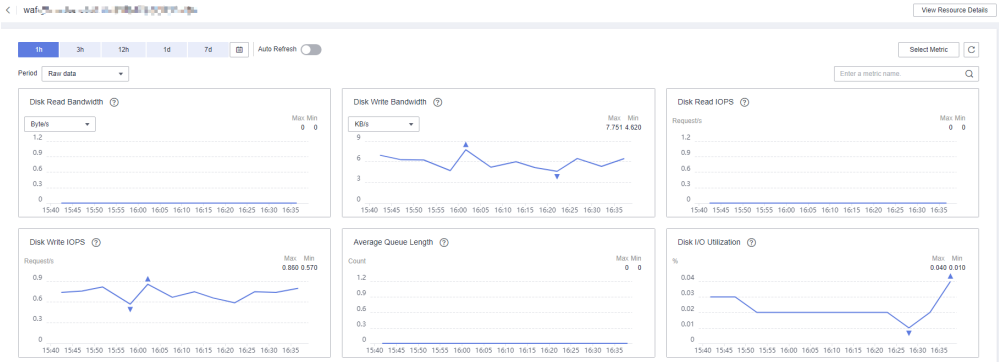
   The cloud service page is displayed.
4. Locate the row that contains the cloud service resource you want to monitor and click **View Graph** in the **Operation** column.

   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.

Figure 2-1 Viewing graphs



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. Near the top right corner of the page, click **Select Metric**.

   The **Select Metric** dialog box is displayed.

   Select at least one metric. Drag and drop the selected metrics at desired locations to sort them. This helps you customize metrics to be viewed.

6. 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 **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.

Figure 2-2 Disk Write IOPS

7. In the upper right corner of the monitoring view, click  to create an alarm rule for a metric.
8. To export data, click **Export Data** on the **Cloud Service Monitoring** page, configure parameters as prompted, and click **Export**. For details, see **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 **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	The monitoring scope of an alarm rule can be **All resources**, **Resource groups**, or **Specified resources**. **NOTE** • If you select **All resources**, an alarm notification will be sent when any instance meets an alarm policy, and existing alarm rules will be automatically applied for newly purchased resources. • 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.	All resources
Group	This parameter is mandatory when **Monitoring Scope** is set to **Resource groups**.	N/A
Method	You can select an associated template, use an existing template or create a custom template as required. **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 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 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 **Creating a Topic** and **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. Configure the enterprise project.

Figure 2-3 Advanced Settings

Table 2-4 Name and **Description**

Parameter	Description
Enterprise Project	Specifies the enterprise project that the alarm rule belongs to. Only users with the enterprise project permissions can manage the alarm rule. For details about how to create an enterprise project, see **Creating an Enterprise Project**.

e. 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 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.
   - **Name**: Enter a maximum of 128 characters. Only letters, digits, hyphens (-), and underscores (_) are allowed.
   - **Enterprise Project**: If you associate a dashboard with an enterprise project, only users who have the permissions of the enterprise project can manage the dashboard.

     NOTE

     The enterprise project feature is available only in some regions.
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 50 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**
Enterprise Project	Specifies the enterprise project associated with the graph. You can view the monitoring data on the graph only when you have the enterprise project permission.
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 50 monitored objects. You can select a maximum of 50 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.

   On the enlarged graph, you can **Customizing a Period to View the Monitoring Graph** or **Selecting Monitoring Objects and Viewing Metrics**.

   Figure 3-1 Viewing graphs

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.

  Figure 3-2 Customizing a period

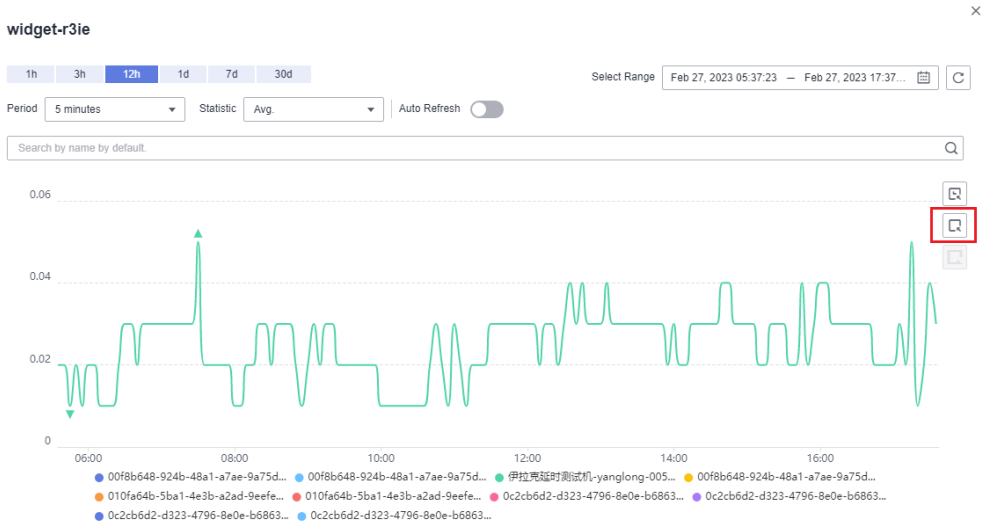
- To go back to the default graph, click the third icon on the right.

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.

Figure 3-3 Selecting the object to be monitored



- 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.

Resource Groups supports enterprise projects. If a resource group is associated with an enterprise project, only users who have the permission of the enterprise project can view and manage the resource group.

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.

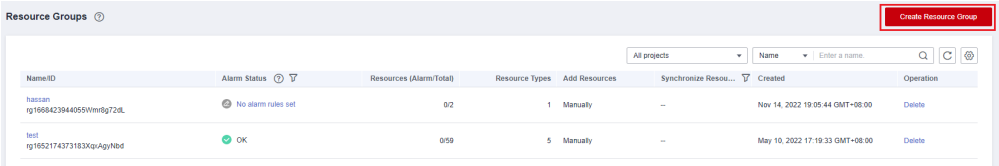
Restrictions

- 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**.

Figure 4-1 Creating a resource group



6. Enter the group name and select an enterprise project.

   You are advised to associate the resource group with an enterprise project. Only users who have permission of the enterprise project can view and manage the associated resource group. In this way, permission assignment is more reasonable and refined. For details about how to create an enterprise project, see **Creating an Enterprise Project**.

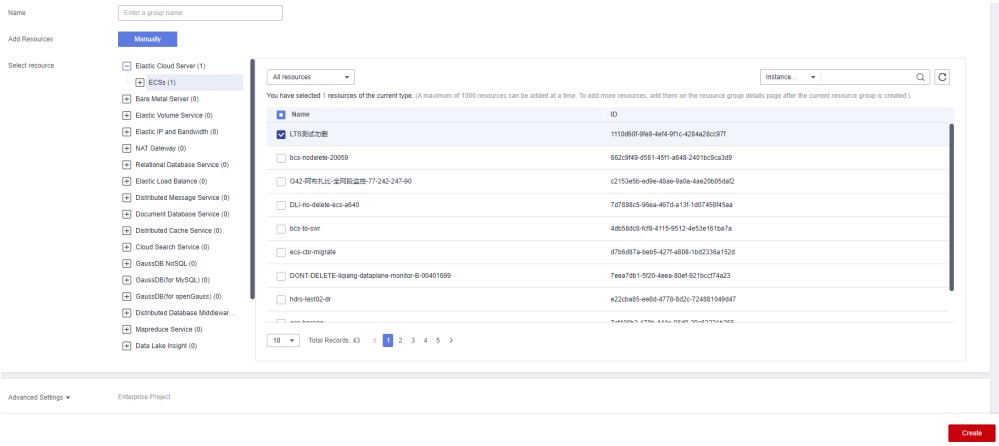
   NOTE

   The enterprise project feature is available only in some regions.

7. Select the target cloud service resources and configure **Associate Enterprise Project**.

   You are advised to associate an enterprise project. After an enterprise project is associated, resources added to or deleted from the enterprise project are automatically added to or deleted from the resource group. If resources are frequently added or deleted, you can improve the efficiency of maintaining resource groups.

Figure 4-2 Selecting 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**.
Enterprise Project	Specifies the name of the enterprise project that has the resource group permission.
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.
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.

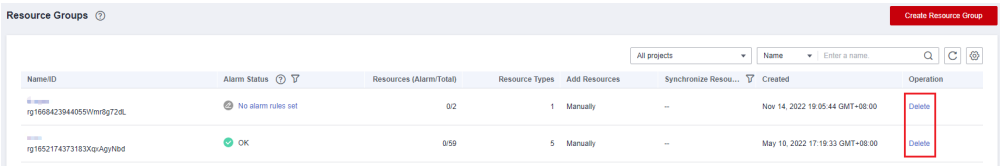
4.4 Managing Resource Groups

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.

Figure 4-3 Deleting a resource group



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 SMS messages, 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.

The Alarm Rules function supports enterprise projects. If an alarm rule is associated with an enterprise project, only users who have the permission of the enterprise project can view and manage the alarm rule.

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.

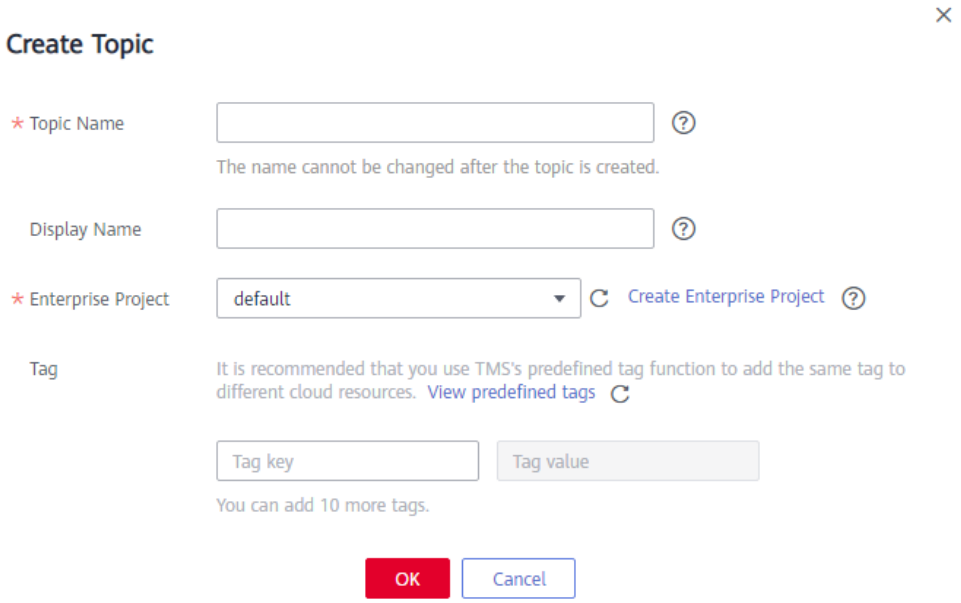
2. In the upper left corner, select a region and project.
3. In the service list, select **Simple Message Notification**.

   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.

Figure 5-1 Creating a topic



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**.

Parameter	Description
Enterprise Project	Centrally manages cloud resources and members by project.
Tag	Tags identify cloud resources so that they can be categorized easily and searched quickly. • For each resource, each tag key must be unique, and each tag key can have only one tag value. • A tag key can contain a maximum of 36 characters, including digits, letters, underscores (_), and hyphens (-). • A tag value can contain a maximum of 43 characters, including digits, letters, underscores (_), periods (.), and hyphens (-). • You can add up to 20 tags to a topic.

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.

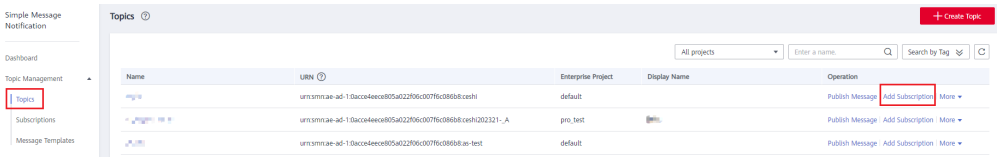
Adding Subscriptions

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**.

   The **Topics** page is displayed.

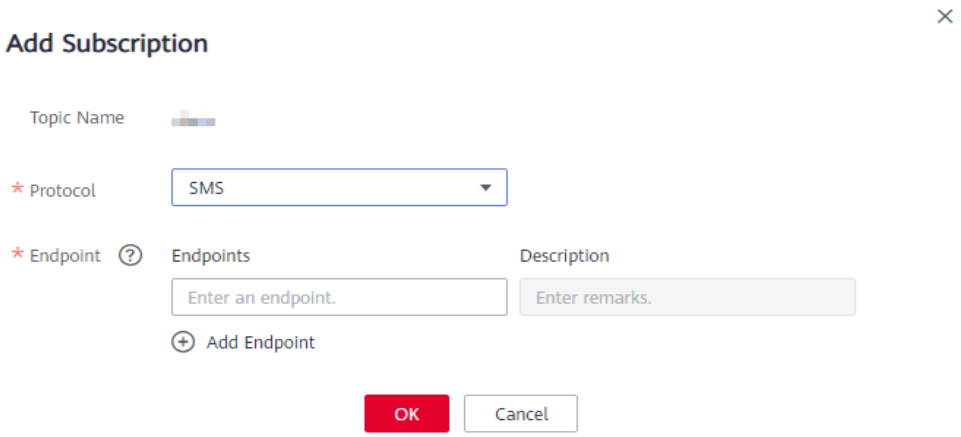
Figure 5-2 Topics



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.

   Figure 5-3 Adding Subscription



5. Specify the subscription protocol and endpoints.

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

   For details about how to add an endpoint, see **Adding a Subscription**.

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	The monitoring scope of an alarm rule can be **All resources**, **Resource groups**, or **Specified resources**. **NOTE** • If you select **All resources**, an alarm notification will be sent when any instance meets an alarm policy, and existing alarm rules will be automatically applied for newly purchased resources. • 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.	All resources

Parameter	Description	Example Value
Group	This parameter is mandatory when **Monitoring Scope** is set to **Resource groups**.	N/A
Method	You can select an associated template, use an existing template or create a custom template as required. **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 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
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 **Creating a Topic** and **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. Configure the enterprise project.

Figure 5-4 Advanced Settings

Table 5-5 Name and **Description**

Parameter	Description
Enterprise Project	Specifies the enterprise project that the alarm rule belongs to. Only users with the enterprise project permissions can manage the alarm rule. For details about how to create an enterprise project, see **Creating an Enterprise Project**.

e. 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 Application Example: Creating an ECS CPU Usage Alarm

This topic describes how to create an alarm rule to monitor ECS CPU usage, in which **Threshold** is set to **>= 80%**.

Procedure

1. Log in to the management console.
2. In the navigation pane on the left, choose **Server Monitoring**.

   The list of ECSs on the cloud platform is displayed.
3. Locate the ECS, and choose **More** > **Create Alarm Rule** in the **Operation** column.

   The **Create Alarm Rule** page is displayed.
4. Enter **Name** and **Description**.
5. Configure the following parameters one by one:
   a. **Method**: Select **Configure manually**.
   b. **Metric Name**: Select **CPU Usage** from the drop-down list.
   c. **Alarm Policy**: The value can be **Avg.**, **5 minutes**, **3 consecutive periods**, **>=**, **80%**, and **One day**.
   d. **Alarm Severity**: Set it to **Major**.
   e. Enable **Alarm Notification**.
   f. **Notification Object**: Select the topic created in **Creating Alarm Notification Topics**.
   g. **Notification Window**: Set it to **00:00-23:59**.
   h. **Trigger Condition**: Select **Generated alarm** and **Cleared alarm**.
   i. **Enterprise Project**: Select **default**.
6. Click **Create**.

5.5 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.

5.6 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 5-6 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

Parameter	Description	Example Value
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
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 **Creating a Topic** and **Adding Subscriptions**.	N/A

Parameter	Description	Example Value
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), 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 **Creating an Enterprise Project**.	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 **OK**.

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

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 **OK**.

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

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 **OK**.

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

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 5-7**.

Figure 5-5 Create Custom Template

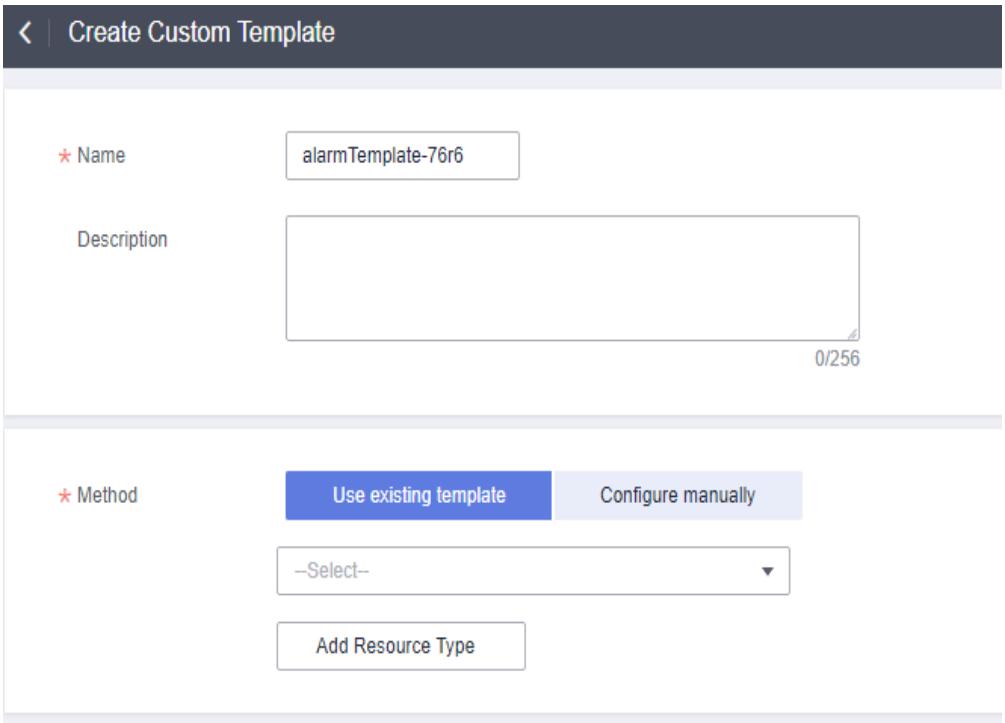


Table 5-7 Parameters

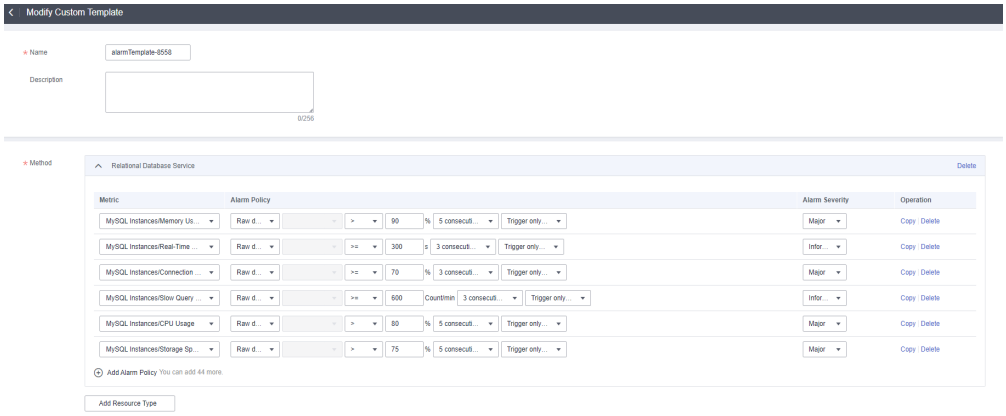
Parameter	Description
Name	Specifies the alarm rule name. The system generates a random name, which you can modify. Example value: **alarmTemplate-c6ft**
Description	(Optional) Provides supplementary information about the custom template.
Method	You can select **Using existing template** or **Configure 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 5-7**.

Figure 5-6 Modify Custom Template

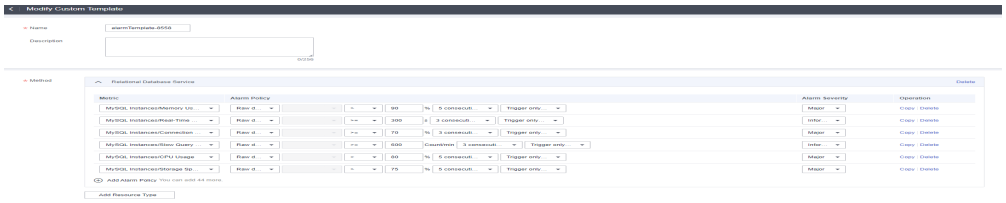


3. Click **Modify**.

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**.

Figure 5-7 Delete Custom Template



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 **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 **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 **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 **(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.

Constraints

Server monitoring is available only for servers installed using public images provided by . If any problem occurs when you use a private image, Cloud Eye will not provide technical support.

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 **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	**Installing and Configuring the Agent on a Linux ECS or BMS**
Installing the Agent on a Windows server	ECS	**Installing and Configuring the Agent on a Windows ECS**
Installing the Agent in batches on Linux servers	ECS	**Installing the Agents in Batches on Linux ECSs**

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.
- For details about the OSs that support the Agent, see **What OSs Does the Agent Support?**
- 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 **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 2.4.1

The Agent can monitor more metrics.

Version 2.3.2

The Agent architecture and installation path are updated.

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 **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 100.125.3.250** to the file. Enter **:wq** and press **Enter** to save the change.

   NOTE

   DNS server address

   ae-ad-1: 100.125.3.250 and 100.125.2.14

Modifying the DNS Server Address (Management Console)

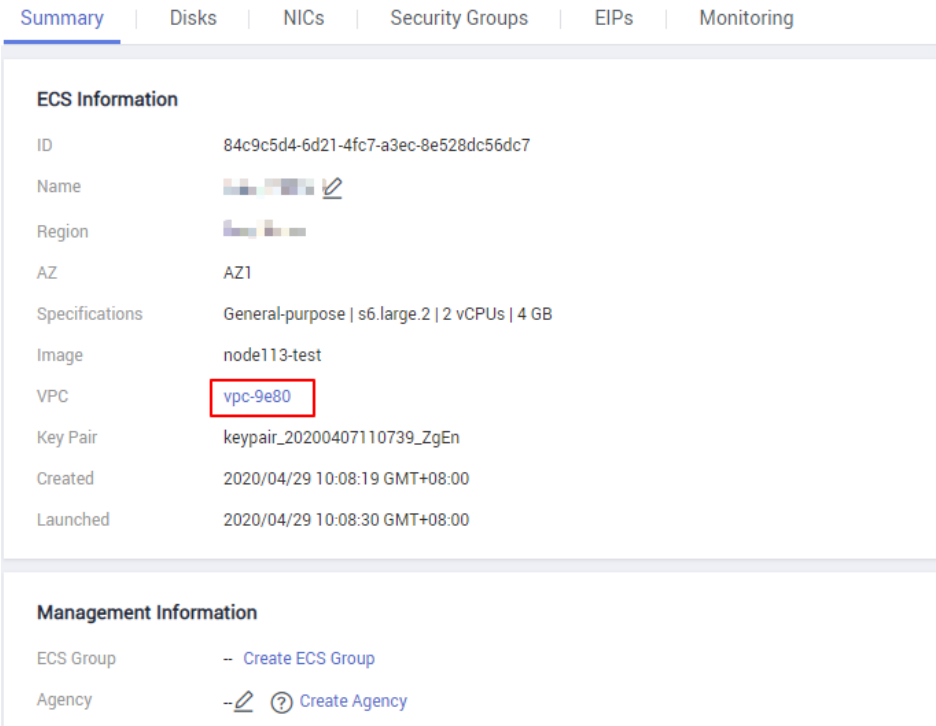
The following describes how to modify the DNS server address of an ECS on the management console. This topic takes an ECS as an example. The operations for BMSs are similar.

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.

Figure 6-1 VPC



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 **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:

   ae-ad-1:

   ```
   cd /usr/local && wget https://telescope-ae-ad-1.obs.ae-ad-1.g42cloud.com/scripts/agentInstall.sh &&
   chmod 755 agentInstall.sh && ./agentInstall.sh
   ```

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

   Figure 6-2 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 **Restoring the Agent Configurations on a Linux Server** or **(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 **(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 **(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

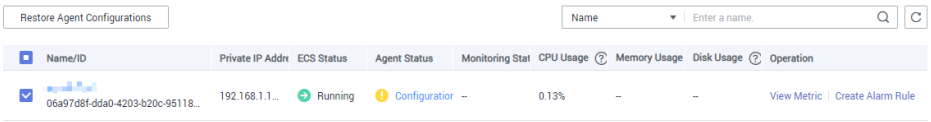
- The **Restore Agent Configurations** option is available for Agent 1.0.14 or later. If the Agent version is earlier than 1.0.14, upgrade the Agent first and then restore the Agent configurations or manually configure the Agent by following the instructions in **(Optional) Manually Configuring the Agent (Linux)**.
- The **Restore Agent Configurations** option is unavailable for BMSs. For details, see **(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**, the Agent has been installed and has started to collect fine-grained metric data.

Figure 6-3 Restore Agent Configurations



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 **How Can I Create an Agency?**

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

BMS parameters

```
{
    "InstanceId":"XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX",
    "ProjectId": "XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX",
    "AccessKey": "XXXXXXXXXXXXXXXXXXXX",
    "SecretKey": "XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX",
    "RegionId": "ae-ad-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 or BMS ID. Otherwise, you cannot see the OS monitoring data on Cloud Eye.

Parameter	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 or BMS 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, **ae-abudhabi-1**. For details, see **https://developer.huaweicloud.com/intl/endpoint**.
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.ae-ad-1.myhuaweicloud.com"
}
```

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 **ae-ad-1**, **Endpoint** is **ces.ae-ad-1.myhuaweicloud.com**.

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

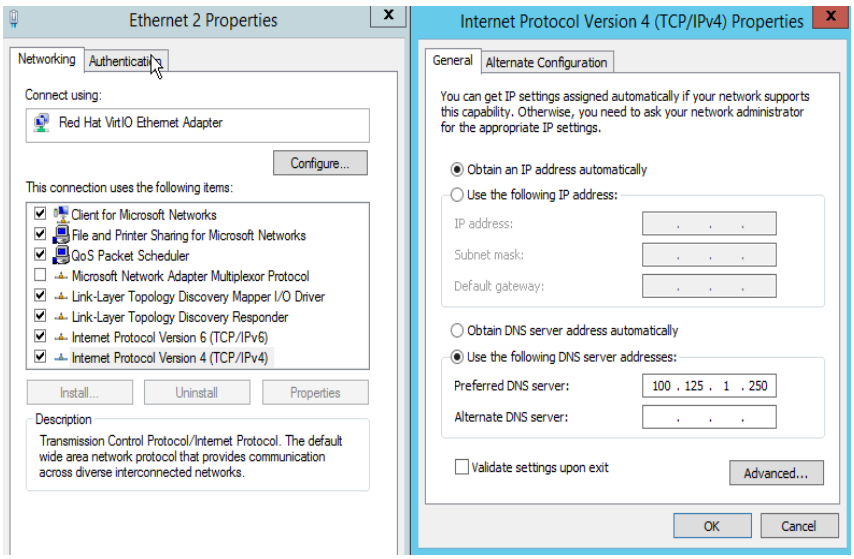
DNS and security group configuration are intended for the primary NIC.

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.

Figure 6-4 Adding the DNS server address (Windows)



NOTE

DNS server address

ae-ad-1: 100.125.3.250 and 100.125.2.14

Modifying the DNS Server Address (Management Console)

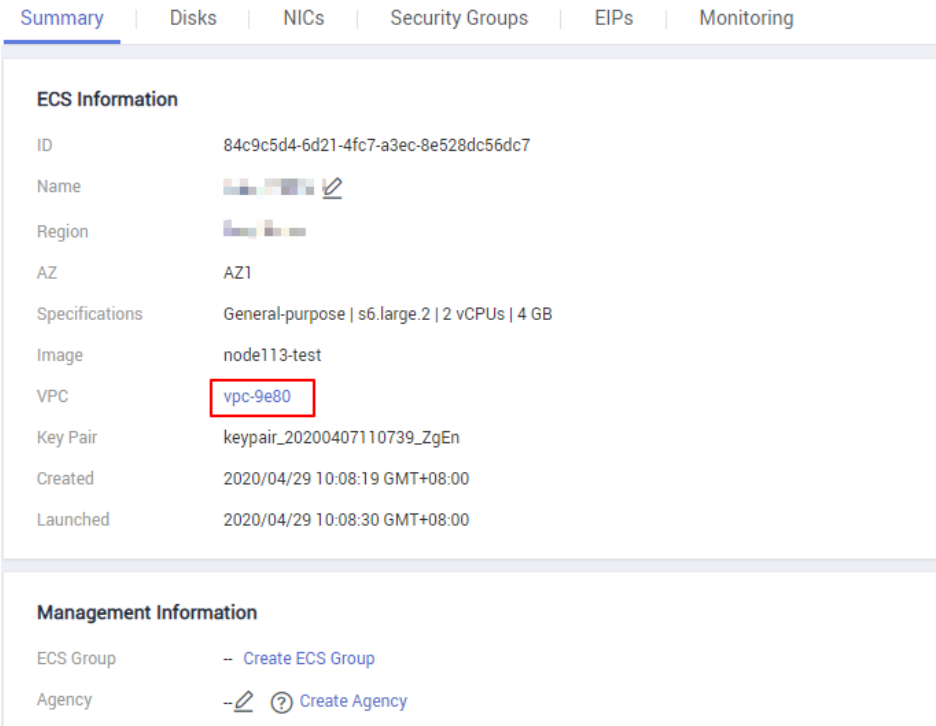
The following describes how to modify the DNS server address of an ECS on the management console. This topic takes an ECS as an example. The operations for BMSs are similar.

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.

Figure 6-5 VPC



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 6-4**.

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.
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.

Windows and Linux OSs are supported. For details, see **What OSs Does the Agent Support?**

Prerequisites

- You have performed operations described in **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	ae-ad-1: **https://telescope-ae-ad-1.obs.ae-ad-1.g42cloud.com/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.

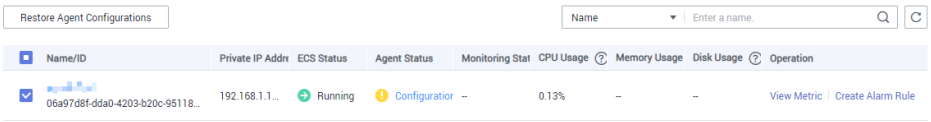
   NOTE

   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, the Agent has been installed and has started to collect fine-grained metric data.

Figure 6-6 Restore Agent Configurations



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.

Windows and Linux OSs are supported. For details, see **What OSs Does the Agent Support?**

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 **How Can I Create an Agency?**

```
{
    "InstanceId":"",
    "ProjectId": "",
    "AccessKey": "",
    "SecretKey": "",
    "RegionId": "ae-abudhabi-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.
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. For details, see **Creating a User Group and Assigning Permissions** and **Creating an IAM User and Adding It to a User Group**. ● 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, **ae-abudhabi-1**. For details, see **https://developer.huaweicloud.com/intl/endpoint**.
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.

Parameter	Description
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 **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:

   UAE-Abu Dhabi

   ```
   cd /usr/local && wget https://telescope-ae-ad-1.obs.ae-ad-1.g42cloud.com/scripts/agentBatchPackage.sh && chmod 755 agentBatchPackage.sh && ./agentBatchPackage.sh
   ```

3. Run the following command to run the script and enter the password (the passwords of multiple ECSs are the same):

   cd /usr/local && ./batchInstall.sh $password

   NOTICE

   - If multiple passwords are involved in the configured **iplist.txt**, enter the preceding commands and passwords for multiple times. If the password of an ECS is incorrect, the Agent installation on the ECS will fail.
   - If the passwords of multiple ECSs are different, run the **cd /usr/local && ./batchInstall.sh** command.
   - Ensure that the ECSs are running during script execution.

4. 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.

5. On the **Server Monitoring** page, select all ECSs and click **Restore Agent Configurations**.
6. On the page that is displayed, click **One-Click Restore**.
7. (Optional) If Pexpect is not required after the installation, run the following commands to delete Pexpect and Ptyprocess from the Python installation directory:

   cd /usr/lib/python2.7/site-packages

   rm pexpect-3.2-py2.7.egg-info -f

   rm ptyprocess-0.5.2-py2.7.egg-info -f

   rm pexpect -rf

   rm ptyprocess -rf

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 **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 Installing the Direct Connect Metric Collection Plug-ins

The Direct Connect plug-ins detect the end-to-end network quality of connections, and mainly monitor two metrics of remote subnets: network latency and packet loss rate.

There are two types of Direct Connect plug-ins:

- dc-nqa-collector: monitors the connections created on the Direct Connect console.
- history-dc-nqa-collector: monitors connections created through self-service.

NOTE

- Automated connections are requested by yourself on the console and are classified into self-service connections and full-service connections. Each connection has at least a virtual gateway and a virtual interface, and their routes are automatically advertised. Connections in most regions are automated connections.
- Historical connections are requested by email or phone. They do not have virtual gateways and virtual interfaces, and their routes must be manually configured. Historical connections exist only in some regions.

Constraints

The plug-in supports only Linux.

Prerequisites

- You have installed the Cloud Eye Agent. For details, see **Agent Installation and Configuration**.

- The Agent has been restored. For details, see **Restoring the Agent Configurations on a Linux Server**.
- You have obtained the password of user **root** for logging in to the target ECS.

Using the One-Click Installation Script to Configure the Plug-ins

In some regions of cloud services, you can use the one-click installation script to configure the plug-ins. **Table 6-8** lists the supported regions.

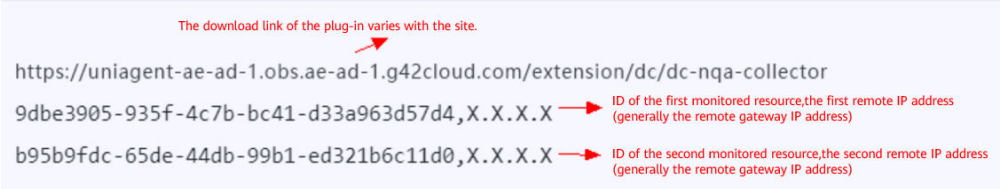
1. Log in to an ECS as user **root**.
2. Run the following command to create the **user.txt** file in the **usr/local/** directory and add user information, including the plug-in download link, monitored resource ID, and remote IP address:

   cd /usr/local/

   vi user.txt

   Figure 6-7 shows the format of the content in the **user.txt** file.

   Figure 6-7 Example of format

   Parameter descriptions are as follows.

   a. Plug-in download link: To monitor the connections created on the Direct Connect console, select the dc-nqa-collector plug-in. To monitor the connections created through self-service, select the history-dc-nqa-collector plug-in. For details about the download address of the installation package in each region, see **Table 6-7**.

   b. Information about monitored resources: One resource occupies one line, and consists of a resource ID and a remote IP address. Use a comma (,) to separate the resource ID and remote IP address. To add multiple resources, add lines in the same format.

      - **Resource ID**: The ID must contain 32 characters, including letters and digits, for example, **b95b9fdc-65de-44db-99b1-ed321b6c11d0** or **b95b9fdc65de44db99b1ed321b6c11d0**.

        - If the dc-nqa-collector plug-in is used, the resource ID is the virtual interface ID, which can be queried on the **Virtual Interfaces** page of the Direct Connect console.

        - If the history-dc-nqa-collector plug-in is used, the resource ID is the ID of the connection created through self-service, which can be queried on the **Historical Connections** page of the Direct Connect console.

      - **Remote IP address**: indicates the remote IP address that needs to be pinged with the VPC. Generally, it is the remote gateway IP address.

- If the dc-nqa-collector plug-in is used, enter the IP address of the remote gateway, which can be obtained on the **Virtual Gateways** page of the Direct Connect console.
- If the history-dc-nqa-collector plug-in is used, enter the host address in the **Remote Subnet** column on the **Historical Connections** page of the Direct Connect console.

NOTE

- Ensure that each monitored resource ID matches one remote IP address. You are not allowed to enter multiple IP addresses nor CIDR blocks.
- After the Agent is installed, if you want to add more resources to be monitored, edit the **user.txt** file by adding new IDs and IP addresses in sequence, and then perform **4**.

Table 6-7 Obtaining the plug-in installation package

Name	Download Path
dc-nqa-collector installation package	ae-ad-1: **https://uniagent-ae-ad-1.obs.ae-ad-1.g42cloud.com/extension/dc/dc-nqa-collector**
history-dc-nqa-collector installation package	ae-ad-1: **https://uniagent-ae-ad-1.obs.ae-ad-1.g42cloud.com/extension/dc/history-dc-nqa-collector**

3. Download the one-click installation script to the **/usr/local/** directory.

   wget *Download path of the target region*

Table 6-8 One-click installation script of the Direct Connect plug-ins

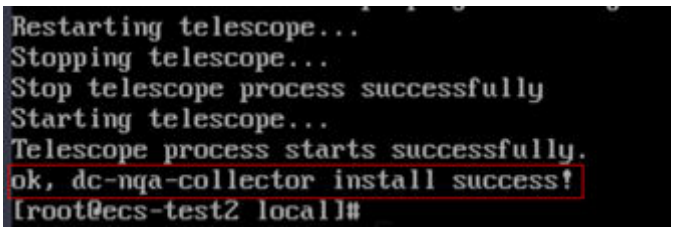
Region	Download Path
ae-ad-1	**https://uniagent-ae-ad-1.obs.ae-ad-1.g42cloud.com/extension/dc/dc-installer.sh**

4. Run the following command to run the plug-in script.

   If the installation is successful, the information shown in **Figure 6-8** is displayed.

   bash dc-installer.sh

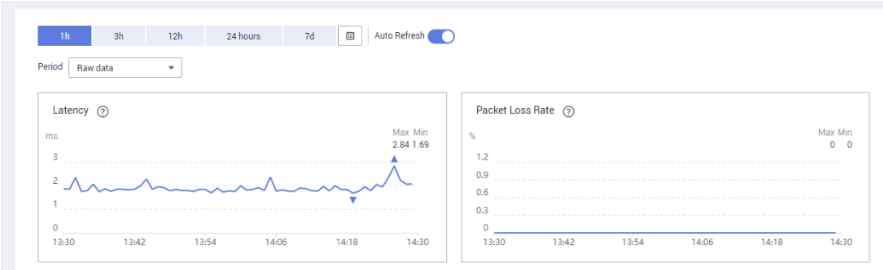
Figure 6-8 Successful installation



5. Wait for about 1 minute after installation and view the Direct Connect monitoring data on the Cloud Eye console.

   Click **Service List**, and select **Cloud Eye**. In the navigation pane on the left, choose **Cloud Service Monitoring** > **Direct Connect**. You can click the name of a monitored object to view the latency and packet loss rate.

   Figure 6-9 Network latency and packet loss rate



6.9 Process Monitoring

6.9.1 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 row that contains the target ECS and click **View Metric** to go to the **OS Monitoring** page.
5. Select the **Process Monitoring** tab.

   In the **System Processes** area, the process information is displayed. **Table 6-9** describes the metrics of system processes.

Table 6-9 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
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

Metric	Description	Value Range	Collection Mode (Linux)	Collection Mode (Windows)
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 row that contains the target ECS and click **View Metric** to go to the **OS Monitoring** page.
5. Select the **Process Monitoring** tab.
6. In the **Monitored Processes** area, click  in the upper right corner to view **Top 5 Processes with Highest CPU Usage**.
7. 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 6-10** lists **Process Monitoring** metrics.

Figure 6-10 Process monitoring

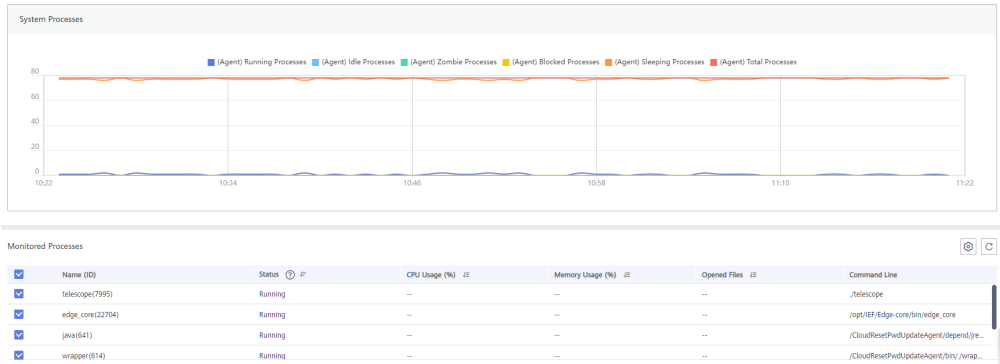


Table 6-10 Process Monitoring metrics

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

8. 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.

6.10 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 **Services Interconnected with Cloud Eye**.

Prerequisites

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

Procedure

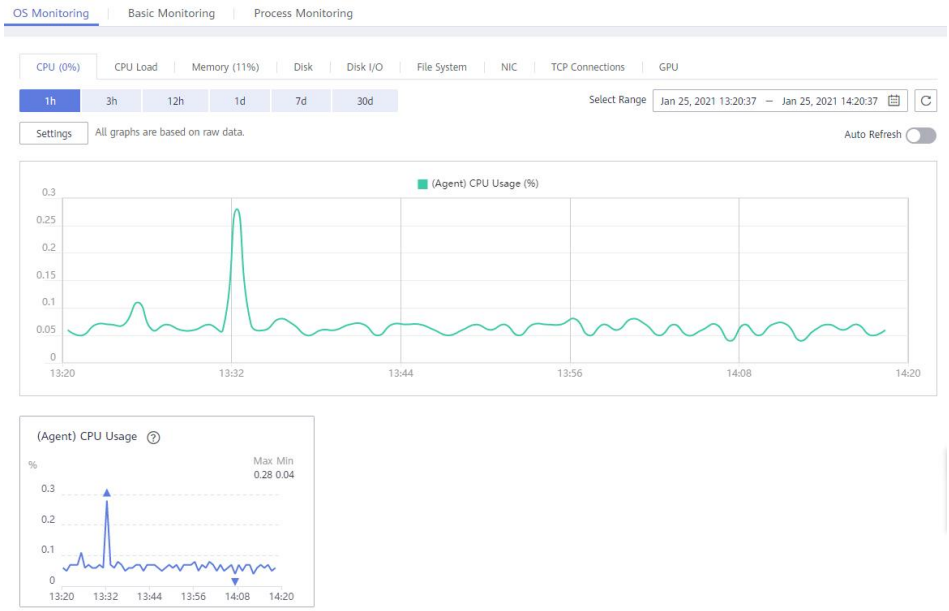
1. Log in to the management console.
2. Click **Service List** in the upper left corner, and select **Cloud Eye**.
3. View ECS or BMS metrics.

   NOTE

   For services that support enterprise projects, the system displays, by default, the host list of the enterprise projects on which you have permissions.

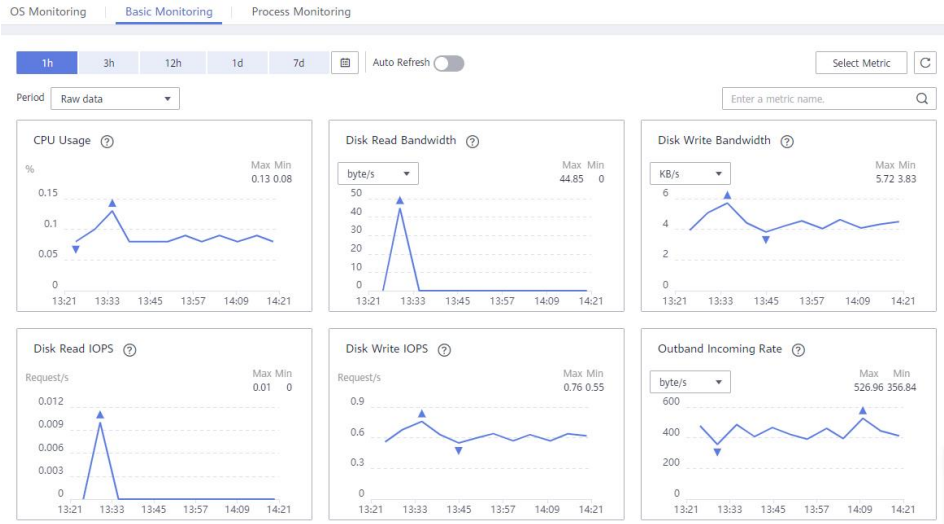
   – To view OS monitoring metrics of an ECS, in the left navigation pane, choose **Server Monitoring** > **Elastic Cloud Server**, locate the ECS, and click **View Metric** in the **Operation** column.

Figure 6-11 OS monitoring



– 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.

Figure 6-12 Basic Monitoring



– 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.

– To view processing monitoring metrics, click the **Process Monitoring** tab.

4. View metrics.

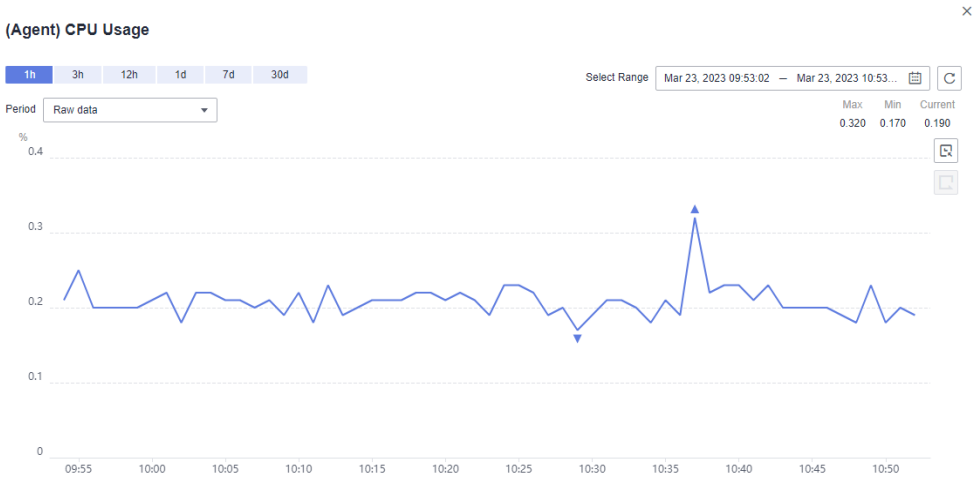
   In the upper part of the **OS Monitoring** page, different metric types, such as CPU, memory, and disk metrics are displayed.

   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.

Figure 6-13 (Agent) CPU Usage



6. In the upper left corner of the graph, locate **Period** and configure the rollup method.
   - If you select **1h**, **3h**, **12h**, or **1d**, raw data is displayed by default.
   - If you select **7d** or **30d**, aggregated data is displayed by default.
   - After clicking the zoom in icon in the upper right of an enlarged graph, you can drag the mouse to customize a time range.

6.11 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. In the **Operation** column, click **More**, and select **Create Alarm Rule**.
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 6-11 Parameter description

Parameter	Description
Name	Specifies the alarm rule name. The system generates a random name, which you can modify.

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

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

Table 6-12 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
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

Parameter	Description	Example Value
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 **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 6-13 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 **Creating a Topic** and **Adding Subscriptions**. For the HTTP(S) messages, see the *Simple Message Notification User Guide*.

Parameter	Description
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. Configure the enterprise project as prompted.

Figure 6-14 Advanced Settings

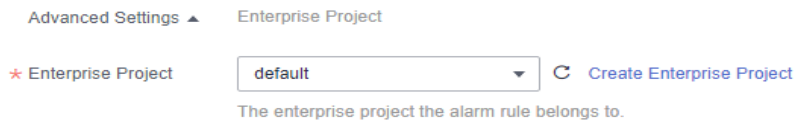


Table 6-14 Name and **Description**

Parameter	Description
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 **Creating an Enterprise Project**.

e. 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 **Adding Monitoring Data**.

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 **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**.

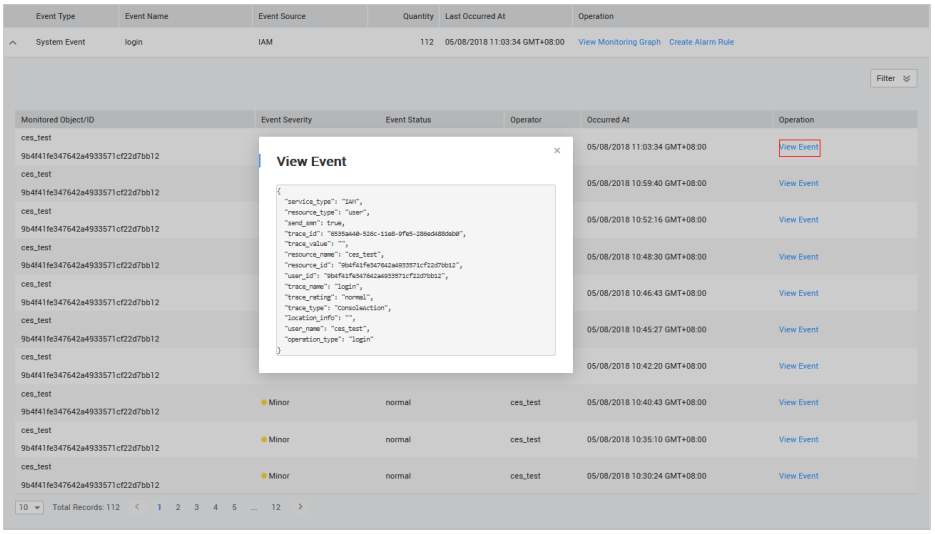
   On the displayed **Event Monitoring** page, all system events generated in the last 24 hours are displayed by default.

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

Figure 8-1 Event monitoring

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

Figure 8-2 Viewing event details



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.
Event Type	Specifies the event type, which can be **System event** or **Custom 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**.
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 **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**.

Parameter	Description
Trigger Mode	You can select immediate trigger or accumulative trigger based on the operation severity. Example value: **Immediate trigger**
Alarm Policy	Specifies the policy for triggering an alarm. For example, an alarm is triggered if the event occurred for three consecutive periods of 5 minutes. **NOTE** This parameter is mandatory when **Triggering Mode** is set to **Accumulative Trigger**.
Alarm Severity	Specifies the alarm severity, which can be **Critical**, **Major**, **Minor**, or **Informational**. Example value: **Major**
Operation	Select **Delete** to delete the alarm policy.

c. Configure the alarm notification.

Figure 8-3 Alarm notification

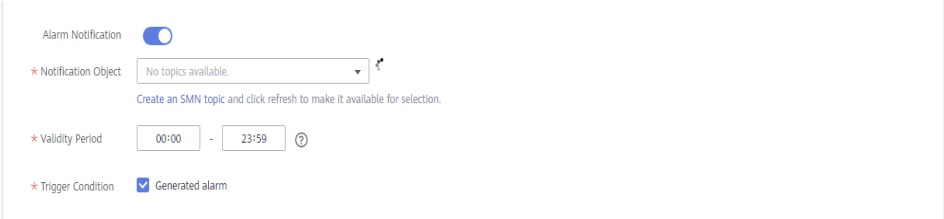


Table 8-3 Parameters for configuring alarm notifications

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 **Creating a Topic** and **Adding Subscriptions**.

Parameter	Description
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 trigger of alarm notifications.

d. Configure the enterprise project as prompted.

Figure 8-4 Advanced Settings

Table 8-4 Name and **Description**

Parameter	Description
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 **Creating an Enterprise Project**.

e. Click **Create**.

8.4 Events Supported by Event Monitoring

Table 8-5 Elastic Cloud Server (ECS)

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
ECS	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
	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
	GPU link fault	GPULinkFault	Critical	The GPU of the host running the ECS 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.
	FPGA link fault	FPGALinkFault	Critical	The FPGA of the host running the ECS was faulty or was recovering from a fault.	Deploy service applications in HA mode. After the FPGA fault is rectified, check whether services are restored.	Services are interrupted.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	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 was 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.
	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.

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 8-6 Bare Metal Server (BMS)

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
BMS	BMS restarted	osReboot	Major	The BMS was restarted ● on the management console. ● by calling APIs.	● Deploy service applications in HA mode. ● After the BMS is restarted, check whether services recover.	Services are interrupted.
	BMS unexpected restart	serverReboot	Major	The BMS restarted unexpectedly, which may be caused by ● OS faults. ● hardware faults.	● Deploy service applications in HA mode. ● After the BMS is restarted, check whether services recover.	Services are interrupted.
	BMS stopped	osShutdown	Major	The BMS was stopped ● on the management console. ● by calling APIs.	● Deploy service applications in HA mode. ● After the BMS is restarted, check whether services recover.	Services are interrupted.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	BMS unexpected shutdown	serverShutdown	Major	The BMS was stopped unexpectedly due to ● unexpected power-off. ● hardware faults.	● Deploy service applications in HA mode. ● After the BMS is restarted, check whether services recover.	Services are interrupted.
	Network disconnection	linkDown	Major	The BMS network was disconnected. Possible causes are as follows: ● The BMS was stopped or restarted unexpectedly. ● The switch was faulty. ● The gateway was faulty.	● Deploy service applications in HA mode. ● After the BMS is restarted, check whether services recover.	Services are interrupted.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	PCIe error	pcieError	Major	The PCIe device or main board on the BMS was faulty due to ● main board faults. ● PCIe device faults.	● Deploy service applications in HA mode. ● After the BMS is started, check whether services recover.	The network or disk read/write services are affected.
	Disk fault	diskError	Major	The hard disk backplane or the hard disk on the BMS was faulty due to ● disk backplane faults. ● disk faults.	● Deploy service applications in HA mode. ● After the fault is rectified, check whether services recover.	Data read/write services are affected, or the BMS cannot be started.
	EVS error	storageError	Major	The BMS failed to connect to EVS disks due to ● SDI card faults. ● Remote storage device faults.	● Deploy service applications in HA mode. ● After the fault is rectified, check whether services recover.	Data read/write services are affected, or the BMS cannot be started.

Table 8-7 Elastic IP (EIP)

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
EIP	EIP bandwidth exceeded	EIPBandwidthOverflow	Major	The used bandwidth exceeded the purchased one, which may slow down the network or cause packet loss. The value of this event is the maximum value in a monitoring period, and the value of the EIP inbound and outbound bandwidth is the value at a specific time point in the period. The metrics are described as follows: **egressDropBandwidth**: dropped outbound packets (bytes) **egressAcceptBandwidth**: accepted outbound packets (bytes) **egressMaxBandwidthPerSec**: peak outbound bandwidth (byte/s) **ingressAcceptBandwidth**: accepted inbound packets (bytes) **ingressMaxBandwidthPerSec**:	Check whether the EIP bandwidth keeps increasing and whether services are normal. Increase bandwidth if necessary.	The network becomes slow or packets are lost.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
				peak inbound bandwidth (byte/s) **ingressDropBandwidth**: dropped inbound packets (bytes)		
	EIP released	deleteEip	Minor	The EIP was released.	Check whether the EIP was release by mistake.	The server that has the EIP bound cannot access the Internet.
	EIP blocked	blockEIP	Critical	The used bandwidth of an EIP exceeded 5 Gbit/s, the EIP were blocked and packets were discarded. Such an event may be caused by DDoS attacks.	Replace the EIP to prevent services from being affected. Locate and deal with the fault.	Services are impacted.
	EIP unblocked	unblockEIP	Critical	The EIP was unblocked.	Use the previous EIP again.	None
	EIP traffic scrubbing started	ddosCleanEIP	Major	Traffic scrubbing on the EIP was started to prevent DDoS attacks.	Check whether the EIP was attacked.	Services may be interrupted.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	EIP traffic scrubbing ended	ddosEndCleanEip	Major	Traffic scrubbing on the EIP to prevent DDoS attacks was ended.	Check whether the EIP was attacked.	Services may be interrupted.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	QoS bandwidth exceeded	EIPBandwidthRuleOverflow	Major	The used QoS bandwidth exceeded the allocated one, which may slow down the network or cause packet loss. The value of this event is the maximum value in a monitoring period, and the value of the EIP inbound and outbound bandwidth is the value at a specific time point in the period. **egressDropBandwidth**: dropped outbound packets (bytes) **egressAcceptBandwidth**: accepted outbound packets (bytes) **egressMaxBandwidthPerSec**: peak outbound bandwidth (byte/s) **ingressAcceptBandwidth**: accepted inbound packets (bytes) **ingressMaxBandwidthPerSec**: peak inbound bandwidth (byte/s)	Check whether the EIP bandwidth keeps increasing and whether services are normal. Increase bandwidth if necessary.	The network becomes slow or packets are lost.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
				ingressDropBandwidth: dropped inbound packets (bytes)		

Table 8-8 Elastic IP (EIP)

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

Table 8-9 Advanced Anti-DDoS (AAD)

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
AAD	DDoS Attack Events	ddosAttackEvents	Major	A DDoS attack occurs in the AAD protected lines.	Judge the impact on services based on the attack traffic and attack type. If the attack traffic exceeds your purchased elastic bandwidth, change to another line or increase your bandwidth.	Services may be interrupted.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Domain name scheduling event	domainName Dispatch Events	Major	The high-defense CNAME corresponding to the domain name is scheduled, and the domain name is resolved to another high-defense IP address.	Pay attention to the workloads involving the domain name.	Services are not affected.
	Blackhole event	blackHole Events	Major	The attack traffic exceeds the purchased AAD protection threshold.	A blackhole is canceled after 30 minutes by default. The actual blackhole duration is related to the blackhole triggering times and peak attack traffic on the current day. The maximum duration is 24 hours. If you need to permit access before a blackhole becomes ineffective, contact technical support.	Services may be interrupted.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Cancel Blackhole	cancelBlackHole	Informational	The customer's AAD instance recovers from the black hole state.	This is only a prompt and no action is required.	Customer services recover.

Table 8-10 Cloud Backup and Recovery (CBR)

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
CBR	Failed to create the backup.	backupFailed	Critical	The backup failed to be created.	Manually create a backup or contact customer service.	Data loss may occur.
	Failed to restore the resource using a backup.	restorationFailed	Critical	The resource failed to be restored using a backup.	Restore the resource using another backup or contact customer service.	Data loss may occur.
	Failed to delete the backup.	backupDeleteFailed	Critical	The backup failed to be deleted.	Try again later or contact customer service.	Charging may be abnormal.
	Failed to delete the vault.	vaultDeleteFailed	Critical	The vault failed to be deleted.	Try again later or contact technical support.	Charging may be abnormal.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Replication failure	replicationFailed	Critical	The backup failed to be replicated.	Try again later or contact technical support.	Data loss may occur.
	The backup is created successfully.	backupSucceeded	Major	The backup was created.	None	None
	Resource restoration using a backup succeeded.	restorationSucceeded	Major	The resource was restored using a backup.	Check whether the data is successfully restored.	None
	The backup is deleted successfully.	backupDeletionSucceeded	Major	The backup was deleted.	None	None
	The vault is deleted successfully.	vaultDeletionSucceeded	Major	The vault was deleted.	None	None
	Replication success	replicationSucceeded	Major	The backup was replicated successfully.	None	None
	Client offline	agentOffline	Critical	The backup client was offline.	Ensure that the Agent status is normal and the backup client can be connected to cloud service platform.	Backup tasks may fail.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Client online	agentOnline	Major	The backup client was online.	None	None

Table 8-11 Relational Database Service (RDS) — resource exception

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
RDS	DB instance creation failure	createInstanceFailed	Major	A DB instance fails to create because the number of disks is insufficient, the quota is insufficient, or underlying resources are exhausted.	Check the number and quota of disks. Release resources and create DB instances again.	DB instances cannot be created.
	Full backup failure	fullBackupFailed	Major	A single full backup failure does not affect the files that have been successfully backed up, but prolong the incremental backup time during the point-in-time restore (PITR).	Create a manual backup again.	Backup failed.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Primary/standby switchover or failure	activeStandBySwitchFailed	Major	The standby DB instance does not take over workloads from the primary DB instance due to network or server failures. The original primary DB instance continues to provide workloads within a short time.	Check whether the connection between your application and the database is re-established.	None

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Replication status abnormal	abnormalReplicationStatus	Major	The possible causes are as follows: The replication delay between the primary instance and the standby instance or a read replica is too long, which usually occurs when a large amount of data is being written to databases or a large transaction is being processed. During peak hours, data may be blocked. The network between the primary instance and the standby instance or a read replica is disconnected.	Submit a service ticket.	Your applications are not affected because this event does not interrupt data read and write.
	Replication status recovered	replicationStatusRecovered	Major	The replication delay between the primary and standby instances is within the normal range, or the network connection between them has restored.	No further action is required.	None

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	DB instance faulty	faultyDBInstance	Major	A single or primary DB instance was faulty due to a disaster or a server failure.	Check whether an automated backup policy has been configured for the DB instance and submit a service ticket.	The database service may be unavailable.
	DB instance recovered	DBInstanceRecovered	Major	RDS rebuilds the standby DB instance with its high availability. After the instance is rebuilt, this event will be reported.	No further action is required.	None
	Failure of changing single DB instance to primary/standby	singleToHaFailed	Major	A fault occurs when RDS is creating the standby DB instance or configuring replication between the primary and standby DB instances. The fault may occur because resources are insufficient in the data center where the standby DB instance is located.	Submit a service ticket.	Your applications are not affected because this event does not interrupt data read and write of the DB instance.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Database process restarted	DatabaseProcessRestarted	Major	The database process is stopped due to insufficient memory or high load.	Log in to the Cloud Eye console. Check whether the memory usage increases sharply, the CPU usage is too high for a long time, or the storage space is insufficient. You can increase the CPU and memory specifications or optimize the service logic.	When the process exits abnormally, workloads are interrupted. In this case, RDS automatically restarts the database process and attempts to recover the workloads.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Instance storage full	instanceDiskFull	Major	Generally, the cause is that the data space usage is too high.	Scale up the instance.	The DB instance becomes read-only because the storage space is full, and data cannot be written to the database.
	Instance storage full recovered	instanceDiskFullRecovered	Major	The instance disk is recovered.	No action is required.	The instance is restored and supports both read and write operations.
	Kafka connection failed	kafkaConnectionFailed	Major	The network is unstable or the Kafka server does not work properly.	Check your network connection and the Kafka server status.	Audit logs cannot be sent to the Kafka server.

Table 8-12 Relational Database Service (RDS) — operations

Event Source	Event Name	Event ID	Event Severity	Description
RDS	Reset administrator password	resetPassword	Major	The password of the database administrator is reset.
	Operate DB instance	instanceAction	Major	The storage space is scaled or the instance class is changed.
	Delete DB instance	deleteInstance	Minor	The DB instance is deleted.
	Modify backup policy	setBackupPolicy	Minor	The backup policy is modified.
	Modify parameter group	updateParameterGroup	Minor	The parameter group is modified.
	Delete parameter group	deleteParameterGroup	Minor	The parameter group is deleted.
	Reset parameter group	resetParameterGroup	Minor	The parameter group is reset.
	Change database port	changeInstancePort	Major	The database port is changed.
	Primary/standby switchover or failover	PrimaryStandbySwitched	Major	A switchover or failover is performed.

Table 8-13 Document Database Service (DDS)

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
DDS	DB instance creation failure	DDSCreateInstanceFailed	Major	A DDS instance fails to be created due to insufficient disks, quotas, and underlying resources.	Check the number and quota of disks. Release resources and create DDS instances again.	DDS instances cannot be created.
	Replication failed	DDSAbnormalReplicationStatus	Major	The possible causes are as follows: The replication delay between the primary instance and the standby instance or a read replica is too long, which usually occurs when a large amount of data is being written to databases or a large transaction is being processed. During peak hours, data may be blocked. The network between the primary instance and the standby instance or a read replica is disconnected.	Submit a service ticket.	Your applications are not affected because this event does not interrupt data read and write.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Replication recovered	DDSReplicationStatusRecovered	Major	The replication delay between the primary and standby instances is within the normal range, or the network connection between them has restored.	No action is required.	None
	DB instance failed	DDSFaultyDBInstance	Major	This event is a key alarm event and is reported when an instance is faulty due to a disaster or a server failure.	Submit a service ticket.	The database service may be unavailable.
	DB instance recovered	DDSDBInstanceRecovered	Major	If a disaster occurs, NoSQL provides an HA tool to automatically or manually rectify the fault. After the fault is rectified, this event is reported.	No action is required.	None
	Faulty node	DDSFaultyDBNode	Major	This event is a key alarm event and is reported when a database node is faulty due to a disaster or a server failure.	Check whether the database service is available and submit a service ticket.	The database service may be unavailable.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Node recovered	DDSDBNodeRecovered	Major	If a disaster occurs, NoSQL provides an HA tool to automatically or manually rectify the fault. After the fault is rectified, this event is reported.	No action is required.	None
	Primary/standby switchover or failover	DDSPrimaryStandbySwitched	Major	A primary/standby switchover is performed or a failover is triggered.	No action is required.	None
	Insufficient storage space	DDSRiskyDataDiskUsage	Major	The storage space is insufficient.	Scale up storage space. For details, see section "Scaling Up Storage Space" in the corresponding user guide.	The instance is set to read-only and data cannot be written to the instance.
	Data disk expanded and being writable	DDSDataDiskUsageRecovered	Major	The capacity of a data disk has been expanded and the data disk becomes writable.	No further action is required.	No adverse impact.

Table 8-14 GaussDB NoSQL

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
GaussDB NoSQL	DB instance creation failed	NoSQL CreateInstance Failed	Major	The instance quota or underlying resources are insufficient.	Release the instances that are no longer used and try to provision them again, or submit a service ticket to adjust the quota.	DB instances cannot be created.
	Specifications modification failed	NoSQL ResizeInstance Failed	Major	The underlying resources are insufficient.	Submit a service ticket. The O&M personnel will coordinate resources in the background, and then you need to change the specifications again.	Services are interrupted.
	Node adding failed	NoSQL AddNodesFailed	Major	The underlying resources are insufficient.	Submit a service ticket. The O&M personnel will coordinate resources in the background, and then you delete the node that failed to be added and add a new node.	None
	Node deletion failed	NoSQL DeleteNodesFailed	Major	The underlying resources fail to be released.	Delete the node again.	None

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Storage space scale-up failed	NoSQL ScaleUpStorageFailed	Major	The underlying resources are insufficient.	Submit a service ticket. The O&M personnel will coordinate resources in the background and then you scale up the storage space again.	Services may be interrupted.
	Password reset failed	NoSQL ResetPasswordFailed	Major	Resetting the password times out.	Reset the password again.	None
	Parameter group change failed	NoSQL UpdateInstanceParamGroupFailed	Major	Changing a parameter group times out.	Change the parameter group again.	None
	Backup policy configuration failed	NoSQL SetBackupPolicyFailed	Major	The database connection is abnormal.	Configure the backup policy again.	None
	Manual backup creation failed	NoSQL CreateManualBackupFailed	Major	The backup files fail to be exported or uploaded.	Submit a service ticket to the O&M personnel.	Data cannot be backed up.
	Automated backup creation failed	NoSQL CreateAutomatedBackupFailed	Major	The backup files fail to be exported or uploaded.	Submit a service ticket to the O&M personnel.	Data cannot be backed up.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Faulty DB instance	NoSQL FaultyDBInstance	Major	This event is a key alarm event and is reported when an instance is faulty due to a disaster or a server failure.	Submit a service ticket.	The database service may be unavailable.
	DB instance recovered	NoSQL DBInstanceRecovered	Major	If a disaster occurs, NoSQL provides an HA tool to automatically or manually rectify the fault. After the fault is rectified, this event is reported.	No action is required.	None
	Faulty node	NoSQL FaultyDBNode	Major	This event is a key alarm event and is reported when a database node is faulty due to a disaster or a server failure.	Check whether the database service is available and submit a service ticket.	The database service may be unavailable.
	Node recovered	NoSQL DBNodeRecovered	Major	If a disaster occurs, NoSQL provides an HA tool to automatically or manually rectify the fault. After the fault is rectified, this event is reported.	No action is required.	None

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Primary/standby switchover or failover	NoSQLPrimaryStandbySwitched	Major	This event is reported when a primary/standby switchover is performed or a failover is triggered.	No action is required.	None
	HotKey occurred	HotKeyOccurs	Major	The primary key is improperly configured. As a result, hotspot data is distributed in one partition. The improper application design causes frequent read and write operations on a key.	1. Choose a proper partition key. 2. Add service cache. The service application reads hotspot data from the cache first.	The service request success rate is affected, and the cluster performance and stability also be affected.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	BigKey occurred	BigKeyOccurs	Major	The primary key design is improper. The number of records or data in a single partition is too large, causing unbalanced node loads.	1. Choose a proper partition key. 2. Add a new partition key for hashing data.	As the data in the large partition increases, the cluster stability deteriorates.
	Insufficient storage space	NoSQLRiskyDataDiskUsage	Major	The storage space is insufficient.	Scale up storage space. For details, see section "Scaling Up Storage Space" in the corresponding user guide.	The instance is set to read-only and data cannot be written to the instance.
	Data disk expanded and being writable	NoSQLDataDiskUsageRecovered	Major	The capacity of a data disk has been expanded and the data disk becomes writable.	No operation is required.	None

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Index creation failed	NoSQL CreateIndexFailed	Major	The service load exceeds what the instance specifications can take. In this case, creating indexes consumes more instance resources. As a result, the response is slow or even frame freezing occurs, and the creation times out.	Select the matched instance specifications based on the service load. Create indexes during off-peak hours. Create indexes in the background. Select indexes as required.	The index fails to be created or is incomplete. As a result, the index is invalid. Delete the index and create an index.
	Write speed decreased	NoSQL Stalling Occurs	Major	The write speed is fast, which is close to the maximum write capability allowed by the cluster scale and instance specifications. As a result, the flow control mechanism of the database is triggered, and requests may fail.	1. Adjust the cluster scale or node specifications based on the maximum write rate of services. 2. Measures the maximum write rate of services.	The success rate of service requests is affected.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Data write stopped	NoSQLStoppingOccurs	Major	The data write is too fast, reaching the maximum write capability allowed by the cluster scale and instance specifications. As a result, the flow control mechanism of the database is triggered, and requests may fail.	1. Adjust the cluster scale or node specifications based on the maximum write rate of services. 2. Measures the maximum write rate of services.	The success rate of service requests is affected.
	Database restart failed	NoSQLRestartDBFailed	Major	The instance status is abnormal.	Submit a service ticket to the O&M personnel.	The DB instance status may be abnormal.
	Restoration to new DB instance failed	NoSQLRestoreToNewInstanceFailed	Major	The underlying resources are insufficient.	Submit a service order to ask the O&M personnel to coordinate resources in the background and add new nodes.	Data cannot be restored to a new DB instance.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Restoration to existing DB instance failed	NoSQL RestoreToExistInstanceFailed	Major	The backup file fails to be downloaded or restored.	Submit a service ticket to the O&M personnel.	The current DB instance may be unavailable.
	Backup file deletion failed	NoSQL DeleteBackupFailed	Major	The backup files fail to be deleted from OBS.	Delete the backup files again.	None
	Failed to enable Show Original Log	NoSQL SwitchSlowlogPlainTextFailed	Major	The DB engine does not support this function.	Refer to the *GaussDB NoSQL User Guide* to ensure that the DB engine supports Show Original Log. Submit a service ticket to the O&M personnel.	None
	EIP binding failed	NoSQL BindEipFailed	Major	The node status is abnormal, an EIP has been bound to the node, or the EIP to be bound is invalid.	Check whether the node is normal and whether the EIP is valid.	The DB instance cannot be accessed from the Internet.
	EIP unbinding failed	NoSQL UnbindEipFailed	Major	The node status is abnormal or the EIP has been unbound from the node.	Check whether the node and EIP status are normal.	None

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Parameter modification failed	NoSQL ModifyParameterFailed	Major	The parameter value is invalid.	Check whether the parameter value is within the valid range and submit a service ticket to the O&M personnel.	None
	Parameter group application failed	NoSQL ApplyParameterGroupFailed	Major	The instance status is abnormal. As a result, the parameter group cannot be applied.	Submit a service ticket to the O&M personnel.	None
	Failed to enable or disable SSL	NoSQL SwitchSSLFailed	Major	Enabling or disabling SSL times out.	Try again or submit a service ticket. Do not change the connection mode.	The connection mode cannot be changed.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Row size too large	LargeRowOccurs	Major	If there is too much data in a single row, queries may time out, causing faults like OOM error.	1. Control the length of each column and row so that the sum of key and value lengths in each row does not exceed the preset threshold. 2. Check whether there are invalid writes or encoding resulting in large keys or values.	If there are rows that are too large, the cluster performance will deteriorate as the data volume grows.

Table 8-15 GaussDB(for MySQL)

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
GaussDB(for MySQL)	Incremental backup failure	TaurusIncrementalBackupInstanceFailed	Major	The network between the instance and the management plane (or the OBS) is disconnected, or the backup environment created for the instance is abnormal.	Submit a service ticket.	Backup jobs fail.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Read replica creation failure	addReadonlyNodesFailed	Major	The quota is insufficient or underlying resources are exhausted.	Check the read replica quota. Release resources and create read replicas again.	Read replicas fail to be created.
	DB instance creation failure	createInstanceFailed	Major	The instance quota or underlying resources are insufficient.	Check the instance quota. Release resources and create instances again.	DB instances fail to be created.
	Read replica promotion failure	activeStandBySwitchFailed	Major	The read replica fails to be promoted to the primary node due to network or server failures. The original primary node takes over services quickly.	Submit a service ticket.	The read replica fails to be promoted to the primary node.
	Instance specifications change failure	flavorAlterationFailed	Major	The quota is insufficient or underlying resources are exhausted.	Submit a service ticket.	Instance specifications fail to be changed.
	Faulty DB instance	TaurusInstanceRunningStatusAbnormal	Major	The instance process is faulty or the communications between the instance and the DFV storage are abnormal.	Submit a service ticket.	Services may be affected.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	DB instance recovered	TaurusInstanceRunningStatusRecovered	Major	The instance is recovered.	Observe the service running status.	None
	Faulty node	TaurusNodeRunningStatusAbnormal	Major	The node process is faulty or the communications between the node and the DFV storage are abnormal.	Observe the instance and service running statuses.	A read replica may be promoted to the primary node.
	Node recovered	TaurusNodeRunningStatusRecovered	Major	The node is recovered.	Observe the service running status.	None
	Read replica deletion failure	TaurusDeleteReadOnlyNodeFailed	Major	The communications between the management plane and the read replica are abnormal or the VM fails to be deleted from IaaS.	Submit a service ticket.	Read replicas fail to be deleted.
	Password reset failure	TaurusResetInstancePasswordFailed	Major	The communications between the management plane and the instance are abnormal or the instance is abnormal.	Check the instance status and try again. If the fault persists, submit a service ticket.	Passwords fail to be reset for instances.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	DB instance reboot failure	TaurusRestartInstanceFailed	Major	The network between the management plane and the instance is abnormal or the instance is abnormal.	Check the instance status and try again. If the fault persists, submit a service ticket.	Instances fail to be rebooted.
	Restoration to new DB instance failure	TaurusRestoreToNewInstanceFailed	Major	The instance quota is insufficient, underlying resources are exhausted, or the data restoration logic is incorrect.	If the new instance fails to be created, check the instance quota, release resources, and try to restore to a new instance again. In other cases, submit a service ticket.	Backup data fails to be restored to new instances.
	EIP binding failure	TaurusBindEIPToInstanceFailed	Major	The binding task fails.	Submit a service ticket.	EIPs fail to be bound to instances.
	EIP unbinding failure	TaurusUnbindEIPFromInstanceFailed	Major	The unbinding task fails.	Submit a service ticket.	EIPs fail to be unbound from instances.
	Parameter modification failure	TaurusUpdateInstanceParameterFailed	Major	The network between the management plane and the instance is abnormal or the instance is abnormal.	Check the instance status and try again. If the fault persists, submit a service ticket.	Instance parameters fail to be modified.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Parameter template application failure	TaurusApplyParameterGroupToInstanceFailed	Major	The network between the management plane and instances is abnormal or the instances are abnormal.	Check the instance status and try again. If the fault persists, submit a service ticket.	Parameter templates fail to be applied to instances.
	Full backup failure	TaurusBackupInstanceFailed	Major	The network between the instance and the management plane (or the OBS) is disconnected, or the backup environment created for the instance is abnormal.	Submit a service ticket.	Backup jobs fail.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Primary/standby failover	TaurusActiveStandbySwitched	Major	When the network, physical machine, or database of the primary node is faulty, the system promotes a read replica to primary based on the failover priority to ensure service continuity.	1. Check whether the service is running properly. 2. Check whether an alarm is generated, indicating that the read replica failed to be promoted to primary.	During the failover, database connection is interrupted for a short period of time. After the failover is complete, you can reconnect to the database.
	Database read-only	NodeReadonlyMode	Major	The database supports only query operations.	Submit a service ticket.	After the database becomes read-only, write operations cannot be processed.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Database read/write	NodeReadWriteMode	Major	The database supports both write and read operations.	Submit a service ticket.	None.

Table 8-16 GaussDB

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
GaussDB	Process status alarm	ProcessStatusAlarm	Major	Key processes exit, including CMS/CMA, ETCD, GTM, CN, and DN processes.	Wait until the process is automatically recovered or a primary/standby failover is automatically performed. Check whether services are recovered. If no, contact SRE engineers.	If processes on primary nodes are faulty, services are interrupted and then rolled back. If processes on standby nodes are faulty, services are not affected.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Component status alarm	ComponentStatusAlarm	Major	Key components do not respond, including CMA, ETCD, GTM, CN, and DN components.	Wait until the process is automatically recovered or a primary/standby failover is automatically performed. Check whether services are recovered. If no, contact SRE engineers.	If processes on primary nodes do not respond, neither do the services. If processes on standby nodes are faulty, services are not affected.
	Cluster status alarm	ClusterStatusAlarm	Major	The cluster status is abnormal. For example, the cluster is read-only; majority of ETCDs are faulty; or the cluster resources are unevenly distributed.	Contact SRE engineers.	If the cluster status is read-only, only read services are processed. If the majority of ETCDs are fault, the cluster is unavailable. If resources are unevenly distributed, the instance performance and reliability deteriorate.
	Hardware resource alarm	HardwareResourceAlarm	Major	A major hardware fault occurs in the instance, such as disk damage or GTM network fault.	Contact SRE engineers.	Some or all services are affected.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Status transition alarm	StateTransitionAlarm	Major	The following events occur in the instance: DN build failure, forcible DN promotion, primary/standby DN switchover/failover, or primary/standby GTM switchover/failover.	Wait until the fault is automatically rectified and check whether services are recovered. If no, contact SRE engineers.	Some services are interrupted.
	Other abnormal alarm	OtherAbnormalAlarm	Major	Disk usage threshold alarm	Focus on service changes and scale up storage space as needed.	If the used storage space exceeds the threshold, storage space cannot be scaled up.
	Faulty DB instance	TaurusInstanceRunningStatusAbnormal	Major	This event is a key alarm event and is reported when an instance is faulty due to a disaster or a server failure.	Submit a service ticket.	The database service may be unavailable.
	DB instance recovered	TaurusInstanceRunningStatusRecovered	Major	GaussDB(openGauss) provides an HA tool for automated or manual rectification of faults. After the fault is rectified, this event is reported.	No further action is required.	None

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Faulty DB node	TaurusNodeRunningStatusAbnormal	Major	This event is a key alarm event and is reported when a database node is faulty due to a disaster or a server failure.	Check whether the database service is available and submit a service ticket.	The database service may be unavailable.
	DB node recovered	TaurusNodeRunningStatusRecovered	Major	GaussDB(openGauss) provides an HA tool for automated or manual rectification of faults. After the fault is rectified, this event is reported.	No further action is required.	None
	DB instance creation failure	GaussDBV5CreateInstanceFailed	Major	Instances fail to be created because the quota is insufficient or underlying resources are exhausted.	Release the instances that are no longer used and try to provision them again, or submit a service ticket to adjust the quota.	DB instances cannot be created.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Node adding failure	GaussDBV5ExpandClusterFailed	Major	The underlying resources are insufficient.	Submit a service ticket. The O&M personnel will coordinate resources in the background, and then you delete the node that failed to be added and add a new node.	None
	Storage scale-up failure	GaussDBV5EnlargeVolumeFailed	Major	The underlying resources are insufficient.	Submit a service ticket. The O&M personnel will coordinate resources in the background and then you scale up the storage space again.	Services may be interrupted.
	Reboot failure	GaussDBV5RestartInstanceFailed	Major	The network is abnormal.	Retry the reboot operation or submit a service ticket to the O&M personnel.	The database service may be unavailable.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Full backup failure	GaussDBV5FullBackupFailed	Major	The backup files fail to be exported or uploaded.	Submit a service ticket to the O&M personnel.	Data cannot be backed up.
	Differential backup failure	GaussDBV5DifferentialBackupFailed	Major	The backup files fail to be exported or uploaded.	Submit a service ticket to the O&M personnel.	Data cannot be backed up.
	Backup deletion failure	GaussDBV5DeleteBackupFailed	Major	This function does not need to be implemented.	N/A	N/A
	EIP binding failure	GaussDBV5BindEIPFailed	Major	The EIP is bound to another resource.	Submit a service ticket to the O&M personnel.	The instance cannot be accessed from the Internet.
	EIP unbinding failure	GaussDBV5UnbindEIPFailed	Major	The network is faulty or EIP is abnormal.	Unbind the IP address again or submit a service ticket to the O&M personnel.	IP addresses may be residual.
	Parameter template application failure	GaussDBV5ApplyParamFailed	Major	Modifying a parameter template times out.	Modify the parameter template again.	None

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Parameter modification failure	GaussDBV5UpdateInstanceParamGroupFailed	Major	Modifying a parameter template times out.	Modify the parameter template again.	None
	Backup and restoration failure	GaussDBV5RestoreFromBcakupFailed	Major	The underlying resources are insufficient or backup files fail to be downloaded.	Submit a service ticket.	The database service may be unavailable during the restoration failure.

Table 8-17 Distributed Database Middleware (DDM)

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
DDM	Failed to create a DDM instance	createDdmInstanceFailed	Major	The underlying resources are insufficient.	Release resources and create the instance again.	DDM instances cannot be created.
	Failed to change class of a DDM instance	resizeFlavorFailed	Major	The underlying resources are insufficient.	Submit a service ticket to the O&M personnel to coordinate resources and try again.	Services on some nodes are interrupted.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Failed to scale out a DDM instance	enlargeNodeFailed	Major	The underlying resources are insufficient.	Submit a service ticket to the O&M personnel to coordinate resources, delete the node that fails to be added, and add a node again.	The instance fails to be scaled out.
	Failed to scale in a DDM instance	reduceNodeFailed	Major	The underlying resources fail to be released.	Submit a service ticket to the O&M personnel to release resources.	The instance fails to be scaled in.
	Failed to restart a DDM instance	restartInstanceFailed	Major	The DB instances associated are abnormal.	Check whether DB instances associated are normal. If the instances are normal, submit a service ticket to the O&M personnel.	Services on some nodes are interrupted.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Failed to create a schema	createLogicDbFailed	Major	The possible causes are as follows: ● The DB instance account is incorrect. ● The DDM instance and its associated DB instances cannot communicate with each other because their security groups are not configured correctly.	Check the following items: ● Whether the DB instance account is correct. ● Whether the security groups associated with the DDM instance and its associated DB instance are correctly configured.	Services cannot run properly.
	Failed to bind an EIP	bindEipFailed	Major	The EIP is abnormal.	Try again later. In case of emergency, contact O&M personnel to rectify the fault.	The DDM instance cannot be accessed from the Internet.
	Failed to scale out a schema	migrateLogicDbFailed	Major	The underlying resources fail to be processed.	Submit a service ticket to the O&M personnel.	The schema cannot be scaled out.
	Failed to re-scale out a schema	retryMigrateLogicDbFailed	Major	The underlying resources fail to be processed.	Submit a service ticket to the O&M personnel.	The schema cannot be scaled out.

Table 8-18 Cloud Phone

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
CPH	Server shutdown	cphServerOsShutdown	Major	The cloud phone server was stopped ● on the management console. ● by calling APIs.	Deploy service applications in HA mode. After the fault is rectified, check whether services recover.	Services are interrupted.
	Server abnormal shutdown	cphServerShutdown	Major	The cloud phone server was stopped unexpectedly. Possible causes are as follows: ● The cloud phone server was powered off unexpectedly. ● The cloud phone server was stopped due to hardware faults.	Deploy service applications in HA mode. After the fault is rectified, check whether services recover.	Services are interrupted.
	Server reboot	cphServerOsReboot	Major	The cloud phone server was rebooted ● on the management console. ● by calling APIs.	Deploy service applications in HA mode. After the fault is rectified, check whether services recover.	Services are interrupted.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Server abnormal reboot	cphServerReboot	Major	The cloud phone server was rebooted unexpectedly due to ● OS faults. ● hardware faults.	Deploy service applications in HA mode. After the fault is rectified, check whether services recover.	Services are interrupted.
	Network disconnection	cphServerlinkDown	Major	The network where the cloud phone server was deployed was disconnected. Possible causes are as follows: ● The cloud phone server was stopped unexpectedly and rebooted. ● The switch was faulty. ● The gateway node was faulty.	Deploy service applications in HA mode. After the fault is rectified, check whether services recover.	Services are interrupted.
	PCIe error	cphServerPcieError	Major	The PCIe device or main board on the cloud phone server was faulty.	Deploy service applications in HA mode. After the fault is rectified, check whether services recover.	The network or disk read/write is affected.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Disk error	cphServerDiskError	Major	The disk on the cloud phone server was faulty due to ● disk backplane faults. ● disk faults.	Deploy service applications in HA mode. After the fault is rectified, check whether services recover.	Data read/write services are affected, or the BMS cannot be started.
	Storage error	cphServerStorageError	Major	The cloud phone server could not connect to EVS disks. Possible causes are as follows: ● SDI card faults ● Remote storage devices were faulty.	Deploy service applications in HA mode. After the fault is rectified, check whether services recover.	Data read/write services are affected, or the BMS cannot be started.
	GPU offline	cphServerGpuOffline	Major	GPU of the cloud phone server was loose and disconnected.	Stop the cloud phone server and reboot it.	Faults occur on cloud phones whose GPUs are disconnected. Cloud phones cannot run properly even if they are restarted or reconfigured.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	GPU timeout	cphServerGpuTimeOut	Major	GPU of the cloud phone server timed out.	Reboot the cloud phone server.	Cloud phones whose GPUs timed out cannot run properly and are still faulty even if they are restarted or reconfigured.
	Disk space full	cphServerDiskFull	Major	Disk space of the cloud phone server was used up.	Clear the application data in the cloud phone to release space.	Cloud phone is sub-healthy, prone to failure, and unable to start.
	Disk readonly	cphServerDiskReadOnly	Major	The disk of the cloud phone server became read-only.	Reboot the cloud phone server.	Cloud phone is sub-healthy, prone to failure, and unable to start.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Cloud phone metadata damaged	cphPhoneMetaDataDamage	Major	Cloud phone metadata was damaged.	Contact O&M personnel.	The cloud phone cannot run properly even if it is restarted or reconfigured.
	GPU failed	gpuAbnormal	Critical	The GPU was faulty.	Submit a service ticket.	Services are interrupted.
	GPU recovered	gpuNormal	Informational	The GPU was running properly.	No further action is required.	N/A
	Kernel crash	kernelCrash	Critical	The kernel log indicated crash.	Submit a service ticket.	Services are interrupted during the crash.
	Kernel OOM	kernelOom	Major	The kernel log indicated out of memory.	Submit a service ticket.	Services are interrupted.
	Hardware malfunction	hardwareError	Critical	The kernel log indicated **Hardware Error**.	Submit a service ticket.	Services are interrupted.
	PCIe error	pcieAer	Critical	The kernel log indicated **PCIe Bus Error**.	Submit a service ticket.	Services are interrupted.
	SCSI error	scsiError	Critical	The kernel log indicated SCSI Error.	Submit a service ticket.	Services are interrupted.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Image storage became read-only	partReadOnly	Critical	The image storage became read-only.	Submit a service ticket.	Services are interrupted.
	Image storage superblock damaged	badSuperBlock	Critical	The superblock of the file system of the image storage was damaged.	Submit a service ticket.	Services are interrupted.
	Image storage /.sharedpath/master became read-only	isuladMasterReadOnly	Critical	Mount point /.sharedpath/master of the image storage became read-only.	Submit a service ticket.	Services are interrupted.
	Cloud phone data disk became read-only	cphDiskReadOnly	Critical	The cloud phone data disk became read-only.	Submit a service ticket.	Services are interrupted.
	Cloud phone data disk superblock damaged	cphDiskBadSuperBlock	Critical	The superblock of the file system of the cloud phone data disk was damaged.	Submit a service ticket.	Services are interrupted.

Table 8-19 Layer 2 Connection Gateway (L2CG)

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
L2CG	IP addresses conflicted	IPConflict	Major	A cloud server and an on-premises server that need to communicate use the same IP address.	Check the ARP and switch information to locate the servers that have the same IP address and change the IP address.	The communications between the on-premises and cloud servers may be abnormal.

Table 8-20 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 8-21 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

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	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.
	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 8-22 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

Event Source	Event Name	Event ID	Event Severity
	Identity provider created	createIdentityProvider	Minor
	Identity provider deleted	deleteIdentityProvider	Major
	Identity provider updated	updateIdentityProvider	Minor
	Metadata updated	updateMetadata	Minor
	Security policy updated	updateSecurityPolicies	Major
	Credential added	addCredential	Major
	Credential deleted	deleteCredential	Major
	Project created	createProject	Minor
	Project updated	updateProject	Minor
	Project suspended	suspendProject	Major

Table 8-23 Data Encryption Workshop (DEW)

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

Table 8-24 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

Event Source	Event Name	Event ID	Event Severity
	Bucket policy configured	setBucketPolicy	Minor

Table 8-25 Cloud Eye

Event Source	Event Name	Event ID	Event Severity	Description	Solution
Cloud Eye	Agent heartbeat interruption	agentHeartbeatInterrupted	Major	The Agent sends a heartbeat message to Cloud Eye every minute. If Cloud Eye cannot receive a heartbeat for 3 minutes, **Agent Status** is displayed as **Faulty**.	• Confirm that the Agent domain name cannot be resolved. • Check whether your account is in arrears. • The Agent process is faulty. Restart the Agent. If the Agent process is still faulty after the restart, the Agent files may be damaged. In this case, reinstall the Agent. • Confirm that the server time is inconsistent with the local standard time. • Update the Agent to the latest version.

Table 8-26 DataSpace

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
DataSpace	New revision	newRevision	Minor	An updated version was released.	After receiving the notification, export the data of the updated version as required.	None.

Table 8-27 Enterprise Switch

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
Enterprise Switch	IP addresses conflicted	IPConflict	Major	A cloud server and an on-premises server that need to communicate use the same IP address.	Check the ARP and switch information to locate the servers that have the same IP address and change the IP address.	The communications between the on-premises and cloud servers may be abnormal.

Table 8-28 Distributed Cache Service (DCS)

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
DCS	Full synchronization during online migration retry	migrationFullResync	Minor	If online migration fails, full synchronization will be triggered because incremental synchronization cannot be performed.	To check whether repeated full retries occur, check whether the network connection to the source instance is normal and whether the source instance is overloaded. If full retry is repeatedly performed, contact O&M personnel.	The migration task is interrupted from the source instance, triggering full synchronization again. As a result, the CPU usage of the source instance may increase sharply.
	Redis master/replica switchover	masterStandbyFailover	Minor	The master node was abnormal, promoting a replica to master.	Check the original master node and rectify the fault.	None
	Memcached master/standby switchover	memcachedMasterStandbyFailover	Minor	The master node was abnormal, promoting the standby node to master.	Check whether services are normal. If the application is not recovered, restart the application to recover it.	The persistent connection of the instance is interrupted.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Redis server exception	redisNodeStatusAbnormal	Major	The Redis server status was abnormal.	Check whether services are affected. If yes, contact O&M personnel.	The node status is abnormal. If the active node is abnormal, the active/standby switchover is automatically performed. The standby node is abnormal. If the client directly connects to the standby node for read/write splitting, the read operation will be abnormal.
	Redis server recovered	redisNodeStatusNormal	Major	The Redis server status recovered.	Check whether services are restored. If the application is not reconnected, restart the application.	The status of the Redis server returns to normal.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Synchronization failure in data migration	migrateSyncDataFail	Major	Online migration failed.	Configure the migrate task again and execute it. If the fault persists, contact O&M personnel.	Data migration fails.
	Memcached instance abnormal	memcachedInstanceStatusAbnormal	Major	The Memcached node status was abnormal.	Check whether services are affected. If yes, contact O&M personnel.	The DCS Memcached instance is abnormal and may be inaccessible.
	Memcached instance recovered	memcachedInstanceStatusNormal	Major	The Memcached node status recovered.	Check whether services are restored. If the application is not reconnected, restart the application.	The status of the Memcached node returns to normal.
	Instance backup failure	instanceBackupFailure	Major	The DCS instance fails to be backed up due to an OBS access failure.	Try manual backup.	Automatic backup fails.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Instance node abnormal restart	instanceNodeAbnormalRestart	Major	DCS nodes restarted unexpectedly when they became faulty.	Check whether services are restored. If the application is not reconnected, restart the application.	The persistent connection of the instance is interrupted.
	Long-running Lua scripts stopped	scriptsStopped	Informational	Lua scripts that had timed out automatically stopped running.	Optimize the **lua** scrip to prevent execution timeout.	The execution of the lua scripts takes a long time and is forcibly interrupted. If the execution of the lua scripts takes a long time, the entire instance is blocked.
	Node restarted	nodeRestarted	Informational	After write operations had been performed, the node automatically restarted to stop Lua scripts that had timed out.	Check whether services are normal. If the application is not recovered, restart the application to recover it.	The persistent connection of the instance is interrupted.

Table 8-29 Intelligent Cloud Access (ICA)

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
ICA	BGP peer disconnection	BgpPeerDisconnection	Major	The BGP peer is disconnected.	Log in to the gateway and locate the cause.	Service traffic may be interrupted.
	BGP peer connection success	BgpPeerConnectionSuccess	Major	The BGP peer is successfully connected.	None	None
	Abnormal GRE tunnel status	AbnormalGreTunnelStatus	Major	The GRE tunnel status is abnormal.	Log in to the gateway and locate the cause.	Service traffic may be interrupted.
	Normal GRE tunnel status	NormalGreTunnelStatus	Major	The GRE tunnel status is normal.	None	None
	WAN interface goes up	EquipmentWanGoingOnline	Major	The WAN interface goes online.	None	None
	WAN interface goes down	EquipmentWanGoingOffline	Major	The WAN interface goes offline.	Check whether the event is caused by a manual operation or device fault.	The device cannot be used.
	Intelligent enterprise gateway going online	IntelligentEnterpriseGatewayGoingOnline	Major	The intelligent enterprise gateway goes online.	None	None

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Intelligent enterprise gateway going offline	IntelligentEnterpriseGatewayGoingOffline	Major	The intelligent enterprise gateway goes offline.	Check whether the event is caused by a manual operation or device fault.	The device cannot be used.

Table 8-30 Multi-Site High Availability Service (MAS)

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
MAS	Abnormal database instance	dbError	Major	Abnormal database instance is detected by MAS.	Log in to the MAS console to view the cause and rectify the fault.	Services are interrupted.
	Database instance recovered	dbRecovery	Major	The database instance is recovered.	None	Services are interrupted.
	Abnormal Redis instance	redisError	Major	Abnormal Redis instance is detected by MAS.	Log in to the MAS console to view the cause and rectify the fault.	Services are interrupted.
	Redis instance recovered	redisRecovery	Major	The Redis instance is recovered.	None	Services are interrupted.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Abnormal MongoDB database	mongodbError	Major	Abnormal MongoDB database is detected by MAS.	Log in to the MAS console to view the cause and rectify the fault.	Services are interrupted.
	MongoDB database recovered	mongodbRecovery	Major	The MongoDB database is recovered.	None	Services are interrupted.
	Abnormal Elasticsearch instance	esError	Major	Abnormal Elasticsearch instance is detected by MAS.	Log in to the MAS console to view the cause and rectify the fault.	Services are interrupted.
	Elasticsearch instance recovered	esRecovery	Major	The Elasticsearch instance is recovered.	None	Services are interrupted.
	Abnormal API	apiError	Major	The abnormal API is detected by MAS.	Log in to the MAS console to view the cause and rectify the fault.	Services are interrupted.
	API recovered	apiRecovery	Major	The API is recovered.	None	Services are interrupted.
	Area status changed	netChange	Major	Area status changes are detected by MAS.	Log in to the MAS console to view the cause and rectify the fault.	Network of the multi-active areas may change.

Table 8-31 Resource Management Service (RMS)

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
RMS	Configuration noncompliance notification	configurationNoncomplianceNotification	Major	The assignment evaluation result is **Non-compliant**.	Modify the noncompliant configuration items of the resource.	None
	Configuration compliance notification	configurationComplianceNotification	Informational	The assignment evaluation result changed to be **Compliant**.	None	None

Table 8-32 Cloud Storage Gateway (CSG)

Event Source	Event Name	Event ID	Event Severity	Description
CSG	Abnormal CSG process status	gatewayProcessStatusAbnormal	Major	This event is triggered when an exception occurs in the CSG process status.
	Abnormal CSG connection status	gatewayToServiceConnectAbnormal	Major	This event is triggered when no CSG status report is returned for five consecutive periods.
	Abnormal connection status between CSG and OBS	gatewayToObsConnectAbnormal	Major	This event is triggered when CSG cannot connect to OBS.
	Read-only file system	gatewayFileSystemReadOnly	Major	This event is triggered when the partition file system on CSG becomes read-only.

Event Source	Event Name	Event ID	Event Severity	Description
	Read-only file share	gatewayFileShareReadOnly	Major	This event is triggered when the file share becomes read-only due to insufficient cache disk storage space.

Table 8-33 MapReduce Service (MRS)

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
MRS	DBServer Switchover	dbServerSwitchover	Minor	The DBServer switchover occurs.	Confirm with O&M personnel whether the active/standby switchover is caused by normal operations.	Consecutive active/standby switchovers may affect Hive service availability.
	Flume Channel overflow	flumeChannelOverflow	Minor	Flume Channel overflow	Check whether the Flume channel configuration is proper and whether the service volume increases sharply.	Flume tasks cannot write data to the backend.
	NameNode Switchover	namenodeSwitchover	Minor	The NameNode switchover occurs.	Confirm with O&M personnel whether the active/standby switchover is caused by normal operations.	Consecutive active/standby switchovers may cause HDFS file read/write failures.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	ResourceManager Switchover	resourceManagerSwitchover	Minor	ResourceManager Switchover	Confirm with O&M personnel whether the active/standby switchover is caused by normal operations.	Consecutive active/standby switchovers may cause exceptions or even failures of YARN tasks.
	JobHistory Server Switchover	jobHistoryServerSwitchover	Minor	The JobHistoryServer switchover occurs.	Confirm with O&M personnel whether the active/standby switchover is caused by normal operations.	Consecutive active/standby switchovers may cause failures to read MapReduce task logs.
	HMaster Failover	hmasterFailover	Minor	The HMaster failover occurs.	Confirm with O&M personnel whether the active/standby switchover is caused by normal operations.	Consecutive active/standby switchovers may affect HBase service availability.
	Hue Failover	hueFailover	Minor	The Hue failover occurs.	Confirm with O&M personnel whether the active/standby switchover is caused by normal operations.	The active/standby switchover may affect the display of the HUE page.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Impala HaProxy Failover	impalaHaProxyFailover	Minor	The Impala HaProxy switchover occurs.	Confirm with O&M personnel whether the active/standby switchover is caused by normal operations.	Consecutive active/standby switchovers may affect Impala service availability.
	Impala StateStore Catalog Failover	impalaStateStoreCatalogFailover	Minor	The Impala StateStoreCatalog failover occurs.	Confirm with O&M personnel whether the active/standby switchover is caused by normal operations.	Consecutive active/standby switchovers may affect Impala service availability.
	LdapServer Failover	ldapServerFailover	Minor	The LdapServer failover occurs.	Confirm with O&M personnel whether the active/standby switchover is caused by normal operations.	Consecutive active/standby switchovers may affect LdapServer service availability.
	Loader Switchover	loaderSwitchover	Minor	The Loader switchover occurs.	Confirm with O&M personnel whether the active/standby switchover is caused by normal operations.	The active/standby switchover may affect Loader service availability.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Manager Switchover	managerSwitchover	Informational	The Manager switchover occurs.	Confirm with O&M personnel whether the active/standby switchover is caused by normal operations.	The active/standby Manager switchover may cause the Manager page inaccessible and abnormal values of some monitoring items.
	Job Running Failed	jobRunningFailed	Warning	A job fails to be executed.	On the **Jobs** tab page, check whether the failed task is normal.	The job fails to be executed.
	Job Killed	jobkilled	Informational	The job is terminated.	Check whether the task is manually terminated.	The job execution process is terminated.
	Oozie Workflow Execution Failure	oozieWorkflowExecutionFailure	Minor	Oozie workflows fail to execute.	View Oozie logs to locate the failure cause.	Oozie workflows fail to execute.
	Oozie Scheduled Job Execution Failure	oozieScheduledJobExecutionFailure	Minor	Oozie scheduled tasks fail to execute.	View Oozie logs to locate the failure cause.	Oozie scheduled tasks fail to execute.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	ClickHouse Service Unavailable	clickHouseServiceUnavailable	Critical	The ClickHouse service is unavailable.	For details, see section "ALM-45425 ClickHouse Service Unavailable" in *MapReduce Service User Guide*.	The ClickHouse service is abnormal. Cluster operations cannot be performed on the ClickHouse service on FusionInsight Manager, and the ClickHouse service function cannot be used.
	DBService Service Unavailable	dbServiceServiceUnavailable	Critical	DBService is unavailable	For details, see section "ALM-27001 DBService Service Unavailable" in *MapReduce Service User Guide*.	The database service is unavailable and cannot provide data import and query functions for upper-layer services. As a result, service exceptions occur.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	DBService Heartbeat Interruption Between the Active and Standby Nodes	dbServiceHeartbeatInterruptionBetweentheActiveAndStandbyNodes	Major	DBService Heartbeat Interruption Between the Active and Standby Nodes	For details, see section "ALM-27003 Heartbeat Interruption Between the Active and Standby Nodes" in *MapReduce Service User Guide*.	During the DBService heartbeat interruption, only one node can provide the service. If this node is faulty, no standby node is available for failover and the service is unavailable.
	Data Inconsistency Between Active and Standby DBServices	dataInconsistencyBetweenActiveAndStandbyDBServices	Critical	Data Inconsistency Between Active and Standby DBServices	For details, see section "ALM-27004 Data Inconsistency Between Active and Standby DBService" in *MapReduce Service User Guide*.	When data is not synchronized between the active and standby DBServices, the data may be lost or abnormal if the active instance becomes abnormal.
	Database Enters the Read-Only Mode	databaseEnterstheReadOnlyMode	Critical	The database enters the read-only mode.	For details, see section "ALM-27007 Database Enters the Read-Only Mode" in *MapReduce Service User Guide*.	The database enters the read-only mode, causing service data loss.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Flume Service Unavailable	flumeService Unavailable	Critical	Flume Service Unavailable	For details, see section "ALM-24000 Flume Service Unavailable" in *MapReduce Service User Guide*.	Flume is running abnormally and the data transmission service is interrupted.
	Flume Agent Exception	flume Agent Exception	Major	The Flume Agent is abnormal.	For details, see section "ALM-24001 Flume Agent Exception" in *MapReduce Service User Guide*.	The Flume agent instance for which the alarm is generated cannot provide services properly, and the data transmission tasks of the instance are temporarily interrupted. Real-time data is lost during real-time data transmission.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Flume Client Disconnection Alarm	flumeClientDisconnected	Major	Flume Client Disconnection Alarm	For details, see section "ALM-24003 Flume Client Interrupted" in *MapReduce Service User Guide*.	The Flume Client for which the alarm is generated cannot communicate with the Flume Server and the data of the Flume Client cannot be sent to the Flume Server.
	Exception Occurs When Flume Reads Data	exceptionOccursWhenFlumeReadsData	Major	Exceptions occur when flume reads data.	For details, see section "ALM-24004 Exception Occurs When Flume Reads Data" in *MapReduce Service User Guide*.	If data is found in the data source and Flume Source continuously fails to read data, the data collection is stopped.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Exception Occurs When Flume Transmits Data	exceptionOccursWhenFlumeTransmitsData	Major	Exceptions occur when flume transmits data.	For details, see section "ALM-24005 Exception Occurs When Flume Transmits Data" in *MapReduce Service User Guide*.	If the disk usage of Flume Channel increases continuously, the time required for importing data to a specified destination prolongs. When the disk usage of Flume Channel reaches 100%, the Flume agent process pauses.
	Flume Certificate File Is Invalid	flumeCertificateFileIsinvalid	Major	The Flume certificate file is invalid or damaged.	For details, see section "ALM-24010 Flume Certificate File Is Invalid or Damaged" in *MapReduce Service User Guide*.	The Flume certificate file is invalid or damaged, and the Flume client cannot access the Flume server.
	Flume Certificate File Is About to Expire	flumeCertificateFileIsAboutToExpire	Major	The Flume certificate file is about to expire.	For details, see section "ALM-24011 Flume Certificate File Is About to Expire" in *MapReduce Service User Guide*.	The Flume certificate file is about to expire, which has no adverse impact on the system.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Flume Certificate File Is Expired	flumeCertificateFileIsExpired	Major	The Flume certificate file has expired.	For details, see section "ALM-24012 Flume Certificate File Has Expired" in *MapReduce Service User Guide*.	The Flume certificate file has expired and functions are restricted. The Flume client cannot access the Flume server.
	Flume MonitorServer Certificate File Is Invalid	flumeMonitorServerCertificateFileIsInvalid	Major	The Flume MonitorServer certificate file is invalid.	For details, see section "ALM-24013 Flume MonitorServer Certificate File Is Invalid or Damaged" in *MapReduce Service User Guide*.	The MonitorServer certificate file is invalid or damaged, and the Flume client cannot access the Flume server.
	Flume MonitorServer Certificate File Is About to Expire	flumeMonitorServerCertificateFileIsAboutToExpire	Major	The Flume MonitorServer certificate file is about to expire.	For details, see section "ALM-24014 Flume MonitorServer Certificate Is About to Expire" in *MapReduce Service User Guide*.	The MonitorServer certificate is about to expire, which has no adverse impact on the system.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Flume MonitorServer Certificate File Is Expired	flumeMonitorServerCertificateFileIsExpired	Major	The Flume MonitorServer certificate file has expired.	For details, see section "ALM-24015 Flume MonitorServer Certificate File Has Expired" in *MapReduce Service User Guide*.	The MonitorServer certificate file has expired and functions are restricted. The Flume client cannot access the Flume server.
	HDFS Service Unavailable	hdfsServiceUnavailable	Critical	The HDFS service is unavailable.	For details, see section "ALM-14000 HDFS Service Unavailable" in *MapReduce Service User Guide*.	HDFS fails to provide services for HDFS service-based upper-layer components, such as HBase and MapReduce. As a result, users cannot read or write files.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	NameService Service Unavailable	nameServiceService Unavailable	Major	The NameService service is abnormal.	For details, see section "ALM-14010 NameService Service Is Abnormal" in *MapReduce Service User Guide*.	HDFS fails to provide services for upper-layer components based on the NameService service, such as HBase and MapReduce. As a result, users cannot read or write files.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	DataNode Data Directory Is Not Configured Properly	datanodeDataDirectoryIsNotConfiguredProperly	Major	The DataNode data directory is not configured properly.	For details, see section "ALM-14011 DataNode Data Directory Is Not Configured Properly" in *MapReduce Service User Guide*.	If the DataNode data directory is mounted on critical directories such as the root directory, the disk space of the root directory will be used up after running for a long time. This causes a system fault. If the DataNode data directory is not configured properly, HDFS performance will deteriorate.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Journalnode Is Out of Synchronization	journalnodeIsOutOfSynchronization	Major	The Journalnode data is not synchronized.	For details, see section "ALM-14012 JournalNode Is Out of Synchronization" in *MapReduce Service User Guide*.	When a JournalNode is working incorrectly, data on the node is not synchronized with that on other JournalNodes. If data on more than half of JournalNodes is not synchronized, the NameNode cannot work correctly, making the HDFS service unavailable.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Failed to Update the NameNode FsImage File	failedToUpdateTheNameNodeFsImageFile	Major	The NameNode FsImage file failed to be updated.	For details, see section "ALM-14013 Failed to Update the NameNode FsImage File" in *MapReduce Service User Guide*.	If the FsImage file in the data directory of the active NameNode is not updated, the HDFS metadata combination function is abnormal and requires rectification. If it is not rectified, the Editlog files increase continuously after HDFS runs for a period. In this case, HDFS restart is time-consuming because a large number of Editlog files need to be loaded. In addition, this alarm also indicates that the standby NameNode is abnormal and the

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
						NameNode high availability (HA) mechanism becomes invalid. When the active NameNode is faulty, the HDFS service becomes unavailable.
	DataNode Disk Fault	datanodeDiskFault	Major	The DataNode disk is faulty.	For details, see section "ALM-14027 DataNode Disk Fault" in *MapReduce Service User Guide*.	If a DataNode disk fault alarm is reported, a faulty disk partition exists on the DataNode. As a result, files that have been written may be lost.
	Yarn Service Unavailable	yarnServiceUnavailable	Critical	The Yarn service is unavailable.	For details, see section "ALM-18000 Yarn Service Unavailable" in *MapReduce Service User Guide*.	The cluster cannot provide the Yarn service. Users cannot run new applications. Submitted applications cannot be run.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	NodeManager Heartbeat Lost	nodemanagerHeartbeatLost	Major	The NodeManager heartbeat is lost.	For details, see section "ALM-18002 NodeManager Heartbeat Lost" in *MapReduce Service User Guide*.	The lost NodeManager node cannot provide the Yarn service. The number of containers decreases, so the cluster performance deteriorates.
	NodeManager Unhealthy	nodemanagerUnhealthy	Major	The NodeManager is unhealthy.	For details, see section "ALM-18003 NodeManager Unhealthy" in *MapReduce Service User Guide*.	The faulty NodeManager node cannot provide the Yarn service. The number of containers decreases, so the cluster performance deteriorates.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Yarn Application Timeout	yarnApplicationTimeout	Minor	Yarn task execution timed out.	For details, see section "ALM-18020 Yarn Task Execution Timeout" in *MapReduce Service User Guide*.	The alarm persists after task execution times out. However, the task can still be properly executed, so this alarm does not exert any impact on the system.
	MapReduce Service Unavailable	mapreduceService Unavailable	Critical	The MapReduce service is unavailable.	For details, see section "ALM-18021 MapReduce Service Unavailable" in *MapReduce Service User Guide*.	The cluster cannot provide the MapReduce service. For example, MapReduce cannot be used to view task logs and the log archive function is unavailable.
	Insufficient Yarn Queue Resources	insufficientYarnQueueResources	Minor	Yarn queue resources are insufficient.	For details, see section "ALM-18022 Insufficient Yarn Queue Resources" in *MapReduce Service User Guide*.	It takes long time to end an application. A new application cannot run for a long time after submission.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	HBase Service Unavailable	hbaseServiceUnavailable	Critical	The HBase service is unavailable.	For details, see section "ALM-19000 HBase Service Unavailable" in *MapReduce Service User Guide*.	Operations cannot be performed, such as reading or writing data and creating tables.
	System Table Path or File of HBase Is Missing	systemTablePathOrFileOfHBaseIsMissing	Critical	The table directories or files of the HBase System are lost.	For details, see section "ALM-19012 HBase System Table Directory or File Lost" in *MapReduce Service User Guide*.	The HBase service fails to restart or start.
	Hive Service Unavailable	hiveServiceUnavailable	Critical	The Hive service is unavailable.	For details, see section "ALM-16004 Hive Service Unavailable" in *MapReduce Service User Guide*.	Hive cannot provide data loading, query, and extraction services.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Hive Data Warehouse Is Deleted	hiveDataWarehouseIsDeleted	Critical	The Hive data warehouse is deleted.	For details, see section "ALM-16045 Hive Data Warehouse Is Deleted" in *MapReduce Service User Guide*.	If the default Hive data warehouse is deleted, databases and tables fail to be created in the default data warehouse, affecting service usage.
	Hive Data Warehouse Permission Is Modified	hiveDataWarehousePermissionIsModified	Critical	The Hive data warehouse permissions are modified.	For details, see section "ALM-16046 Hive Data Warehouse Permission Is Modified" in *MapReduce Service User Guide*.	If the permissions on the Hive default data warehouse are modified, the permissions for users or user groups to create databases or tables in the default data warehouse are affected. The permissions will be expanded or reduced.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	HiveServer has been deregistered from zookeeper	hiveServerHasBeenDeregisteredFromZookeeper	Major	HiveServer has been deregistered from zookeeper.	For details, see section "ALM-16047 HiveServer Has Been Deregistered from ZooKeeper" in *MapReduce Service User Guide*.	If Hive configurations cannot be read from ZooKeeper, HiveServer will be unavailable.
	Tez or Spark Library Path Does Not Exist	tezlibOrSparklibIsNotExist	Major	The tez or spark library path does not exist.	For details, see section "ALM-16048 Tez or Spark Library Path Does Not Exist" in *MapReduce Service User Guide*.	The Hive on Tez and Hive on Spark functions are affected.
	Hue Service Unavailable	hueServiceUnavailable	Critical	The Hue service is unavailable.	For details, see section "ALM-20002 Hue Service Unavailable" in *MapReduce Service User Guide*.	The system cannot provide data loading, query, and extraction services.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Impala Service Unavailable	impalaServiceUnavailable	Critical	The Impala service is unavailable.	For details, see section "ALM-29000 Impala Service Unavailable" in *MapReduce Service User Guide*.	The Impala service is abnormal. Cluster operations cannot be performed on Impala on FusionInsight Manager, and Impala service functions cannot be used.
	Kafka Service Unavailable	kafkaServiceUnavailable	Critical	The Kafka service is unavailable.	For details, see section "ALM-38000 Kafka Service Unavailable" in *MapReduce Service User Guide*.	The cluster cannot provide the Kafka service, and users cannot perform new Kafka tasks.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Status of Kafka Default User Is Abnormal	statusOfKafkaDefaultUserIsAbnormal	Critical	The status of Kafka default user is abnormal.	For details, see section "ALM-38007 Status of Kafka Default User Is Abnormal" in *MapReduce Service User Guide*.	If the Kafka default user status is abnormal, metadata synchronization between Brokers and interaction between Kafka and ZooKeeper will be affected, affecting service production, consumption, and topic creation and deletion.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Abnormal Kafka Data Directory Status	abnormalKafkaDataDirectoryStatus	Major	The status of Kafka data directory is abnormal.	For details, see section "ALM-38008 Abnormal Kafka Data Directory Status" in *MapReduce Service User Guide*.	If the Kafka data directory status is abnormal, the current replicas of all partitions in the data directory are brought offline, and the data directory status of multiple nodes is abnormal at the same time. As a result, some partitions may become unavailable.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Topics with Single Replica	topicsWithSingleReplica	Warning	A topic with a single replica exists.	For details, see section "ALM-38010 Topics with Single Replica" in *MapReduce Service User Guide*.	There is the single point of failure (SPOF) risk for topics with only one replica. When the node where the replica resides becomes abnormal, the partition does not have a leader, and services on the topic are affected.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	KrbServer Service Unavailable	krbServerServiceUnavailable	Critical	The KrbServer service is unavailable.	For details, see section "ALM-25500 KrbServer Service Unavailable" in *MapReduce Service User Guide*.	When this alarm is generated, no operation can be performed for the KrbServer component in the cluster. The authentication of KrbServer in other components will be affected. The running status of components that depend on KrbServer in the cluster is faulty.
	Kudu Service Unavailable	kuduService Unavailable	Critical	The Kudu service is unavailable.	For details, see section "ALM-29100 Kudu Service Unavailable" in *MapReduce Service User Guide*.	Users cannot use the Kudu service.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	LdapServer Service Unavailable	ldapServerServiceUnavailable	Critical	The LdapServer service Is unavailable.	For details, see section "ALM-25000 LdapServer Service Unavailable" in *MapReduce Service User Guide*.	When this alarm is generated, no operation can be performed for the KrbServer users and LdapServer users in the cluster. For example, users, user groups, or roles cannot be added, deleted, or modified, and user passwords cannot be changed on the FusionInsight Manager portal. The authentication for existing users in the cluster is not affected.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Abnormal LdapServer Data Synchronization	abnormalLdapServerData Synchronization	Critical	The LdapServer data synchronization is abnormal.	For details, see section "ALM-25004 Abnormal LdapServer Data Synchronization" in *MapReduce Service User Guide*.	LdapServer data inconsistency occurs because LdapServer data on Manager or in the cluster is damaged. The LdapServer process with damaged data cannot provide services externally, and the authentication functions of Manager and the cluster are affected.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Nscd Service Is Abnormal	nscdServiceIsAbnormal	Major	The Nscd service is abnormal.	For details, see section "ALM-25005 nscd Service Exception" in *MapReduce Service User Guide*.	If the Nscd service is abnormal, the node may fail to synchronize data from an LDAP server. In this case, running the id command may fail to obtain data from an LDAP server, affecting upper-layer services.
	Sssd Service Is Abnormal	sssdServiceIsAbnormal	Major	The Sssd service is abnormal.	For details, see section "ALM-25006 Sssd Service Exception" in *MapReduce Service User Guide*.	If the Sssd service is abnormal, the node may fail to synchronize data from LdapServer. In this case, running the id command may fail to obtain LDAP data, affecting upper-layer services.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Loader Service Unavailable	loaderService Unavailable	Critical	The Loader service is unavailable.	For details, see section "ALM-23001 Loader Service Unavailable" in *MapReduce Service User Guide*.	When the Loader service is unavailable, the data loading, import, and conversion functions are unavailable.
	Oozie Service Unavailable	oozieService Unavailable	Critical	The Oozie service is unavailable.	For details, see section "ALM-17003 Oozie Service Unavailable" in *MapReduce Service User Guide*.	The Oozie service cannot be used to submit jobs.
	Ranger Service Unavailable	rangerService Unavailable	Critical	The Ranger service is unavailable.	For details, see section "ALM-45275 Ranger Service Unavailable" in *MapReduce Service User Guide*.	When the Ranger service is unavailable, the Ranger cannot work properly and the native UI of the Ranger cannot be accessed.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Abnormal RangerAdmin status	abnormalRangerAdminStatus	Major	The RangerAdmin status is abnormal.	For details, see section "ALM-45276 Abnormal RangerAdmin Status" in *MapReduce Service User Guide*.	If the status of a single RangerAdmin is abnormal, the access to the Ranger native UI is not affected. If the status of two RangerAdmins is abnormal, the Ranger native UI cannot be accessed and operations such as creating, modifying, and deleting policies cannot be performed.
	Spark2x Service Unavailable	spark2xServiceUnavailable	Critical	The Spark2x service is unavailable.	For details, see section "ALM-43001 Spark2x Service Unavailable" in *MapReduce Service User Guide*.	The Spark tasks submitted by users fail to be executed.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Storm Service Unavailable	stormService Unavailable	Critical	The Storm service is unavailable.	For details, see section "ALM-26051 Storm Service Unavailable" in *MapReduce Service User Guide*.	The cluster cannot provide the Storm service externally, and users cannot execute new Storm tasks.
	ZooKeeper Service Unavailable	zooKeeperServiceUnavailable	Critical	The ZooKeeper service is unavailable.	For details, see section "ALM-13000 ZooKeeper Service Unavailable" in *MapReduce Service User Guide*.	ZooKeeper fails to provide coordination services for upper-layer components and the components depending on ZooKeeper may not run properly.
	Failed to Set the Quota of Top Directories of ZooKeeper Component	failedToSetTheQuotaOfTopDirectoriesOfZooKeeperComponent	Minor	The quota of top directories of ZooKeeper components failed to be configured.	For details, see section "ALM-13005 Failed to Set the Quota of Top Directories of ZooKeeper Components" in *MapReduce Service User Guide*.	Components can write a large amount of data to the top-level directory of ZooKeeper. As a result, the ZooKeeper service is unavailable.

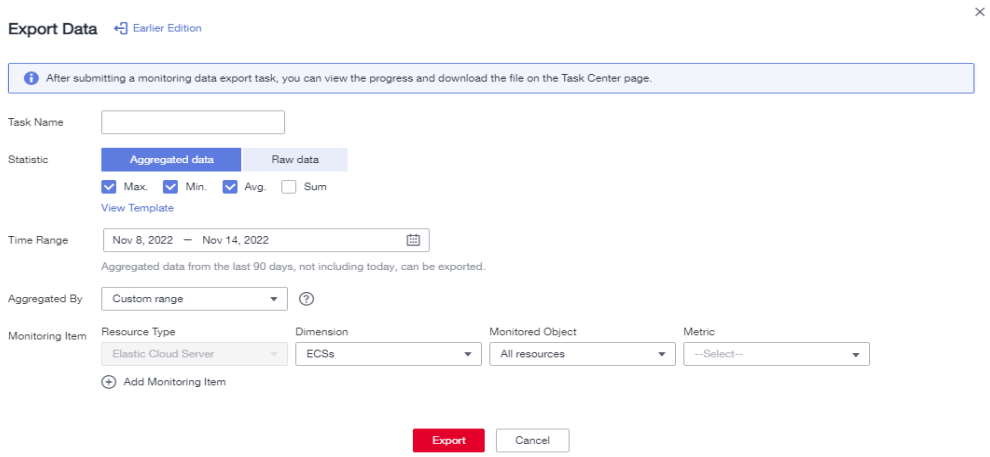
9 Task Center

On the **Task Center** page, you can export data including monitoring data and alarm records. You can go to the **Alarm Records** and **Server Monitoring** pages to create an export task. After the export task is submitted, you can view the progress and download the file on the **Task Center** page.

Exporting Monitoring Data

1. Log in to the management console.
2. Choose **Service List** > **Cloud Eye**.
3. In the navigation pane on the left, choose **Server Monitoring** > **Elastic Cloud Server**.
4. Click **Export Data** in the upper right corner.

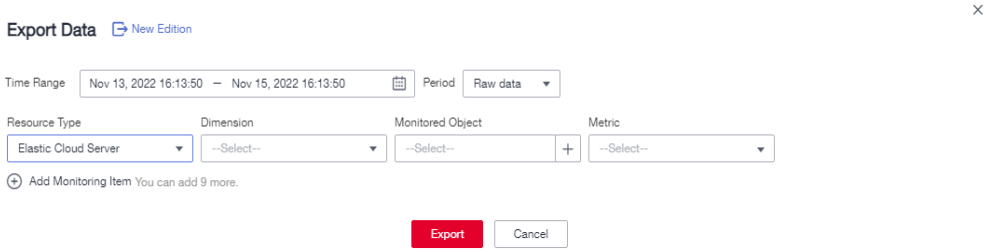
Figure 9-1 Exporting data



NOTE

By default, the page of the new edition is displayed. To return to the earlier edition, click **Earlier Edition**. In the earlier edition, the data export task is not displayed on the **Task Center** page and can be downloaded on the current page.

Figure 9-2 Earlier edition of the **Export Data** page



5. On the **Export Data** page, set parameters as prompted.

Table 9-1 Configuring parameters for exporting data

Parameter	Description
Task Name	Name of an export task. It contains 1 to 32 characters.
Statistic	There are two modes: **Aggregated data** and **Raw data**. ● **Aggregated data**: Data can be exported after being aggregated using the maximum value, minimum value, average value, or sum value. ● **Raw data**: The original data is exported.
Time Range	Select the time range for the data to be exported. ● Data of a maximum of the last 90 days can be exported for an aggregate value. ● Raw data from the last 48 hours is available for export.
Aggregated By	This parameter is mandatory when **Statistics** is set to **Aggregate data**. If you select **Custom range**, data aggregated during your configured time range will be exported. If you select one of the other options, data will be aggregated based on your selected granularity and then exported.
Monitoring Item	● **Resource Type**: The default value is **Elastic Cloud Server**. You do not need to set this parameter. ● **Dimension**: Specify the dimension name of the metric to be exported. ● **Monitored Object**: You can select **All Resources** or **Specific resources**. ● **Metric**: Specify the metric to be exported.

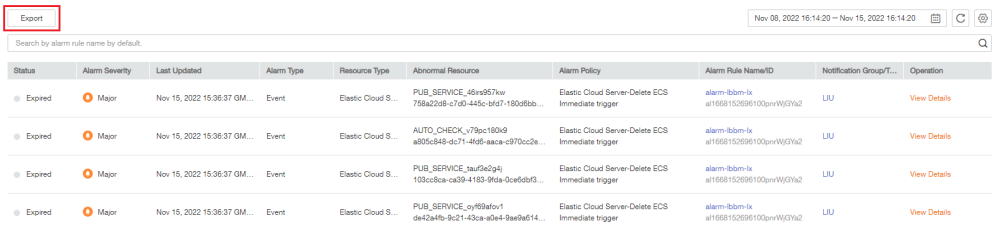
6. After the configuration is complete, click **Export**.
7. After the export task is submitted, you can view and download the monitoring data under the **Monitoring Data Export Tasks** tab on the **Task Center** page.

Figure 9-3 Viewing export tasks

Exporting Alarm Records

1. Log in to the management console.
2. Choose **Service List** > **Cloud Eye**.
3. Choose **Alarm Management** > **Alarm Records**.
4. On the **Alarm Records** page, click **Export**.

Figure 9-4 Alarm Records page



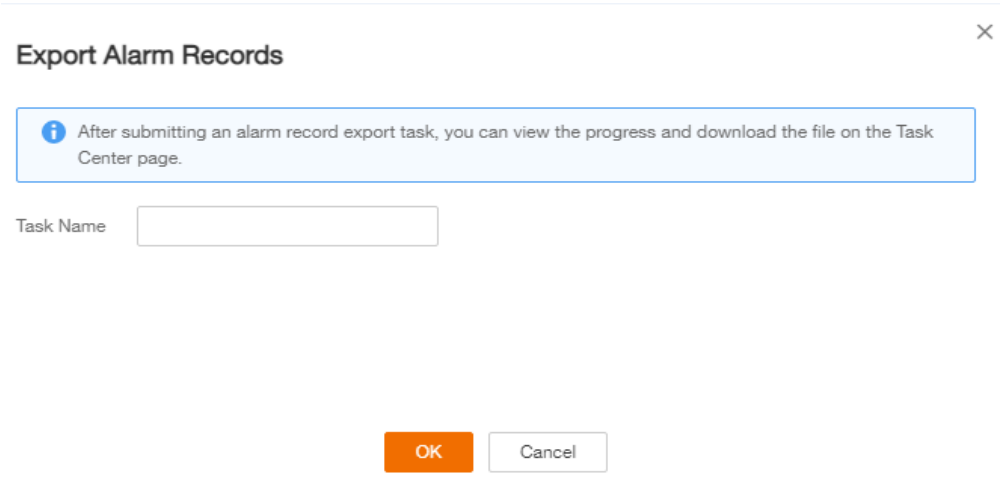
NOTE

You can export all alarm records or alarm records filtered by status, alarm severity, alarm rule name, resource type, resource ID, and alarm rule ID above the alarm record list.

5. In the displayed **Export Alarm Records** dialog box, enter an export task name and click **OK**.

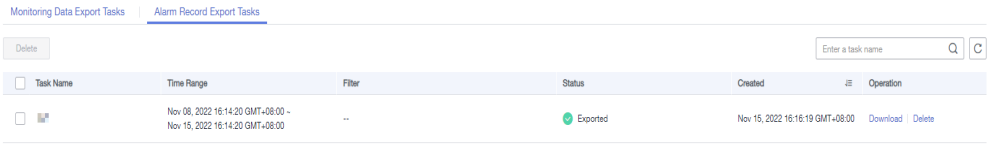
   The task name contains 1 to 32 characters.

Figure 9-5 Entering an export task name



6. After the export task is submitted, you can view and download the alarm records under the **Alarm Record Export Task** tab on the **Task Center** page.

Figure 9-6 Viewing export tasks



10 Data Dump

10.1 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.

Figure 10-1 Adding a dump task

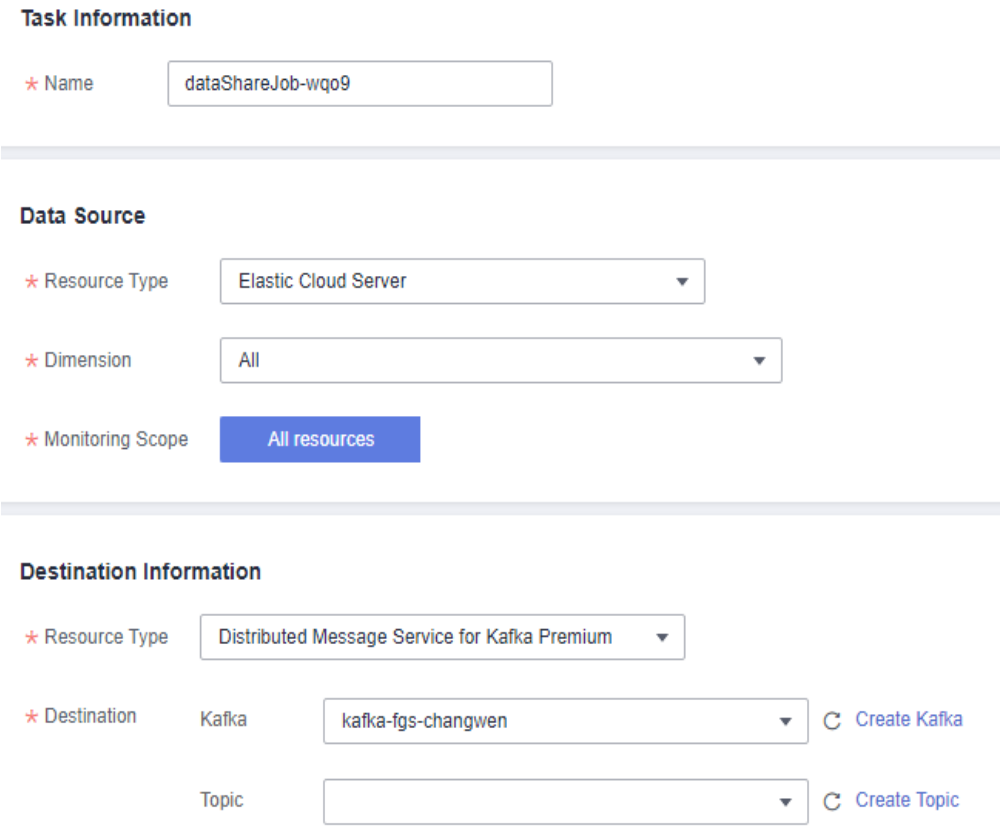


Table 10-1 Dump task parameters

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**
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.

Parameter	Description
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**.

10.2 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**.

11 Cloud Service Monitoring

11.1 Introduction to Cloud Service Monitoring

Scenarios

Cloud Service Monitoring collects data of built-in metrics of cloud services. You can monitor these metrics to track the status of corresponding cloud services. On the **Cloud Service Monitoring** page, in addition to viewing monitoring data, you can also create alarm rules and export raw data.

What You Can Do with Cloud Service Monitoring

- Viewing metrics: On the page displaying metrics, you can view graphs of raw data collected from lats 1 hour, 3 hours, 12 hours, and 24 hours. You can customize the metrics to be viewed and view monitoring data that is automatically refreshed.
- Creating an alarm rule: You can configure alarm rules for key metrics of cloud services. When the conditions in the alarm rule are met, Cloud Eye sends emails, SMS messages, and HTTP/HTTPS requests, enabling you to quickly respond to resource changes.
- Exporting monitoring data: Cloud Service Monitoring allows you to export a maximum of 10 monitoring items in your selected time range and rollup period. The exported monitoring report contains the username, region name, service name, instance name, instance ID, metric name, metric data, time, and timestamp, facilitating query and filtering.

11.2 Viewing Metrics

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 the cloud service whose resources you want to view.
4. Locate the target cloud service resource, in the **Operation** column, click **View Metric**.

NOTE

- You can sort graphs by dragging them based on service requirements.
- If **Auto Refresh** is enabled, data is automatically refreshed every minute.
- 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.
- You can search for a specific metric in the search box.
- To export monitoring data, see **How Can I Export Collected Data?**.

5. Near the top right corner of the page, click **Select Metric**.

   The **Select Metric** dialog box is displayed.

   Select at least one metric. Drag and drop the selected metrics at desired locations to sort them. This helps you customize metrics to be viewed.

6. 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.

   NOTE

   - If you select **1h**, **3h**, **12h**, or **1d**, raw data is displayed by default. You can set **Period** and **Statistic** to change the rollup period of monitoring data. For details about rollup periods, see **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.

7. In the upper right corner of the monitoring graph, click  to create alarm rules for the metric. For details about the parameters, see **Creating an Alarm Rule**.

12 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.

12.1 Key Cloud Eye Operations

Table 12-1 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

12.2 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.

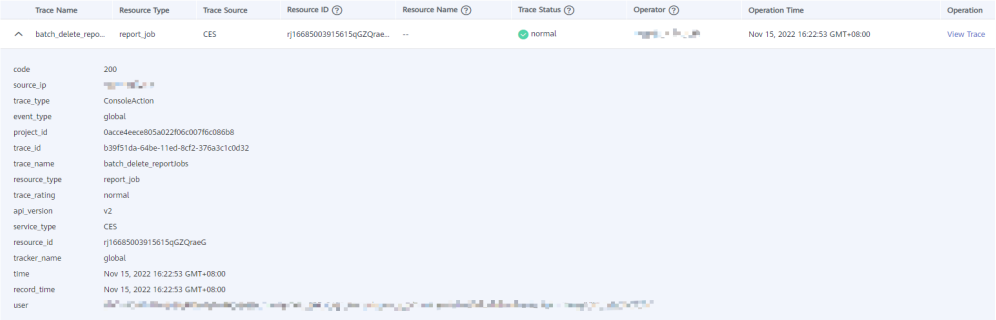
     After you select **Trace name** for **Search By**, you also need to select a trace name.

     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.

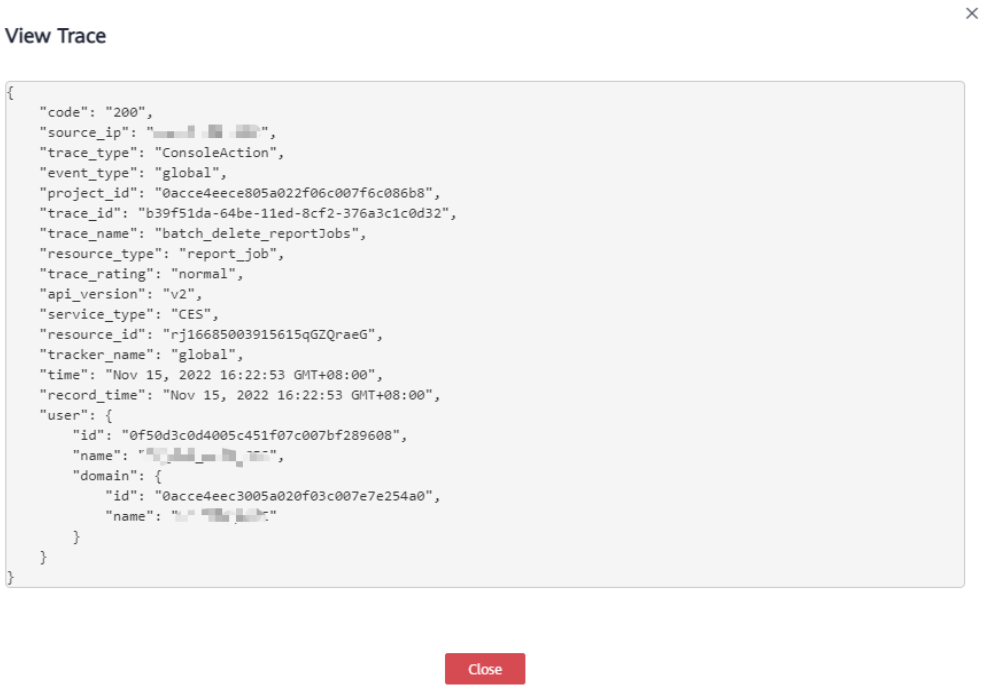
Figure 12-1 Expanding trace details

Figure 12-2 Expanding trace details



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

Figure 12-3 View Trace



13 Permissions Management

13.1 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 13-1**).

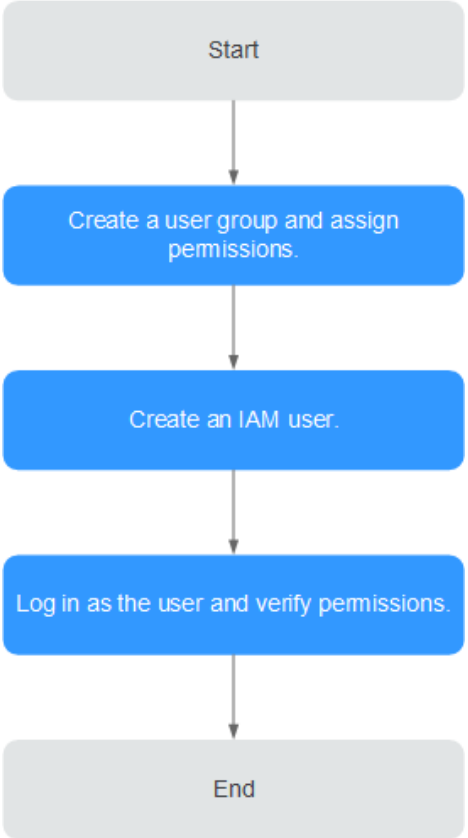
Prerequisites

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 13-1 Process for granting Cloud Eye permissions



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 an IAM user and log in**.

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

3. **Log in** 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.

13.2 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"
        }
    ]
}
```

14 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.

15 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
Network	Elastic IP and bandwidth	SYS.VPC	VPC metrics
	Elastic Load Balance	SYS.ELB	ELB metrics
	NAT Gateway	SYS.NAT	NAT Gateway metrics
Application	Distributed Message Service	SYS.DMS	DMS metrics (Kafka) DMS metrics (RabbitMQ)
	Distributed Cache Service	SYS.DCS	DCS metrics
Database	Relational Database Service	SYS.RDS	RDS for MySQL metrics RDS for PostgreSQL metrics

Category	Service	Namespace	Reference
	Document Database Service	SYS.DDS	**DDS metrics**
Enterprise Intelligence	Cloud Search Service	SYS.ES	**CSS metrics**

16 FAQs

16.1 General Consulting

16.1.1 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.

16.1.2 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 16-1 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.

16.1.3 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.

16.1.4 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, period, 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**.

16.1.5 Which Services Does Cloud Eye Support Permission- and Region-based Monitoring in the Enterprise Project Dimension?

Currently, resources of the following services can be monitored by Cloud Eye based on the permissions configured for the enterprise project they belong to and the region where the enterprise project is located: ECS, AS, EVS, EIP, ELB, RDS, DCS, DDS, and DMS.

16.1.6 Which Cloud Eye Resources Support the Enterprise Project Feature?

Currently, the monitoring panels, graphs, alarm rules, and resource groups of Cloud Eye support the enterprise project feature..

16.1.7 Why Can a User of an Enterprise Project View the Resource Information of the Account on the Overview Page?

The Cloud Eye Overview page does not support query by enterprise project.

16.2 Server Monitoring

16.2.1 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**.

16.2.2 How Can I Make a Newly Purchased ECS monitor its OS?

Scenarios

This topic describes how to make the newly purchased ECS monitor its OS.

NOTE

A private image can only be used in the region where it is created. If it is used in other regions, no monitoring data will be generated for the ECSs created from this private image.

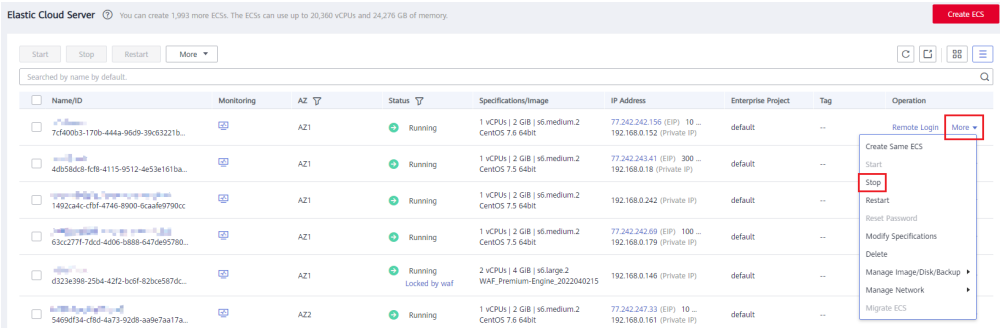
Prerequisites

An ECS with the Agent installed is available.

Procedure

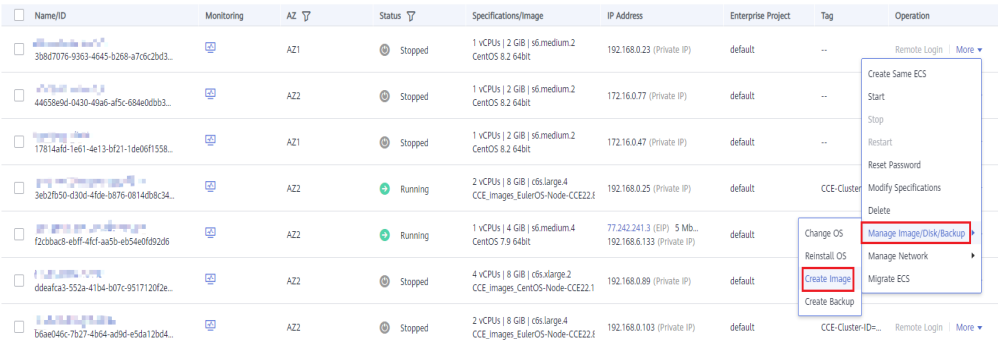
1. Log in to the ECS console. In the ECS list, locate the row containing the ECS with the Agent installed, choose **More** > **Stop** in the **Operation** column, and click **OK**.

Figure 16-1 Stop



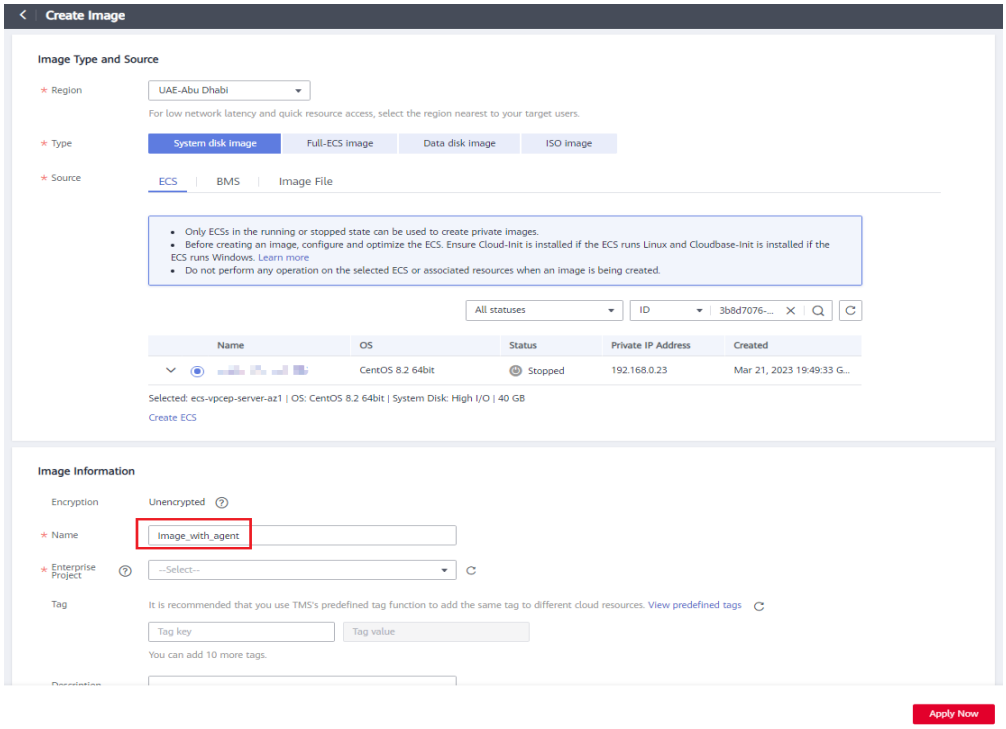
2. Choose **More** > **Manage Image/Disk** > **Create Image**.

Figure 16-2 Create Image



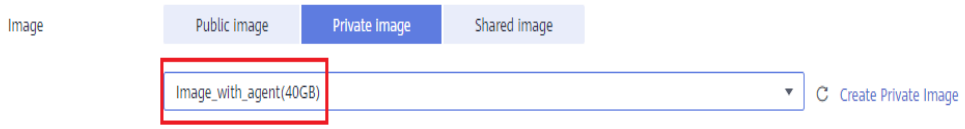
3. Set the private image name to **Image_with_agent** and click **Next**.

Figure 16-3 Image_with_agent



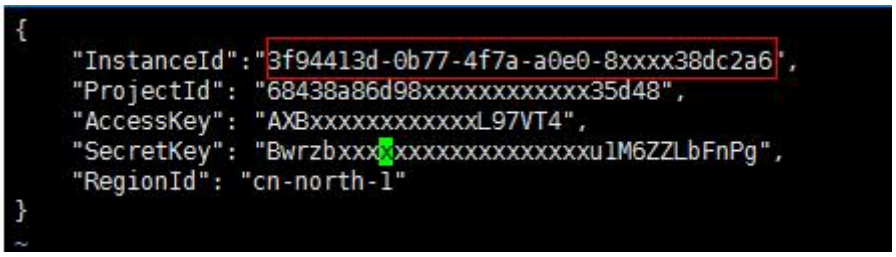
4. Purchase a new ECS and select the newly created private image **Image_with_agent(40GB)**.

Figure 16-4 Image_with_agent(40GB)



5. Log in to the newly purchased ECS. Change **InstanceId** in Agent configuration file **/usr/local/telescope/bin/conf.json** to the ECS name.

Figure 16-5 Modifying the Agent configuration file



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

16.2.4 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 16-2 and **Table 16-3** lists the supported OSs.

Table 16-2 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

OS (64 bit)	Version
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
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 16-3 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.

16.2.5 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 **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 **Modifying the DNS Server Address and Adding Security Group Rules (Linux)** and **(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 **Managing the Agent**.

16.2.6 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 16-4** to the **conf.json** file.

Table 16-4 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 (%)

Parameter	Description
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

```
{
    "InstanceId":"xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx",
    "ProjectId": "b5b92ee0xxxxxxxxxxxxxxxxcab92396",
    "AccessKey": "QZ0XGJXFxxxxxxxxT65R",
    "SecretKey": "lEv2aXAGwxxxxxxxxxxxxxxxxxxxxxxxF8t0Bf18Tn2",
    "RegionId": "ae-abudhabi-1",
    "ClientPort": 0,
    "PortNum": 200,
    "cpu_first_pct_threshold": 35,
    "memory_first_threshold": 314572800,
    "cpu_second_pct_threshold": 70,
    "memory_second_threshold": 734003200
}
```

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.

16.2.7 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.

16.2.8 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 16-5**.

   Table 16-5 Creating an agency

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

16.2.9 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.

16.2.10 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 **How Can I Create an Agency?**

16.2.11 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 **How Can I Create an Agency?**

16.2.12 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.

16.2.13 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 **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 **Modifying the DNS Server Address and Adding Security Group Rules (Linux)** and **(Optional) Manually Configuring the Agent (Linux)**.

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

16.2.14 What Should I Do If the Agent Status Is Stopped?

Starting the Agent

Run the following command to start the Agent:

service telescoped start

If a fault is reported, the Agent has been uninstalled or related files have been deleted. In this case, reinstall the Agent.

16.2.15 What Should I Do If the Agent Status Is Running But There Is No Monitoring Data?

If there is no monitoring data 10 minutes after the Agent is installed, **InstanceId** in the **conf** file may be incorrectly configured.

- Correct the configuration by performing operations described in **(Optional) Manually Configuring the Agent (Linux)**.

16.2.16 How Do I Troubleshoot the Agent One-Click Restoration Failure?

Symptom

After you click **Restore Agent Configurations**, the Agent status is still **Configuration error**.

Possible Causes

The following are possible causes of this issue.

- DNS configuration
- IAM agency configuration
- User permissions

Solution

Step 1 Check the DNS configuration.

1. Log in to the management console.
2. Choose **Compute** > **Elastic Cloud Server**.
3. Click the name of the ECS.

   The ECS details page is displayed.
4. Click the VPC name.

   The VPC console is displayed.
5. In the VPC list, click the VPC name.
6. On the **Subnets** tab, check whether the DNS server addresses are correct.

   For details about how to configure the DNS servers in different regions, see **Modifying the DNS Server Address and Adding Security Group Rules (Windows)** or **Modifying the DNS Server Address and Adding Security Group Rules (Linux)**.

Step 2 Check the IAM agency configuration.

1. Log in to the management console.
2. Under **Management & Governance**, select **Identity and Access Management**.
3. On the IAM console, choose **Agencies**.
4. Check whether there is an agency named **CESAgentAutoConfigAgency**.

   If not, create the agency. You can delete unnecessary agencies if the agency quota has been reached.

Step 3 Check user permissions.

1. Log in to the management console.
2. Under **Management & Governance**, select **Identity and Access Management**.
3. In the navigation pane on the left, click **User Groups**.

4. Locate your user group and click **Authorize** in the **Operation** column.
5. To install the Agent, you must have the following permissions:
   - Global: Security Administrator
   - Region: ECS CommonOperationsr or BMS CommonOperations, and CES Administrator or CES FullAccess

----End

16.2.17 What Can I Do If No Monitoring Data Is Displayed After One-Click Agent Restoration?

Symptoms

The Agent is running normally after being restored, but no monitoring data is generated.

Possible Causes

If no OS monitoring data is generated for an ECS or BMS that has the Agent installed, the possible causes are as follows:

- The Agent status is abnormal.
- The agency is abnormal.
- Temporary AK/SK cannot be obtained due to incorrect route configurations.
- The network is not well connected.

Troubleshooting for Linux

1. Log in to the ECS or BMS as user **root**.
2. Run the following command to check whether the telescope process is running:

   ps -ef |grep telescope

   If the following information is displayed, the telescope process is normal.

   Figure 16-6 Viewing the telescope processes

   ```
   [root@[redacted] ~]# ps -ef |grep telescope
   root      3635     1  0 Jun21 ?        00:00:06 ./telescope
   root      3826  3635  0 Jun21 ?        00:19:24 ./telescope
   root     22829 22805  0 15:17 tty1     00:00:00 grep --color=auto telescope
   [root@[redacted] ~]# _
   ```

   - If yes, go to **4**.
   - If no, go to **3**.
3. Run the following command to start the Agent:

   /usr/local/telescope/telescoped start
4. Run the following command to check whether an agency has been created for the server:

   curl http://169.254.169.254/openstack/latest/securitykey

- If data is returned, the agency is normal and AK/SK can be obtained. No further action is required.
- If the request fails or the following information is displayed, go to **5**.

Figure 16-7 Failing to obtain the AK/SK

```
<html>
 <head>
  <title>401 Unauthorized</title>
 </head>
 <body>
  <h1>401 Unauthorized</h1>
  agency_name is empty in metadata<br /><br />
```

5. On the Cloud Eye console, choose **Server Monitoring** > **Elastic Cloud Server**, select the target ECS, and click **Restore Agent Configurations**.
   - If the problem is resolved, no further action is required.
   - Otherwise, go to **6**.
6. Run the following command to check the route:

   route -n

   The following information indicates that the route is normal.

   Figure 16-8 Normal route configuration-Linux

```
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         192.168.0.1     0.0.0.0         UG    100    0        0 eth0
169.254.169.254 192.168.0.1     255.255.255.255 UGH   100    0        0 eth0
192.168.0.0     0.0.0.0         255.255.255.0   U     100    0        0 eth0
```

   - If the route is normal, no further action is required.
   - Otherwise, go to **7**.
7. If the route does not exist, run the following command to add a route:

   route add -host 169.254.169.254 gw *192.168.0.1*

   NOTE

   Replace *192.168.0.1* in the example command with the gateway of the server.

   Check whether monitoring data can be reported normally.
   - If yes, no further action is required.
   - If no, go to **8**.
8. Run the following command to open the telescope configuration file:

   cat /usr/local/telescope/bin/conf_ces.json
9. Obtain the endpoint from the configuration file.
10. Run the following command to check whether the DNS service is normal:

    ping *ces.ae-ad-1.g42cloud.com*
    - If yes, no further action is required.

– If no, modify the **Modifying the DNS Server Address and Adding Security Group Rules (Linux)** or the Cloud Eye endpoint.

NOTE

For details about the Cloud Eye endpoint in each region, see **Regions and Endpoints**.

Troubleshooting for Windows

1. Log in to the ECS or BMS as an administrator user.
2. Open the **Task Manager** and check whether the telescope process is running.

   If the processes in **Figure 16-9** and **Figure 16-10** are displayed, the telescope process is running.

   Figure 16-9 agent process (Windows)

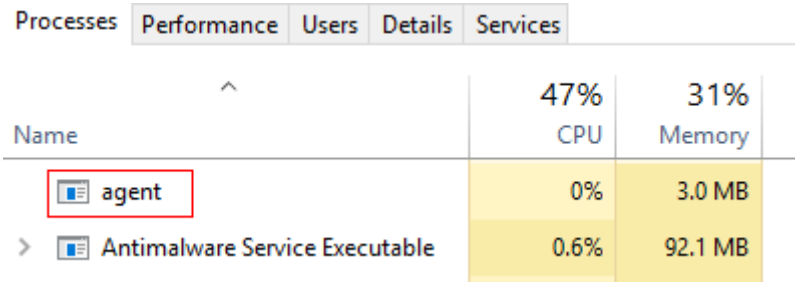
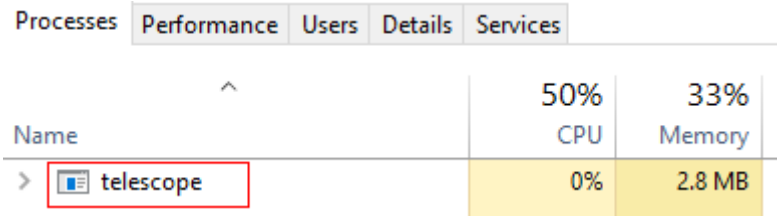
   

   Figure 16-10 telescope process (Windows)

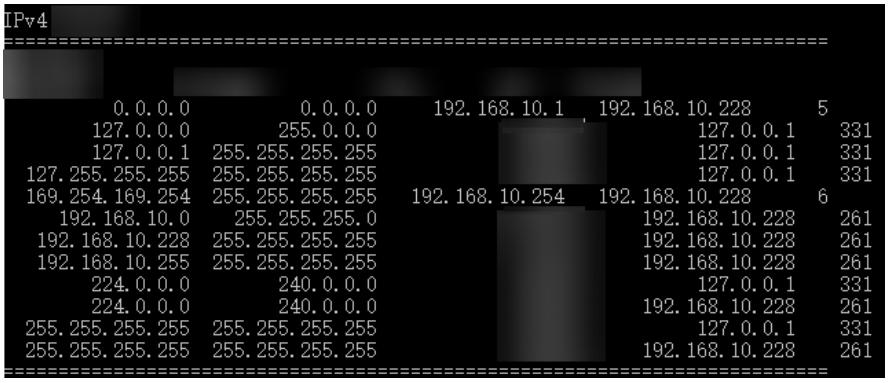
   

   – If yes, go to **4**.
   – If no, go to **3**.
3. Double-click **start.bat** to start the Agent.
4. Access **http://169.254.169.254/openstack/latest/meta_data.json** to check whether the agency has been created.
   – If the website is accessible, the agency is normal. No further action is required.
   – Otherwise, go to **6**.
5. Run the following command to check the route:

   route print

   The following information indicates that the route is normal.

Figure 16-11 Normal route configuration-Windows



```
IPv4
===========================================================================
[redacted]
          0.0.0.0          0.0.0.0      192.168.10.1   192.168.10.228      5
        127.0.0.0        255.0.0.0                          127.0.0.1    331
        127.0.0.1  255.255.255.255                          127.0.0.1    331
  127.255.255.255  255.255.255.255                          127.0.0.1    331
  169.254.169.254  255.255.255.255   192.168.10.254   192.168.10.228      6
     192.168.10.0    255.255.255.0                     192.168.10.228    261
   192.168.10.228  255.255.255.255                     192.168.10.228    261
   192.168.10.255  255.255.255.255                     192.168.10.228    261
        224.0.0.0        240.0.0.0                          127.0.0.1    331
        224.0.0.0        240.0.0.0                     192.168.10.228    261
  255.255.255.255  255.255.255.255                          127.0.0.1    331
  255.255.255.255  255.255.255.255                     192.168.10.228    261
===========================================================================
```

- If the route is normal, no further action is required.
- Otherwise, go to **7**.

6. If the route does not exist, run the following command to add a route:

   route add -host 169.254.169.254 gw *192.168.0.1*

   NOTE

   Replace *192.168.0.1* in the example command with the gateway of the server.

   Check whether monitoring data can be reported normally.

   - If yes, no further action is required.
   - If no, go to **7**.

7. Open the configuration file in **bin/conf_ces.json** in the directory where the telescope installation package is stored.
8. Obtain the endpoint from the **bin/conf_ces.json** file.

   {"Endpoint":"https://ces.ae-ad-1.g42cloud.com"}

9. Run the following command to check whether the DNS service is normal:

   ping *ces.ae-ad-1.g42cloud.com*

   - If the network is normal, no further action is required.
   - Otherwise, modify the **Modifying the DNS Server Address and Adding Security Group Rules (Linux)** or the Cloud Eye endpoint.

     NOTE

     For details about the Cloud Eye endpoint in each region, see **Regions and Endpoints**.

16.3 Alarm Notifications or False Alarms

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

16.3.2 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.

16.3.3 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.

16.3.4 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**.

16.3.5 How Do I Monitor and View the Disk Usage?

To monitor the disk usage, install the server monitoring Agent and create an alarm rule for the disk usage. In the alarm rule, set the metric to **(Agent) Disk Usage (Recommended)** and select a mount point. Enable and configure **Alarm Notification**. For details, see **Creating an Alarm Rule to Monitor a Server**.

After you install the Agent, you can view the data disk usage on the Cloud Eye console. On the **OS Monitoring** page, click the **Disk** tab and select a mount point on the right of the **Auto Refresh** button.

Figure 16-12 Viewing the data disk usage on the **OS Monitoring** page

16.3.6 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 **Topic Management** >**Topics**.

4. Click the name of the target topic.
5. Add subscription endpoints to or delete subscription endpoints from the topic.

16.3.7 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 **Creating a Topic** and **Adding Subscriptions**.

16.3.8 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.

16.4 Monitored Data Exceptions

16.4.1 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 **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.

16.4.2 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.

16.4.3 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.

16.4.4 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.

16.4.5 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.

16.4.6 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.

16.4.7 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 **Agent Installation and Configuration**.

16.4.8 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** .

16.4.9 Why Are the Inbound Bandwidth and Outbound Bandwidth Negative?

If Docker is installed, the early version of the Agent cannot collect statistics on the inbound and outbound bandwidth of virtual NICs when the container is restarted. As a result, a negative value is generated because the difference is calculated.

To update the Agent, see **Managing the Agent**.

16.5 Metric Descriptions

16.5.1 What Are Outband Incoming Rate and Outband Outgoing Rate?

Concept Explanation

You need to understand the meaning of outband and inband:

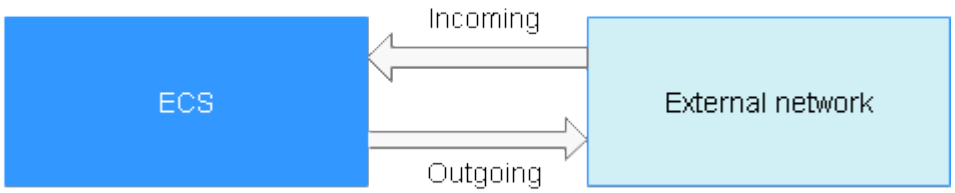
Outband

- Outband is the opposite to inband. Inband indicates that the monitored object is an ECS. Outband indicates that the monitored object is the physical server at the virtualization layer.

Incoming and Outgoing

- Incoming indicates traffic comes to an ECS per second.
- Outgoing indicates traffic sent from an ECS to an external network or client per second.

The following figure shows the traffic directions.



Metric Description

Table 16-6 Outband incoming/outgoing rate

Item	Description
Outband incoming rate	Traffic coming into an ECS per second For example, traffic generated when you download resources to an ECS from an external network or upload files to the ECS. Unit: byte/s
Outband outgoing rate	Traffic going out of an ECS per second For example, traffic generated when users access an ECS via the internet or when the ECS functions as an FTP server for users to download resources. Unit: byte/s

Table 16-7 Outband incoming/outgoing rate

Item	Description
Outband incoming rate	Traffic coming to an ECS per second at the virtualization layer. Generally, the outband incoming rate is slightly larger than the traffic coming to the ECS because the virtualization layer will filter some unnecessary packets. Unit: byte/s
Outband outgoing rate	Traffic going out of an ECS per second at the virtualization layer. Generally, the outband outgoing rate is slightly larger than the traffic sent from the ECS because the virtualization layer will filter some unnecessary packets. Unit: byte/s

16.6 User Permissions

16.6.1 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.

NOTE

Permissions lists the system policies, and operations and policy permissions provided by Cloud Eye.

Figure 16-13 Checking the permissions