Cloud Eye

User Guide

Issue	48
Date	2020-05-30

HUAWEI TECHNOLOGIES CO., LTD.

Contents

1 Monitoring Panels

1.1 Introduction to Monitoring Panels

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

1.2 Creating a Monitoring Panel

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

Procedure

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

   The **Create Panel** dialog box is displayed.
4. Set the panel name.
   - **Name**: Enter a maximum of 128 characters. Only letters, digits, hyphens (-), and underscores (_) are allowed.
   - **Enterprise Project**: If you associate a monitoring panel with an enterprise project, only users who have the permissions of the enterprise project can manage the monitoring panel.

     NOTE

     The enterprise project feature is available only in some regions.
5. Click **OK**.

1.3 Adding a Graph

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

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

Procedure

1. Log in to the management console.
1. Under **Management & Deployment**, select **Cloud Eye**.
2. Choose **Dashboard** > **Monitoring Panels**, switch to the desired panel, and click **Add Graph**.

   The **Add Graph** dialog box is displayed.
3. Set parameters based on **Table 1-1**.

Table 1-1 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 objects of the metric. You can select a maximum of 20 monitored objects at a time.
Metric	Specifies the metric name. Example value: **CPU Usage**

4. Click **Next: Configure Legend**.

   The graph title is displayed on the metric change curve in the monitoring graph. You can set the graph title as required, for example, ECS01-CPU usage. If the CPU usage is 10%, **ECS01 - CPU Usage: 10%** is displayed as the graph title.

   If you do not configure the graph title, the default title in the following format is displayed: monitored object (resource type) - metric: monitoring data. For example, if the CPU usage is 10%, **ECS01 (Elastic Cloud Server) - CPU Usage: 10%** is displayed as the graph title.
5. Click **OK**.

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

1.4 Viewing a Graph

After you add a graph, you can view the metric trends on the **Monitoring Panels** page. The system provides you both default 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. Under **Management & Deployment**, select **Cloud Eye**.
3. Choose **Dashboard** > **Monitoring Panels**.

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

   NOTE

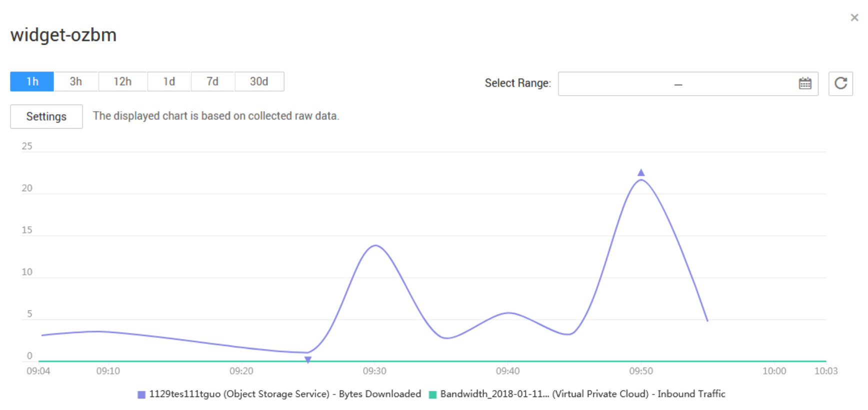
   - You can sort graphs by dragging them.
   - Click **1h**, **3h**, **12h**, **1d**, **7d**, or **30d** in the upper left to switch the monitoring periods of all graphs on the panel.
   - You can also go to the full screen to view the monitoring graphs. For details, see **Using the Full Screen**.

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.

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

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

   Figure 1-1 Viewing graphs



Using the Full Screen

The full screen displays metric data more clearly.

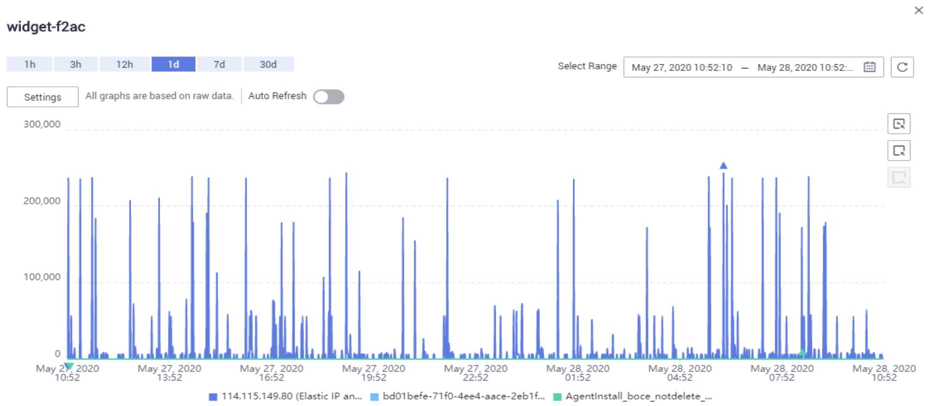
- To enter the full screen, click **Full Screen** in the upper right corner of the **Monitoring Panels** page.
- To exit the full screen, click **Exit Full Screen** in the upper left corner of the page.

Customizing a Period to View the Monitoring Graph

By default, metrics in the last 1 hour, last 3 hours, last 12 hours, last 7 days, and last 30 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 1-2 Customizing a period



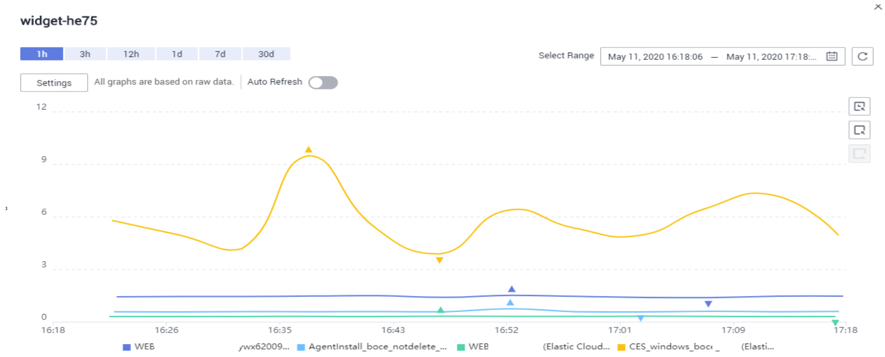
- To go back to the default graph, click the third icon on the right.

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 **Figure 1-3** 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 1-3 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.

1.5 Configuring a Graph

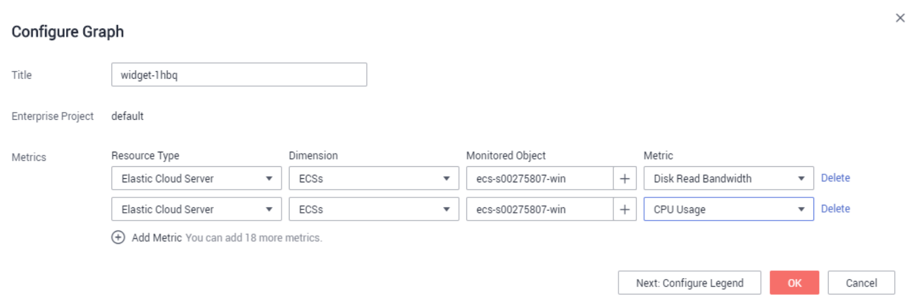
This topic describes how to add, modify, and delete metrics on graphs.

Procedure

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

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

Figure 1-4 Configure Graph



NOTE

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

1.6 Deleting a Graph

1. Log in to the management console.

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

1.7 Deleting a Panel

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

Procedure

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

2 Resource Groups

2.1 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.

The Resource Groups function 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.

2.2 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 1000 cloud service resources.
- The quotas of different resources in a resource group are as follows:
  - ECS: 1000
  - BMS: 500
  - EVS disk: 1000
  - VPC: 200 each for elastic IP addresses and bandwidth
  - RDS: 200 for each type of database
  - DMS: 200
  - DCS: 200
  - ELB: 200

Procedure

1. Log in to the management console.
2. In the upper left corner, select a region and project.
3. Under **Management & Deployment**, select **Cloud Eye**.
4. In the navigation pane on the left, choose **Resource Groups**.
5. In the upper right corner, click **Create Resource Group**.
6. Enter the group name 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 set **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.

   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.
   - The **Associate Enterprise Project** feature is available only in some regions.

     When associating a resource group with an enterprise project, you can select only ECSs, EIPs, or bandwidths. After an enterprise project is associated with a resource group, you cannot perform operations on the resource group directly. To manage resources in the resource group, see **Removing Resources from an Enterprise Project** and **Adding Resources to an Enterprise Project**.
8. Click **Create**.

2.3 Viewing Resource Groups

2.3.1 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 a project.
3. Under **Management & Deployment**, 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 2-1 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.
Health Status	● **Healthy**: No alarms have been generated for the group. ● **Unhealthy**: An alarm or alarms have been generated for a resource or resources in the group. ● **No alarm rule**: No alarm rules have been set for the group.
Associated Object	Specifies the enterprise project associated with the resource group. After the association, the resources in the resource group and those in the enterprise project will automatically be made consistent. **NOTE** The **Associate Enterprise Project** feature is supported only in region **CN North-Beijing1** and **CN East-Shanghai2**.
Unhealthy Resources	Specifies the number of resources in a group whose alarms have been triggered. For example, if there are two ECSs and one EVS disk that are in the **Alarm** state in a resource group, the value of **Unhealthy Resources** is **3**.
Total Resources	Specifies the number of resources in a group. For example, if there are four resources, namely, two ECSs, one EVS disk, and one elastic IP address in a resource group, the value of **Total Resources** is **4**.
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 the value of **Resource Types** is **2**.
Enterprise Project	Specifies the name of the enterprise project that has the resource group permission.
Created	Specifies the time when the resource group was created.
Operation	Specifies the operations that can be performed on a resource group. You can only modify or delete a resource group.

2.3.2 Resource Overview

The **Resource Overview** page displays all resource types in the current group, the number of each resource type, and graphs of each resource type.

Procedure

1. Log in to the management console.
2. In the upper left corner, select a region and a project.
3. Under **Management & Deployment**, 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 Monitoring Preview (in the Alarm State)** page.

2.3.3 Unhealthy Resources

Unhealthy Resources includes all resources in the **Alarm** state in a resource group. This feature enables you to quickly view all unhealthy resources and handle faults.

Procedure

1. Log in to the management console.
2. In the upper left corner, select a region and a project.
3. Under **Management & Deployment**, 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 **Unhealthy Resources** to view all resources in the resource group for which alarms have been triggered.

2.3.4 Alarm Rules

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

Procedure

1. Log in to the management console.
2. In the upper left corner, select a region and a project.
3. Under **Management & Deployment**, 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.

2.3.5 Alarm History

The **Alarm History** page displays the alarm history of all alarm rules in a resource group.

Procedure

1. Log in to the management console.
2. In the upper left corner, select a region and a project.
3. Under **Management & Deployment**, 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 History** to view the alarm history for all resources in the resource group.

2.4 Managing Resource Groups

If your cloud service requirements change, you may need to modify the resources in a resource group.

This topic describes how to modify or delete a resource group.

2.4.1 Modifying a Resource Group

When you need to add resources to or delete resources from a resource group, modify the resource group. If you want to change the enterprise project with which a resource group is associated, see **Removing Resources from an Enterprise Project** and **Adding Resources to an Enterprise Project**.

Procedure

1. Log in to the management console.
2. In the upper left corner, select a region and a project.
3. Under **Management & Deployment**, 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 **Modify** in the **Operation** column.

Figure 2-1 Modifying a resource group

6. On the displayed **Modify Resource Group** page, modify the resource group.
7. Click **Modify**.

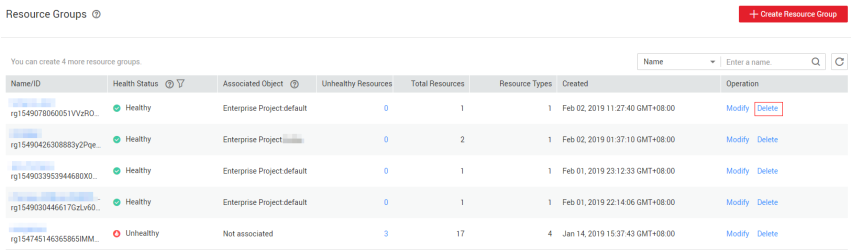
2.4.2 Deleting a Resource Group

Procedure

1. Log in to the management console.
2. In the upper left corner, select a region and a project.

3. Under **Management & Deployment**, 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 2-2 Deleting a resource group



6. In the displayed **Delete Resource Group** dialog box, click **Yes**.

3 Using the Alarm Function

3.1 Introduction to the Alarm Function

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

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

NOTE

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

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.

3.2 Creating Alarm Notification Topics

3.2.1 Creating a Topic

Scenarios

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

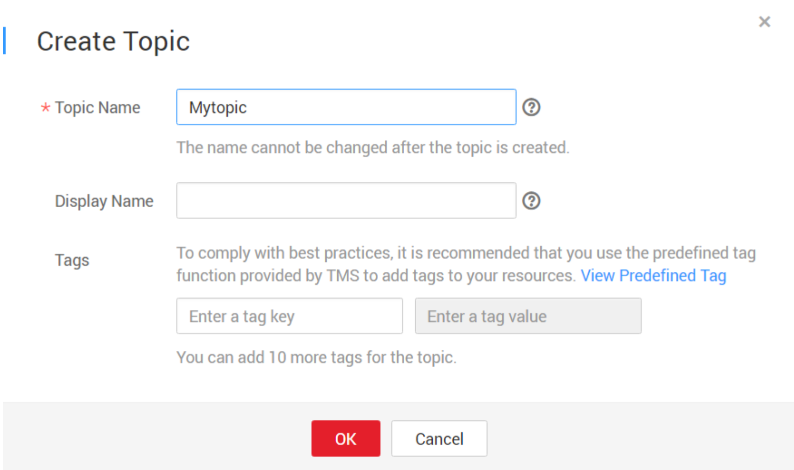
You can create your own topic.

Creating a Topic

1. Log in to the management console.

2. In the upper left corner, select a region and project.
3. Choose **Service List** > **Application** > **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 3-1 Create Topic



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

Table 3-1 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
Tag	Tags identify cloud resources so that they can be categorized easily and searched quickly. ● You can enter a maximum of 36 and 43 characters for **Key** and **Value**, respectively. Both **Key** and **Value** cannot start or end with a space and cannot contain any of the following special characters:=, *, <, >, \, ,, |, / ● Each topic supports up to 10 tags.

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.

3.2.2 Adding Subscriptions

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

Adding Subscriptions

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

   The SMN console is displayed.

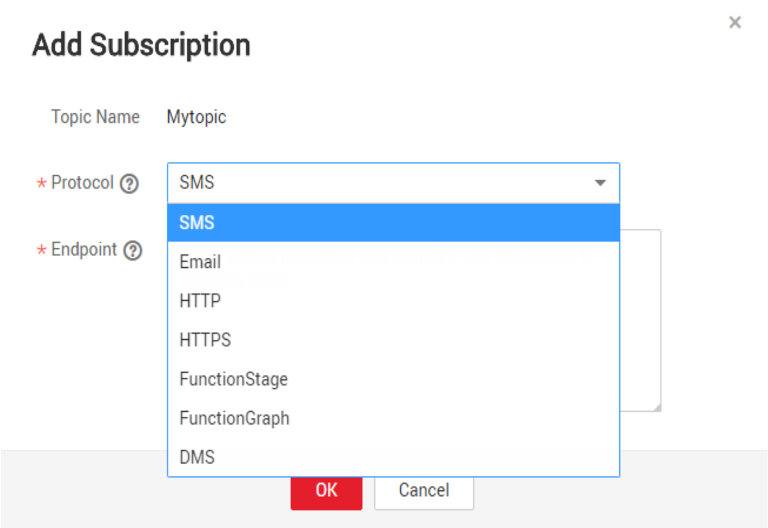
3. In the navigation pane, choose **Topic Management** > **Topics**.

   The **Topics** page is displayed.

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

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

Figure 3-2 Add 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 a subscription, see **Adding a Subscription** in the *Simple Message Notification User Guide*.

6. Click **OK**.

   The subscriptions you added are displayed in the subscription list.

3.3 Creating Alarm Rules

3.3.1 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.

3.3.2 Creating an Alarm Rule

This topic describes how to create an alarm rule.

Creating an Alarm Rule

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

a. Set the alarm rule name and description.

Table 3-2 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.
Enterprise Project	Specifies the enterprise project 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**.

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

Figure 3-3 Alarm Content

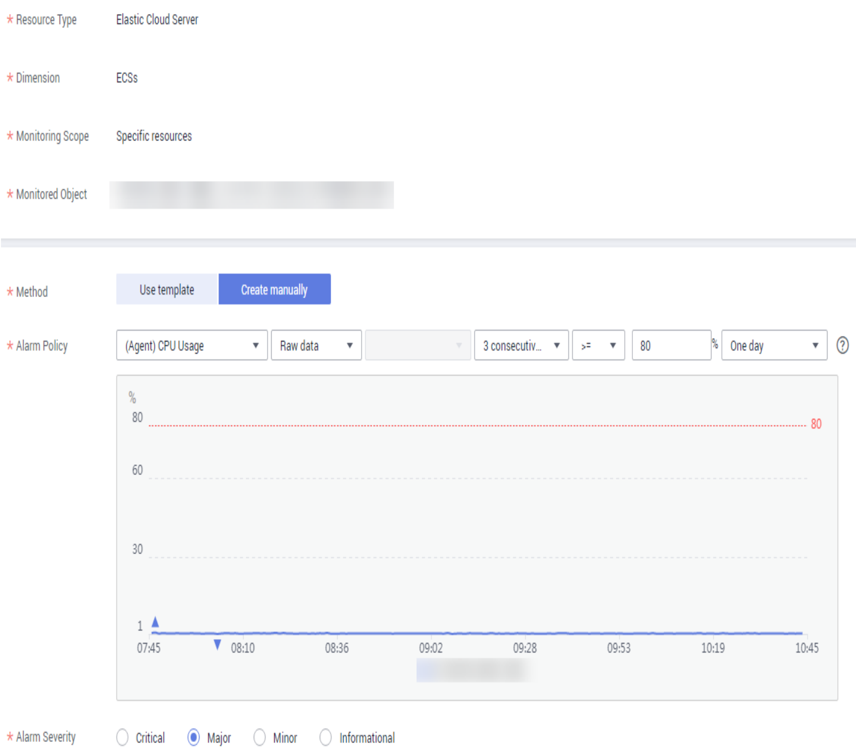


Table 3-3 Parameters

Parameter	Description	Example Value
Resource Type	Specifies the type of the resource the alarm rule is created for.	Elastic Cloud Server
Dimension	Specifies the metric dimension of the selected resource type.	ECSs
Monitoring Scope	Specifies the monitoring scope the alarm rule applies to. You can select **Resource groups** or **Specific resources**. **NOTE** ● If **Resource groups** is selected and any resource in the group meets the alarm policy, an alarm is triggered. ● If you select **Specific resources**, select one or more resources and click to add them to the box on the right.	Specific resources
Select Group	This parameter is mandatory when **Monitoring Scope** is set to **Resource groups**.	-
Threshold Type	For ECSs, you can select **Static** or **Dynamic**. The feature is only available in region CN South-Guangzhou. ● **Static**: Indicates the fixed value set in an alarm rule. If the fixed value is reached, an alarm is triggered. ● **Dynamic**: Indicates the predicative value range calculated based on historical data. If the current metric data deviates from the predicted value range, an alarm is triggered.	Static
Method	There are two options: **Use template** or **Create manually**.	Create manually
Template	Specifies the template to be used. You can select a default alarm template or **a custom template**.	-

Parameter	Description	Example Value
Alarm Policy	Specifies the policy for triggering an alarm. If you set **Resource Type** to **Website Monitoring**, **Log Monitoring**, **Custom Monitoring**, or a specific cloud service, whether to trigger an alarm depends on whether the metric data in consecutive periods reaches the threshold. For example, Cloud Eye triggers an alarm if the average CPU usage of the monitored object is 80% or more for three consecutive 5-minute periods. If you set **Resource Type** is to **Event Monitoring**, the event that triggers the alarm is an instant event. For example, if event improper ECS running occurs, Cloud Eye triggers an alarm.	-
Alarm Severity	Specifies the alarm severity. Valid values are **Critical**, **Major**, **Minor**, and **Informational**.	Major

c. Set **Alarm Notification** parameters.

Figure 3-4 Alarm Notification

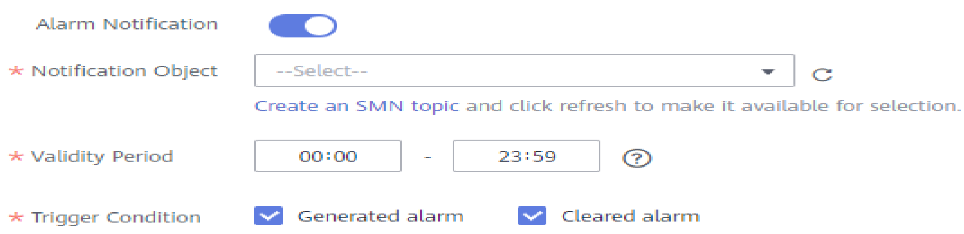


Table 3-4 Alarm Notification parameters

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 that receives alarm notifications. You can select the account contact or a topic. ● **Account contact** is the mobile phone number and email address of the registered account. ● A topic is used to publish messages and subscribe to notifications. If the required topic is unavailable, create one first and add subscriptions to it. For details, see **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 condition for triggering the alarm notification. You can select **Generated alarm** (when an alarm is generated), **Cleared alarm** (when an alarm is cleared), or both.

d. Click **Create**.

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

To view monitoring graphs, click **View Graph** or **View Resource** in the **Operation** column, and click **View Graph** in the displayed **View Resource** dialog box.

3.4 Example: Creating an Alarm Rule to Monitor ECS CPU Usage

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. Under **Management & Deployment**, select **Cloud Eye**.
3. In the navigation pane on the left, choose **Server Monitoring**.

   The list of ECSs on the public cloud platform is displayed.
4. Locate the target ECS. In the **Operation** column, click **More**, and select **Create Alarm Rule**.

   The **Create Alarm Rule** dialog box is displayed.
5. Configure the following parameters one by one:
   a. **Method**: Select **Create manually**.
   b. **Metric**: Select **CPU Usage** from the drop-down list.
   c. **Alarm Policy**: Select **CPU Usage**, **Avg.**, **5 minutes**, **3 consecutive periods**, ≥, and **80%**.
   d. **Alarm Severity**: Set it to **Major**.
   e. Enable **Alarm Notification**.
   f. **Validity Period**: Set it to **00:00-23:59**.
   g. **Topic**: Select the topic created in Creating Alarm Notification Topics.
   h. **Trigger Condition**: Select **Generated alarm** and **Cleared alarm**.

   Click **Next**.

6. Specify **Name** and **Description** of the alarm rule. Click **Finish**.

3.5 Viewing the Alarm History

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

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

Procedure

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

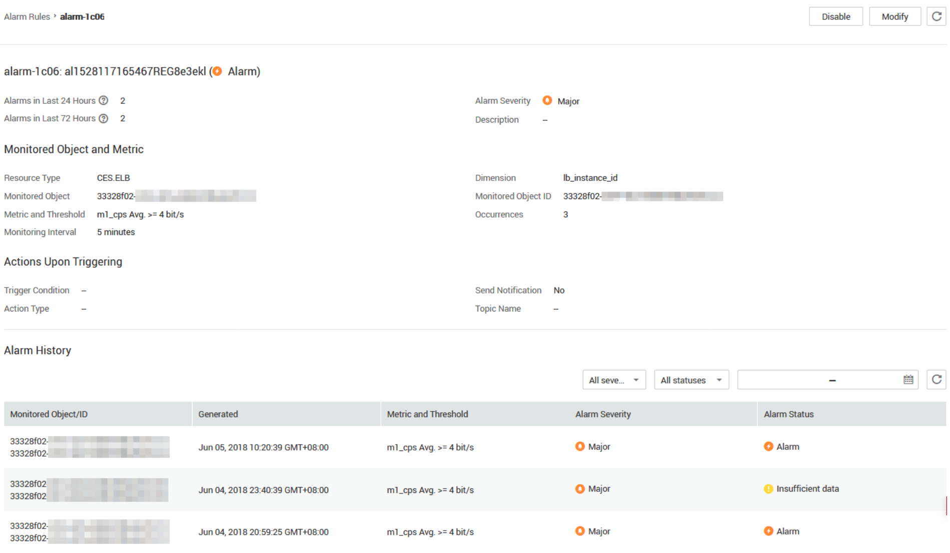
   On the **Alarm History** page, you can view the status changes of all alarm rules from the last 7 days.

   > NOTE
   >
   > You can select a time range to search for the alarm history.
   >
   > You can also view the alarm history by clicking **All resource types**, **All severities**, or **All statuses**.

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

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

Figure 3-5 Alarm history



NOTE

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

3.6 One-Click Monitoring

Application Scenarios

One-click monitoring enables you to quickly and easily enable or disable monitoring of common events for certain services. **Table 3-5** describes differences between one-click monitoring and common monitoring.

Table 3-5 One-click monitoring and common monitoring

Alarm Type	Objective	Scope	Alarm Object	Trigger Condition
One-click monitoring	When an event occurs, Cloud Eye triggers alarms immediately. Advantages: The configuration is simple.	Key events of ECS, EIP, and RDS. For detailed events, see **Supported Cloud Services and Alarm Rules**.	Event monitoring	Immediate trigger
Common monitoring	Cloud Eye triggers alarms based on the preset alarm policies. For example, Cloud Eye triggers an alarm if the average CPU usage is 80% or more for five consecutive times within 5 minutes. Advantages: Alarm policies are flexible and can be configured based on service requirements.	All services supported by Cloud Eye	• Server monitoring • Cloud service monitoring • Custom monitoring • Website monitoring • Log monitoring	Accumulative trigger

Alarm Type	Objective	Scope	Alarm Object	Trigger Condition
	When an event occurs, Cloud Eye triggers alarms based on the alarm policy. Advantages: The configuration is flexible. Only event alarms are supported.	For details about services that support event monitoring, see **Events Supported by Event Monitoring**.	Event monitoring	Immediate trigger or accumulative trigger

This topic describes how to use the one-click monitoring function to monitor key metrics.

Constraints

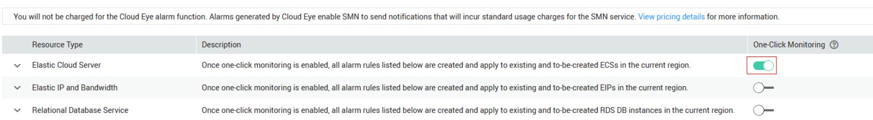
- One-click monitoring sends notifications only when alarms are generated and does not send notifications when alarms are cleared.
- Once the alarm threshold is reached, one-click monitoring will trigger alarms immediately.

Procedure

1. Log in to the management console.
2. Under **Management & Deployment**, select **Cloud Eye**.
3. In the navigation pane on the left, choose **Alarm Management**> **One-Click Monitoring**.
4. Locate the target cloud service, and enable **One-Click Monitoring**.

   For details about the cloud services and alarm rules supported by one-click monitoring, see **Supported Cloud Services and Alarm Rules**.

   Figure 3-6 One-Click Monitoring

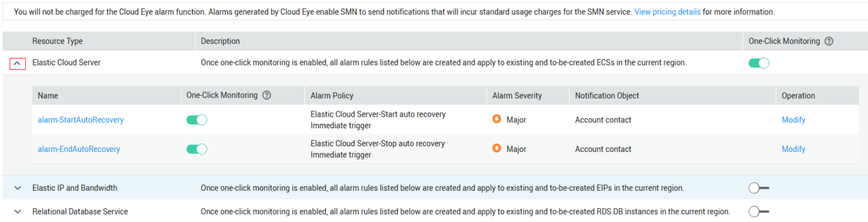
   

5. Click the arrow to the left of the cloud service name to view the automatically generated alarm rules.

   NOTE

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

Figure 3-7 Viewing alarm rules



Supported Cloud Services and Alarm Rules

Table 3-6 ECS

Alarm Name	Alarm Policy	Description	Procedure
alarm-StartAutoRecovery	Elastic Cloud Server-Start auto recovery Immediate trigger	When the host where the ECS resides becomes faulty, the system automatically migrates the ECS to a functional host. This process will cause the ECS to restart and send a "Start auto recovery" event. After the migration is complete and a "Stop auto recovery" event is sent, the ECS is restored.	"Start auto recovery" indicates that a fault has occurred and the ECS cannot be used. In this case, you need to replace the ECS or direct traffic to other ECSs.
alarm-EndAutoRecovery	Elastic Cloud Server-Stop auto recovery Immediate trigger		This alarm indicates that the ECS is working properly and can be used again.

Table 3-7 Elastic IP and Bandwidth

Alarm Name	Alarm Policy	Event Description	Procedure
alarm-BlockEIP	Elastic IP-EIP blocked Immediate trigger	If the bandwidth usage exceeds 5 Gbit/s, the traffic will be discarded. This indicates that the bandwidth usage exceeds the threshold or the system experiences attacks (generally DDoS attacks). An event will be received when the EIP is unblocked.	Change the EIP to prevent services from being affected. In addition. Check the root cause and rectify the fault.
alarm-UnblockEIP	Elastic IP-EIP unblocked Immediate trigger		Use the unblocked EIP again to avoid a waste of resources.

Alarm Name	Alarm Policy	Event Description	Procedure
alarm-EIPBandwidthOverflow	Elastic IP-EIP bandwidth overflow Immediate trigger	If this event is reported, the data traffic exceeds the purchased bandwidth, which may decrease your network speed or cause packet loss.	Check whether the EIP data traffic continues to increase and whether services are normal. Increase the bandwidth if required.

Table 3-8 RDS

Alarm Name	Alarm Policy	Event Description	Procedure
alarm-CreateInstanceFailed	Relational Database Service-DB instance creation failure Immediate trigger	DB instance creation failed because of insufficient disks or quota, or underlying resources have been used up.	Check the number and quota of disks. Release resources and create DB instances again.
alarm-FullBackupFailed	Relational Database Service-Full backup failure Immediate trigger	Full backup failed. 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.
alarm-ActiveStandBySwitchFailed	Relational Database Service-Primary/standby switchover failure Immediate trigger	The standby DB instance does not take over services from the primary DB instance due to network or server failures. The original primary DB instance continues to provide services within a short time.	Check whether the connection between the application and the database is re-established.

Alarm Name	Alarm Policy	Event Description	Procedure
alarm-AbnormalReplicationStatus	Relational Database Service-Replication status abnormal Immediate trigger	The replication delay between the primary and standby DB instances is too long (usually occurs when a large amount of data is written to databases or a large transaction is performed). During off-peak hours, the replication delay between the primary and standby DB instances gradually decreases. Another possible cause is that the network between the primary and standby DB instances is interrupted. However, the network interruption does not interrupt data reads from or writes into a single DB instance, and customers' applications are unaware of the interruption.	Submit a service ticket for processing.
alarm-FaultyDBInstance	Relational Database Service-DB instance faulty Immediate trigger	A single or primary DB instance is faulty due to a disaster or a server failure. This event is critical and may cause the database service to be unavailable.	Check whether an automated backup policy has been configured for the DB instance and submit a service ticket for processing.

Alarm Name	Alarm Policy	Event Description	Procedure
alarm-SingleToHAFailed	Relational Database Service-Failure of changing single DB instance to primary/standby Immediate trigger	When the standby DB instance is created or after the standby DB instance is created, the configuration synchronization between the primary DB instance and the standby DB instance is faulty. Generally, the fault is caused by insufficient resources of the data center where the standby DB instance is located. This event does not interrupt the data reads and writes of the original single DB instance, and customers' applications are unaware of this event.	Submit a service ticket for processing.
alarm-ReplicationStatusRecovered	Relational Database Service-Replication status recovered Immediate trigger	The replication delay between the primary and standby DB instances has been restored to the normal range, or the network connection between them has been restored.	No action is required.
alarm-DBInstanceRecovered	Relational Database Service-DB instance recovered Immediate trigger	RDS uses high availability tools to rebuild the standby DB instance for disaster recovery. After the recovery, this event will be reported.	No action is required.

3.7 Alarm Rule Management

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

3.7.1 Modifying an Alarm Rule

Procedure

1. Log in to the management console.
2. Under **Management & Deployment**, 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 **More** in the **Operation** column, and choose **Modify**.
   – Click the name of the alarm rule you want to modify. On the displayed page, click **Modify** in the upper right corner.
5. On the **Modify Alarm Rule** page, modify alarm rule parameters as needed.

Table 3-9 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
Enterprise Project	Specifies the enterprise project the alarm rule belongs to. Only users with the enterprise project permissions can view and manage the alarm rule.	N/A
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

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. **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
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. You can enable (recommended) or disable this function.	Enable
Notification Object	Specifies the object that receives alarm notifications. You can select the account contact or a topic. ● **Account contact** is the mobile phone number and email address of the registered account. ● 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
Validity Period	Cloud Eye sends notifications only within the validity period specified in the alarm rule. If **Validity Period** 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 the alarm notification. You can select **Generated alarm** (when an alarm is generated), **Cleared alarm** (when an alarm is cleared), or both.	N/A

6. Click **Modify**.

3.7.2 Disabling Alarm Rules

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

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

3.7.3 Enabling Alarm Rules

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

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

3.7.4 Deleting Alarm Rules

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

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

3.8 Alarm Templates

3.8.1 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. Under **Management & Deployment**, select **Cloud Eye**.
3. Choose **Alarm Management** > **Alarm Templates**.

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

3.8.2 Creating a Custom Template

1. On the **Alarm Templates** page, click **Create Custom Template**.
2. In the **Configure Template** step, specify the parameters listed in **Table 3-10**.

Figure 3-8 Create Custom Template

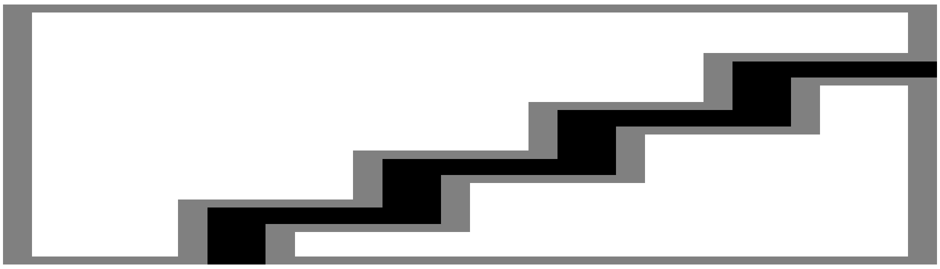


Table 3-10 Parameters

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

3. Click **Next** to go to the **Add Alarm Rule** step. Specify parameters listed in **Table 3-11**. You can add one or more rules to the alarm template.

Figure 3-9 Add Alarm Rule

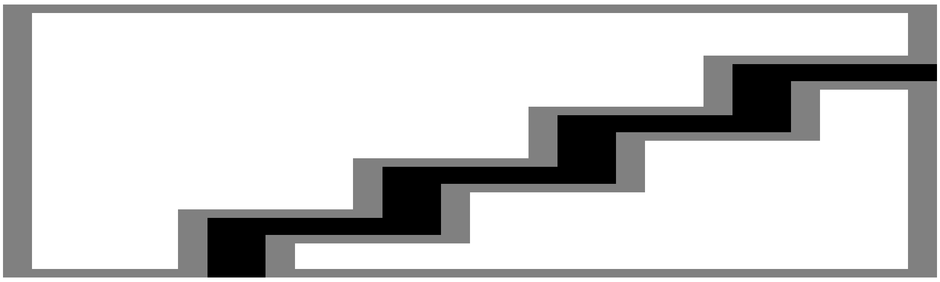


Table 3-11 Parameters

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

4. Click **Next** to go to the **Specify Template Details** step. Specify parameters listed in **Table 3-12**.

Table 3-12 Parameters

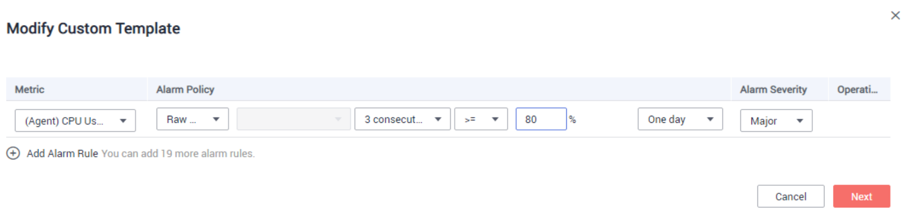
Parameter	Description
Name	Specifies the custom template name. The system generates a random name, which you can modify. Example value: **alarmTemplate-ku0x**
Description	(Optional) Provides supplementary information about the alarm template.

5. Click **Finish**.

3.8.3 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. In the displayed **Modify Custom Template** dialog box, modify the parameter settings based on **Table 3-11** and click **Next**.

Figure 3-10 Modifying a Custom Template

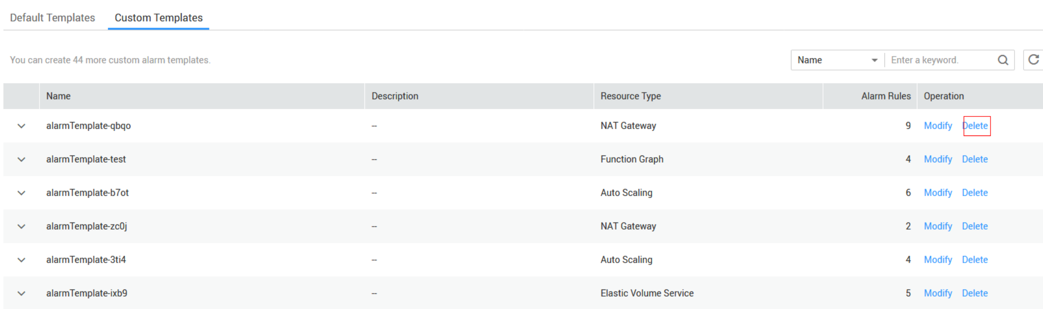


3. Modify the template name and description based on **Table 3-12**, and click **OK**.

3.8.4 Deleting a Custom Template

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

Figure 3-11 Deleting a custom template



4 Server Monitoring

4.1 Introduction to Server Monitoring

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

- Basic monitoring includes metrics automatically reported by ECSs. The data is collected every 5 minutes. For details, see **Services Interconnected with Cloud Eye**.
- OS monitoring provides fine-grained OS monitoring for servers, and it requires the Agent to be installed on all servers that will be monitored. The data is collected every 1 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

- Only Windows and Linux OSs are supported. For details, see **What OSs Does the Agent Support?**
- For the ECS specifications, you are advised to 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 OS, you must have the root permissions. For a Windows OS, 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 HUAWEI CLOUD. If any problem occurs when you use a private image, Cloud Eye will not provide technical support.

Monitoring Capabilities

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.

Resource Usage

The Agent uses considerably less resources. When the Agent is installed on an ECS or BMS, it uses less than 5% of the CPU and less than 100 MB of memory.

4.2 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 methods:

Scenario	Supported Service	Reference
Installing the Agent for Linux OSs	ECS and BMS	**Installing and Configuring the Agent on a Linux ECS or BMS**
Installing the Agent for Windows OSs	ECS	**Installing and Configuring the Agent on a Windows ECS**
Installing the Agent in Batches for Linux OSs	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.
- To check the OSs supported by the Agent, see **What OSs Does the Agent Support?**
- For servers created from CentOS images, versions 7.2 through 7.6, you can click **Not installed** in the **Agent Status** column of the **Server Monitoring** page to install the Agent with one click.
- 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 (Linux)**.

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.

4.3 Agent Features per Version

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

Version 1.1.2

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 Frequently Changes?**

Version 1.0.14

Disk metrics are added to **OS Monitoring**.

Version 1.0.13

- The procedure for installing the Agent is optimized.
- The procedure for installing Agents in batches is optimized.

Version 1.0.11

- The Agent can be installed to a specified directory.
- Ports can be specified for the Agent.
- File system metrics are added to **OS Monitoring**. For details, see **Services Interconnected with Cloud Eye**.

Version 1.0.7

The Agent supports CTS to collect OS logs.

Version 1.0.6

- The Agent supports the Windows OSs. For details, see **What OSs Does the Agent Support?**
- The function of restoring the Agent configurations is added.
- Metrics are added to **Process Monitoring**.

Version 1.0.5

- The **ECS Monitoring** page is replaced by the **Server Monitoring** page.
- Fine-grained monitoring for BMSs is added.
- CPU and disk metrics are added to **OS Monitoring**. For details, see **Services Interconnected with Cloud Eye**.

Version 1.0.4

GPU and disk metrics are added to **OS Monitoring**. For details, see **Services Interconnected with Cloud Eye**.

NOTE

To view GPU metrics, install the plug-in for collecting GPU metrics. For details, see **Installing the Plug-in for Collecting GPU and RAID Metrics (Linux)**.

Version 1.0.3

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

Version 1.0.2

- NIC metrics are added to **OS Monitoring**. For details, see **Services Interconnected with Cloud Eye**.
- **Process Monitoring** is available. For details, see **Viewing Process Monitoring**.

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

4.4.1 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 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.

NOTE

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

Modifying the DNS Server Address (Command Lines)

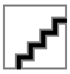
You can modify the DNS server address of an ECS via command lines or the management console.

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 100.125.1.250** and **nameserver 100.125.21.250** to the file. Enter **:wq** and press **Enter** to save the change.

Figure 4-1 Adding the DNS server address (Linux)



NOTE

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

CN North-Beijing1: 100.125.1.250,100.125.21.250

CN North-Beijing4: 100.125.1.250,100.125.129.250

CN Southwest-Guiyang1: 100.125.1.250,100.125.129.250

CN East-Shanghai1: 100.125.1.250,100.125.64.250

CN East-Shanghai2: 100.125.17.29,100.125.135.29

CN South-Guangzhou: 100.125.1.250,100.125.136.29

AP-Hong-Kong: 100.125.1.250,100.125.3.250

AP-Bangkok: 100.125.1.250

AP-Singapore: 100.125.1.250,100.125.128.250

AF-Johannesburg: 100.125.1.250

LA-Santiago: 100.125.1.250

LA-Mexico City1: 100.125.1.22

LA-Sao Paulo1: 100.125.1.22

Modifying the DNS Server Address (Management Console)

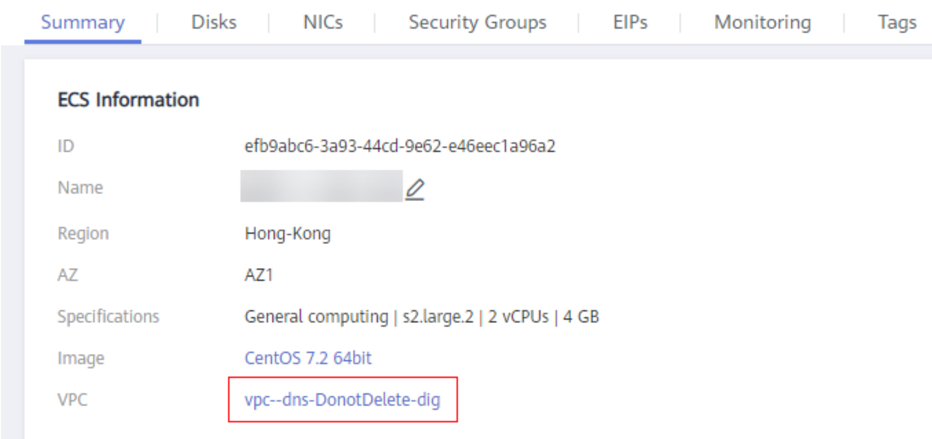
The following describes how to modify the DNS server address of an ECS on the management console. The operations for BMSs are similar.

1. In the upper left corner, select a region and project.
2. On the **Service List** page, choose **Computing** > **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 4-2 VPC



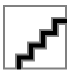
4. Click the name of the target VPC.
5. In the **Networking Components** area, click the number following **Subnets**.

   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**.

   Figure 4-3 Edit DNS Server Address

   
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. 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 4-1**.

Table 4-1 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.

4.4.2 Installing the Agent (Linux)

Scenarios

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

Constraints

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

For servers created from CentOS images, versions 7.2 through 7.6, you can click **Not installed** in the **Agent Status** column of the **Server Monitoring** page to install the Agent with one click.

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:

NOTE

The script supports x86 and Kunpeng Arm-based ECSs.

CN North-Beijing1:

```
cd /usr/local && curl -k -O https://obs.cn-north-1.myhuaweicloud.com/uniagent-cn-north-1/script/agent_install.sh && bash agent_install.sh
```

CN North-Beijing4:

```
cd /usr/local && curl -k -O https://obs.cn-north-4.myhuaweicloud.com/uniagent-cn-north-4/script/agent_install.sh && bash agent_install.sh
```

CN South-Guangzhou:

```
cd /usr/local && curl -k -O https://obs.cn-south-1.myhuaweicloud.com/uniagent-cn-south-1/script/agent_install.sh && bash agent_install.sh
```

CN South-Shenzhen:

```
cd /usr/local && curl -k -O https://obs.cn-south-2.myhuaweicloud.com/uniagent-cn-south-2/script/agent_install.sh && bash agent_install.sh
```

CN East-Shanghai1:

```
cd /usr/local && curl -k -O  https://obs.cn-east-3.myhuaweicloud.com/uniagent-cn-east-3/script/agent_install.sh && bash agent_install.sh
```

CN East-Shanghai2:

```
cd /usr/local && curl -k -O https://obs.cn-east-2.myhuaweicloud.com/uniagent-cn-east-2/script/agent_install.sh && bash agent_install.sh
```

CN Southwest-Guiyang1:

```
cd /usr/local && curl -k -O https://obs.cn-southwest-2.myhuaweicloud.com/uniagent-cn-southwest-2/script/agent_install.sh && bash agent_install.sh
```

AP-Hong-Kong:

```
cd /usr/local && curl -k -O https://obs.ap-southeast-1.myhuaweicloud.com/uniagent-ap-southeast-1/script/agent_install.sh && bash agent_install.sh
```

AP-Bangkok:

```
cd /usr/local && curl -k -O https://obs.ap-southeast-2.myhuaweicloud.com/uniagent-ap-southeast-2/script/agent_install.sh && bash agent_install.sh
```

AP-Singapore:

```
cd /usr/local && curl -k -O https://obs.ap-southeast-3.myhuaweicloud.com/uniagent-ap-southeast-3/script/agent_install.sh && bash agent_install.sh
```

AF-Johannesburg:

```
cd /usr/local && curl -k -O https://obs.af-south-1.myhuaweicloud.com/uniagent-af-south-1/script/agent_install.sh && bash agent_install.sh
```

LA-Santiago:

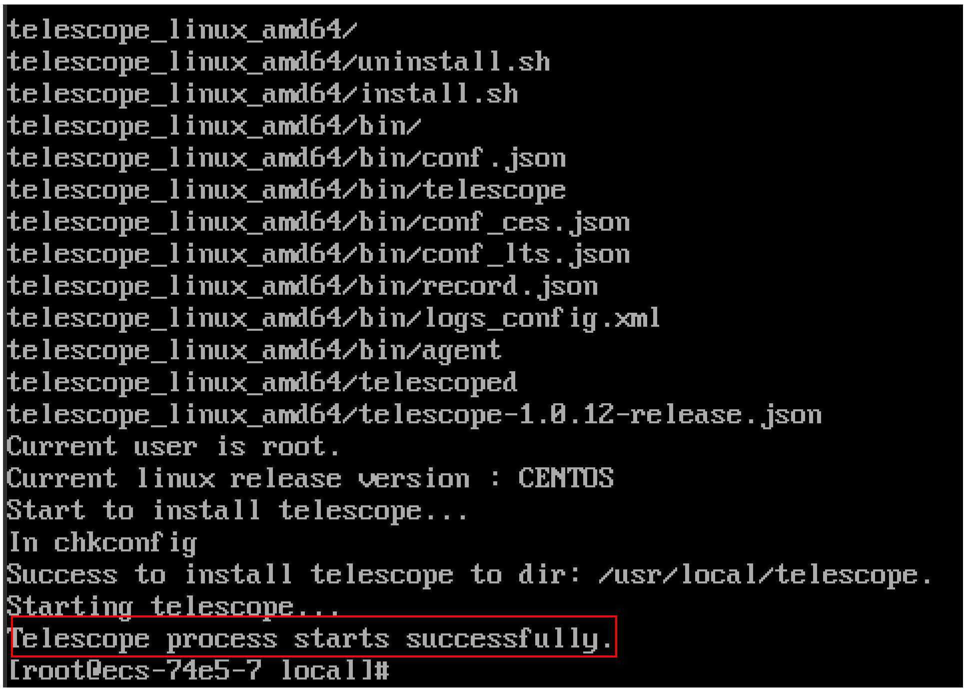
```
cd /usr/local && wget https://telescope-la-south-2.obs.la-south-2.myhuaweicloud.com/scripts/agentInstall.sh && chmod 755 agentInstall.sh && ./agentInstall.sh
```


LA-Sao Paulo1:

```
cd /usr/local && wget https://telescope-sa-brazil-1.obs.sa-brazil-1.myhuaweicloud.com/scripts/
agentInstall.sh && chmod 755 agentInstall.sh && ./agentInstall.sh
```

The Agent is installed if the command output in **Figure 4-4** is displayed.

Figure 4-4 Successful installation



3. Configure the Agent by following the procedure in **Restoring the Agent Configurations (Linux)** or **(Optional) Manually Configuring the Agent (Linux)**.

   NOTE

   - **Restoring Agent Configurations** explains how to configure **AK/SK**, **RegionID**, and **ProjectId** in just a few clicks. You can also modify related configuration files by following the instructions in **(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

4.4.3 Restoring the Agent Configurations (Linux)

Scenarios

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

Most regions support one-click configuration of Agent permissions. You can choose **Server Monitoring** > **Elastic Cloud Server** and click **Configure** on top of the page. After the configuration is complete, the Agent configurations of all servers in these regions are restored by default, and the **Configure** button is no longer displayed. If the system displays a message indicating that you not have the required permission, obtain the permission by referring to What Can I Do If the System Displays a Message Indicating Insufficient Permissions When I Click Configure on the Server Monitoring Page? After the Agent permission is granted for a region, you do not need to perform the following steps.

NOTE

- The **Restore Agent Configurations** option is available for Agent 1.0.5 or later. If the Agent version is earlier than 1.0.5, 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)**.
- For details about how to query the Agent version, see **How Do I Query the Current Agent Version?**
- The **Restore Agent Configurations** option is unavailable for BMSs. For details, see **(Optional) Manually Configuring the Agent (Linux)**.
- After the Agent is configured, 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.

Restoring the Agent Configurations

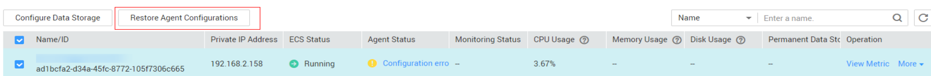
1. Log in to the management console.
2. Under **Management & Deployment**, select **Cloud Eye**. In the navigation pane on the left, choose **Server Monitoring**.
3. On the **Server Monitoring** page, select a server that has the Agent installed.
4. Click **Restore Agent Configurations**.

   NOTE

   Currently, one-click restoration of the Agent configuration is supported in most regions. If there is no **One-Click Restore** button, the Agent configurations of all servers are restored by default.
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 4-5 Restore Agent Configurations



4.4.4 (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 check the Telescope version:

   if [[-f /usr/local/uniagent/extension/install/telescope/bin/telescope]]; then /usr/local/uniagent/extension/install/telescope/bin/telescope -v; else echo 0; fi

   – If **0** is returned, the old Agent is used. For details about how to manually configure the Agent, see **Procedure (Old Agent)**.

   – If other values are returned, the new Agent is used. For details about how to manually configure the Agent, see **Procedure (New Agent)**.

Procedure (New Agent)

1. Log in to an ECS as user **root**.
2. Modify the **conf.json** file in the **conf** directory.

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

      vi /usr/local/uniagent/conf/conf.json

   b. Modify the parameters in the file. For details, see **Table 4-2**.

      ECS parameters

```
{
   "Endpoint":"https://ces.XXXXXXXX.XXX.com",
   "InstanceId": "",
   "ProjectId": "",
   "AccessKey": "",
   "SecretKey": "",
   "AesSecretKey": "rfvt_huawei_iommuylpimafj1dagskm",
}
```

Table 4-2 conf.json parameter description

Parameter	Description
Endpoint	Specifies the Cloud Eye endpoint URL in the region where the ECS or BMS is located. For example, if the ECS or BMS is located in region **CN North-Beijing1**, the value of **Endpoint** is **ces.cn-north-1.myhuaweicloud.com**.

Parameter	Description
InstanceId	If you have logged in to a HUAWEI CLOUD ECS, retain the default value of **InstanceId**. If the server is not running on HUAWEI CLOUD, set this parameter to the server ID. The server ID must be able to identify the server and must be compliant with the following format: b96e7af6-afa6-469c-8532-201f1f93b233.
ProjectId	If you have logged in to a HUAWEI CLOUD ECS, retain the default value of **ProjectId**. For other servers, obtain the value for this parameter by performing 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	If you have logged in to a HUAWEI CLOUD ECS, you do not need to set this parameter. For other servers, obtain the value for this parameter by performing the following operations: Log in to the Cloud Eye console, click the username in the upper right corner, and choose **My Credentials**. In the navigation pane on the left, 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, you are advised to use an IAM username with the **CES Administrator** and **LTS Administrator** permissions. For details, see **Creating a User Group and Assigning Permissions** and **Create IAM Users and Log In**. ● 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.
AesSecretKey	Retain the default value **rfvt_huawei_iommuylpimafj1dagskm**.

3. Modify the **conf.json** file in the **bin** directory.

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

vi /usr/local/uniagent/extension/install/telescope/bin/conf.json

b. Modify the parameters in the file. For details, see **Table 4-3**.

ECS parameters

```
{
    "InstanceId":"XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX",
    "ProjectId": "XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX",
    "AccessKey": "XXXXXXXXXXXXXXXXXXXX",
    "SecretKey": "XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX",
    "RegionId": "cn-east-3",
    "ClientPort": 0,
    "PortNum": 200
}
```

Procedure (Old Agent)

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/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 4-3**.

   ECS parameters

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

   BMS parameters

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

Table 4-3 Public parameters

<table>
<tr><th>Parameter</th><th>Description</th></tr>
<tr><td>InstanceId</td><td>(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.</td></tr>
<tr><td>ProjectId</td><td>(Optional) Specifies the project ID.
If you do not configure ProjectId, retain "ProjectId": "".
If you configure it, perform the following operations:
Log in to the Cloud Eye console, click the username in the upper right corner, and choose My Credentials.
Under Projects, obtain the project ID for the region where the ECS or BMS is located.</td></tr>
<tr><td>AccessKey / SecretKey</td><td>Specifies the access keys, which can be obtained by performing the following operations:
Log in to the Cloud Eye console, click the username in the upper right corner, and choose My Credentials. In the navigation pane on the left, 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, you are advised to use an IAM username with the CES Administrator and LTS Administrator permissions. For details, see Creating a User Group and Assigning Permissions and Create IAM Users and Log In.
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.</td></tr>
<tr><td>RegionId</td><td>Specifies the region ID. For example, if the ECS or BMS is located in region CN North-Beijing1, the value of RegionId is cn-north-1. For IDs of other regions, see https://developer.huaweicloud.com/endpoint.</td></tr>
</table>

Parameter	Description
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 the value of **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 4-4**.
```
{
  "Endpoint": "https://ces.cn-north-1.myhuaweicloud.com"
}
```

Table 4-4 Parameter setting of the metric collection module

Parameter	Description
Endpoint	Specifies the Cloud Eye endpoint URL in the region of the ECS or BMS. For example, if the ECS or BMS is in the CN North-Beijing1 region, the URL is **ces.cn-north-1.myhuaweicloud.com**. For the endpoint values of other regions, log in at **https://developer.huaweicloud.com/endpoint**.

NOTE

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

4.5 Installing and Configuring the Agent on a Windows ECS

4.5.1 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

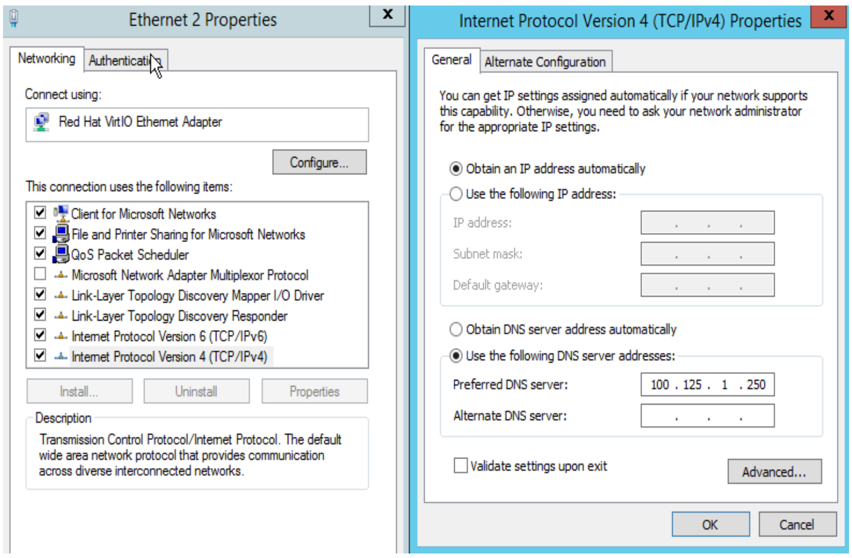
DNS and security group configuration are intended for the primary NIC.

Modifying the DNS Server Address (Windows GUI)

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

1. On the **Service List** page, choose **Computing** > **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 4-6 Adding the DNS server address (Windows)



NOTE

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

CN North-Beijing1: 100.125.1.250,100.125.21.250

CN North-Beijing4: 100.125.1.250,100.125.129.250

CN Southwest-Guiyang1: 100.125.1.250,100.125.129.250

CN East-Shanghai1: 100.125.1.250,100.125.64.250

CN East-Shanghai2: 100.125.17.29,100.125.135.29

CN South-Guangzhou: 100.125.1.250,100.125.136.29

AP-Hong-Kong: 100.125.1.250,100.125.3.250

AP-Bangkok: 100.125.1.250

AP-Singapore: 100.125.1.250,100.125.128.250

AF-Johannesburg: 100.125.1.250

LA-Santiago: 100.125.1.250

LA-Sao Paulo1: 100.125.1.22

Modifying the DNS Server Address (Management Console)

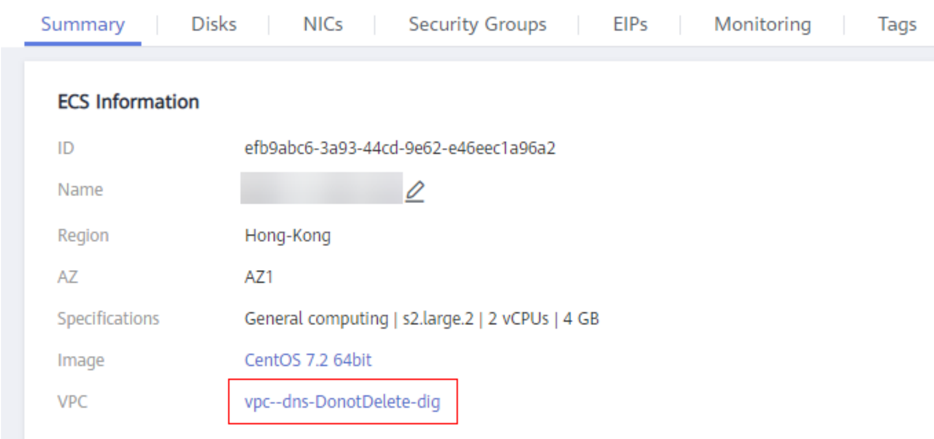
The following describes how to modify the DNS server address of an ECS on the management console. The operations for BMSs are similar.

1. In the upper left corner, select a region and project.
2. On the **Service List** page, choose **Computing** > **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 4-7 VPC



4. Click the name of the target VPC.
5. In the **Networking Components** area, click the number following **Subnets**.

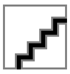
   The **Subnets** page is displayed.
6. In the subnet list, click the name of target subnet.

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**.

   Figure 4-8 Edit DNS Server Address

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. 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 4-5**.

Table 4-5 Security group rules

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

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

4.5.2 Installing and Configuring the Agent (Windows)

Scenarios

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

Constraints

The Agent cannot be installed on the Windows BMSs.

Only 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 4-6 Installation package path

Name	Format	Download Path
Installation package for 64-bit Windows	zip/exe	CN North-Beijing1: **https://obs.cn-north-1.myhuaweicloud.com/uniagent-cn-north-1/script/agent_install.exe** CN North-Beijing4: **https://obs.cn-north-4.myhuaweicloud.com/uniagent-cn-north-4/script/agent_install.exe** CN Southwest-Guiyang 1: **https://obs.cn-southwest-2.myhuaweicloud.com/uniagent-cn-southwest-2/script/agent_install.exe** CN South-Guangzhou: **https://obs.cn-south-1.myhuaweicloud.com/uniagent-cn-south-1/script/agent_install.exe** CN South-Guangzhou: **https://obs.cn-south-2.myhuaweicloud.com/uniagent-cn-south-2/script/agent_install.exe** CN East-Shanghai2: **https://obs.cn-east-2.myhuaweicloud.com/uniagent-cn-east-2/script/agent_install.exe** CN East-Shanghai1: **https://obs.cn-east-3.myhuaweicloud.com/uniagent-cn-east-3/script/agent_install.exe** AP-Hong-Kong: **http://obs.ap-southeast-1.myhuaweicloud.com/uniagent-ap-southeast-1/script/agent_install.exe** AP-Bangkok: **https://obs.ap-southeast-2.myhuaweicloud.com/uniagent-ap-southeast-2/script/agent_install.exe** AP-Bangkok: **https://obs.ap-southeast-3.myhuaweicloud.com/uniagent-ap-southeast-3/script/agent_install.exe** AF-Johannesburg: **https://obs.af-south-1.myhuaweicloud.com/uniagent-af-south-1/script/agent_install.exe** LA-Santiago: **https://telescope-la-south-2.obs.la-south-2.myhuaweicloud.com/agent/telescope_windows_amd64.zip** LA-Sao Paulo 1: **https://telescope-sa-brazil-1.obs.sa-brazil-1.myhuaweicloud.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 or move **agent_install.exe** to this directory.
4. Double-click the **agent_install.exe** or **install.bat** script to install and start the Agent.

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

   NOTE

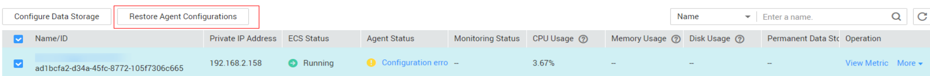
   After the Agent is configured, its status is still displayed as **Uninstalled** because no monitoring data is reported yet. Wait 3 to 5 minutes and refresh the page.

   Most regions support one-click restoration of Agent configurations. You only need to click **Configure** without selecting servers. After the configuration is complete, the Agent configurations of all servers in these regions are restored by default, you do not need to perform the following step, and the **Configure** button is no longer displayed. If the system displays a message indicating that you not have the required permission, obtain the permission by referring to What Can I Do If the System Displays a Message Indicating Insufficient Permissions When I Click Configure on the Server Monitoring 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 4-9 Restore Agent Configurations



4.5.3 (Optional) Manually Configuring the Agent (Windows)

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 the Windows BMSs.

Only 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 an ECS as user **root**.
2. Check the installation path and the Telescope version.
   - The installation path is **C:\Program Files\telescope**. If the old Agent is used, see **Procedure (Old Telescope)**.
   - The installation path is **C:\Program Files\uniagent\extension\install\telescope**. If the new Agent is used, see **Procedure (New Telescope)**.

Procedure (New Telescope)

1. Log in to the ECS.
2. Open the **conf.json** file in the **C:\Program Files\uniagent\conf** folder.
3. Set the following parameters. For details, see **Table 4-7**.

   ECS parameters

```
{
   "Endpoint":"https://ces.XXXXXXXX.XXX.com",
   "InstanceId": "",
   "ProjectId": "",
   "AccessKey": "",
   "SecretKey": "",
   "AesSecretKey": "rfvt_huawei_iommuylpimafj1dagskm",
}
```

Table 4-7 conf.json parameter description

Parameter	Description
Endpoint	Specifies the Cloud Eye endpoint URL in the region where the ECS or BMS is located. For example, if the ECS or BMS is located in region **CN North-Beijing1**, the value of **Endpoint** is **ces.cn-north-1.myhuaweicloud.com**.
InstanceId	If you have logged in to a HUAWEI CLOUD ECS, retain the default value of **InstanceId**. If the server is not running on HUAWEI CLOUD, set this parameter to the server ID. The server ID must be able to identify the server and must be compliant with the following format: b96e7af6-afa6-469c-8532-201f1f93b233.

<table>
<tr><th>Parameter</th><th>Description</th></tr>
<tr><td>ProjectId</td><td>If you have logged in to a HUAWEI CLOUD ECS, retain the default value of ProjectId.
For other servers, obtain the value for this parameter by performing 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.</td></tr>
<tr><td>AccessKey/ SecretKey</td><td>If you have logged in to a HUAWEI CLOUD ECS, you do not need to set this parameter.
For other servers, obtain the value for this parameter by performing the following operations:
Log in to the Cloud Eye console, click the username in the upper right corner, and choose My Credentials. In the navigation pane on the left, 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, you are advised to use an IAM username with the CES Administrator and LTS Administrator permissions. For details, see Creating a User Group and Assigning Permissions and Create IAM Users and Log In.
● 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.</td></tr>
<tr><td>AesSecretKey</td><td>Retain the default value rfvt_huawei_iommuylpimafj1dagskm.</td></tr>
</table>

4. Open the **conf.json** file in the **C:\Program Files\uniagent\extension\install\telescope\bin** folder.
5. Set the following parameters. For details, see **Table 4-8**.

   ECS parameters

```
{
    "InstanceId":"XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX",
    "ProjectId": "XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX",
    "AccessKey": "XXXXXXXXXXXXXXXXXXXX",
    "SecretKey": "XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX",
    "RegionId": "cn-east-3",
    "ClientPort": 0,
    "PortNum": 200
}
```

NOTE

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

Procedure (Old Telescope)

1. Log in to the ECS.
2. Open the **conf.json** file in the **telescope_windows_amd64\bin** folder.
3. Set the following parameters. For details, see **Table 4-8**.

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

Table 4-8 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	(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.

<table>
<tr><th>Parameter</th><th>Description</th></tr>
<tr><td>AccessKey/
SecretKey</td><td>Specifies the access keys, which can be obtained by performing the following operations:
Log in to the Cloud Eye console, click the username in the upper right corner, and choose My Credentials. In the navigation pane on the left, 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, you are advised to use an IAM username with the CES Administrator and LTS Administrator permissions. For details, see Creating a User Group and Assigning Permissions and Create IAM Users and Log In.
● 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.</td></tr>
<tr><td>RegionId</td><td>Specifies the region ID. For example, if the ECS or BMS is located in region CN North-Beijing1, the value of RegionId is cn-north-1. For IDs of other regions, see https://developer.huaweicloud.com/endpoint.</td></tr>
<tr><td>ClientPort</td><td>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.</td></tr>
<tr><td>PortNum</td><td>Specifies the number of ports configured for the Agent.
NOTE
The default value is 200. If the value of ClientPort is 5000, the port range will be 5000 to 5199.</td></tr>
<tr><td>BmsFlag</td><td>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.</td></tr>
</table>

4. Wait for a few minutes, if **Agent Status** is **Running**, the Agent has been installed and starts to collect fine-grained metric data.

4.6 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.
- Agents cannot be installed in batches on BMSs.

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:

   NOTE

   The script supports x86 and Kunpeng Arm-based ECSs.

   CN North-Beijing1:

   ```
   cd /usr/local && curl -k -O  https://obs.cn-north-1.myhuaweicloud.com/uniagent-cn-north-1/script/batch_agent_install.sh && bash batch_agent_install.sh
   ```

   CN North-Beijing4:

   ```
   cd /usr/local && curl -k -O  https://obs.cn-north-4.myhuaweicloud.com/uniagent-cn-north-4/script/batch_agent_install.sh && bash batch_agent_install.sh
   ```

   CN South-Guangzhou:

   ```
   cd /usr/local && curl -k -O  https://obs.cn-south-1.myhuaweicloud.com/uniagent-cn-south-1/script/batch_agent_install.sh && bash batch_agent_install.sh
   ```

   CN South-Shenzhen:

   ```
   cd /usr/local && curl -k -O  https://obs.cn-south-2.myhuaweicloud.com/uniagent-cn-south-2/script/batch_agent_install.sh && bash batch_agent_install.sh
   ```

   CN East-Shanghai1:


```
cd /usr/local && curl -k -O  https://obs.cn-east-3.myhuaweicloud.com/uniagent-cn-east-3/script/
batch_agent_install.sh && bash batch_agent_install.sh
```

CN East-Shanghai2:

```
cd /usr/local && curl -k -O  https://obs.cn-east-2.myhuaweicloud.com/uniagent-cn-east-2/script/
batch_agent_install.sh && bash batch_agent_install.sh
```

CN Southwest-Guiyang1:

```
cd /usr/local && curl -k -O  https://obs.cn-southwest-2.myhuaweicloud.com/uniagent-cn-southwest-2/
script/batch_agent_install.sh && bash batch_agent_install.sh
```

AP-Hong-Kong:

```
cd /usr/local && curl -k -O  https://obs.ap-southeast-1.myhuaweicloud.com/uniagent-ap-southeast-1/
script/batch_agent_install.sh && bash batch_agent_install.sh
```

AP-Bangkok:

```
cd /usr/local && curl -k -O  https://obs.ap-southeast-2.myhuaweicloud.com/uniagent-ap-southeast-2/
script/batch_agent_install.sh && bash batch_agent_install.sh
```

AP-Singapore:

```
cd /usr/local && curl -k -O  https://obs.ap-southeast-3.myhuaweicloud.com/uniagent-ap-southeast-3/
script/batch_agent_install.sh && bash batch_agent_install.sh
```

AF-Johannesburg:

```
cd /usr/local && curl -k -O  https://obs.af-south-1.myhuaweicloud.com/uniagent-af-south-1/script/
batch_agent_install.sh && bash batch_agent_install.sh
```

LA-Santiago:

```
cd /usr/local && wget https://telescope-la-south-2.obs.la-south-2.myhuaweicloud.com/scripts/
agentBatchPackage.sh && chmod 755 agentBatchPackage.sh && ./agentBatchPackage.sh
```

LA-Sao Paulo1:

```
cd /usr/local && wget http://telescope-sa-brazil-1.obs.myhuaweicloud.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 properly started 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 the Agent is configured, 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

4.7 Managing the Agent

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

4.7.1 Managing the Agent (Linux)

NOTE

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

Viewing the Agent Version

1. Log in to the target ECS as user **root**.
2. Run the following command to check the Agent version:

   if [[-f /usr/local/uniagent/extension/install/telescope/bin/telescope]]; then /usr/local/uniagent/extension/install/telescope/bin/telescope -v; else echo 0; fi

   – If **0** is returned, the old Agent version is used.
   – If other results are returned, the new Agent version is used.

Updating the Agent to the Latest Version

Constraints

- Batch Agent update cannot be performed across regions.

Procedure

1. Log in to an ECS as user **root**.
2. Run the following command to check the Agent version:

   if [[-f /usr/local/uniagent/extension/install/telescope/bin/telescope]]; then /usr/local/uniagent/extension/install/telescope/bin/telescope -v; else echo 0; fi

   – If **0** is returned, the old Agent is used.
   – If other values are returned, the new Agent is used.
3. Create the **iplist.txt** file in the **/usr/local** directory of the ECS and sort out all ECSs whose Agent needs to be updated.

NOTE

In the **iplist.txt** file, ensure that each line contains one IP address and one root user password. Then you can perform batch Agent upgrade based on the list.

In the following example, **abcd** is the password. Enter the password based on the site requirements.

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

4. Determine the architecture of the ECS where the script is executed.

   if [[$(arch) == "aarch64"]]; then echo " uniagent_patch_installer_arm64"; else echo " uniagent_patch_installer_amd64";fi

5. Run the batch update command. Replace ***Region ID*** in the following command with the correct region ID, and replace *${batch_installer}* with the returned result in **4**.

   cd /usr/local && curl -k -O https://obs.*${Region_id}*.myhuaweicloud.com/uniagent-*${Region_id}*/script/*${batch_installer}* && chmod +x *${batch_installer}* && ./*${batch_installer}* -c "cd /usr/local/telescope && bash uninstall.sh && cd /usr/local && curl -k -O https://obs.*${Region_id}*.myhuaweicloud.com/uniagent-*${Region_id}*/script/agent_install.sh && bash agent_install.sh"

   Take the x86 ECS in the AP-Hong Kong region as an example. Run the following command:

```
cd /usr/local && curl -k -O https://obs.ap-southeast-1.myhuaweicloud.com/uniagent-ap-southeast-1/script/uniagent_patch_installer_amd64 && chmod +x uniagent_patch_installer_amd64 && ./uniagent_patch_installer_amd64 -c "cd /usr/local/telescope && bash uninstall.sh && cd /usr/local && curl -k -O https://obs.ap-southeast-1.myhuaweicloud.com/uniagent-ap-southeast-1/script/agent_install.sh && bash agent_install.sh"
```

Checking the Agent Status (Old Version)

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:

```
"Telescope process is running well."
```

Checking the Agent Status (New Version)

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

/usr/local/uniagent/extension/install/telescope/telescoped status

The following message indicates that the Agent is running properly:

```
"Telescope process is running well."
```

Starting the Agent (Old Version)

/usr/local/telescope/telescoped start

Starting the Agent (New Version)

/usr/local/uniagent/extension/install/telescope/telescoped start

Restarting the Agent (Old Version)

/usr/local/telescope/telescoped restart

Restarting the Agent (New Version)

Check the Agent PID.

ps -ef |grep telescope

After the process is forcibly stopped, wait for 3 to 5 minutes for the Agent to automatically restart. **Figure 4-10** shows an operation example.

kill -9 *PID*

Figure 4-10 Restarting the Agent

```
[root@arm1-2 ~]# ps -ef |grep telescope
root     11671     1  0 10:23 ?        00:00:00 ./telescope
root     20245 19980  0 10:33 pts/1    00:00:00 grep --color=auto telescope
[root@arm1-2 ~]#
[root@arm1-2 ~]#
[root@arm1-2 ~]# kill -9 11671
```

Stopping the Agent (Old Version)

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

Stopping the Agent (New Version)

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

/usr/local/uniagent/extension/install/telescope/telescoped stop

Uninstalling the Agent (Old Version)

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.

Uninstalling the Agent (New Version)

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**.

Run the following command to uninstall the Agent:

cd /usr/local/uniagent/script/

./uninstall.sh

NOTICE

Before reinstalling the Agent, manually delete the previous Agent installation package. The new Agent installation package is stored in **/usr/local/uniagent_install_amd64.sh**.

4.7.2 Managing the Agent (Windows)

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.

4.8 Installing the Plug-in for Collecting GPU and RAID Metrics (Linux)

Scenarios

This topic describes how to install the plug-in to collect ECS GPU and BMS RAID metrics.

NOTE

- ECSs support GPU metrics while BMSs do not.
- BMSs support RAID metrics while ECSs do not.
- If the Agent is upgraded to 1.0.5 or later, the corresponding plug-in must use the latest version. Otherwise, the metric collection will fail.

Prerequisites

- The Agent has been installed and is running properly.
- GPU metric collection requires ECSs to support GPU.
- Run the following command to check the Agent version:

  if [[-f /usr/local/uniagent/extension/install/telescope/bin/telescope]]; then /usr/local/uniagent/extension/install/telescope/bin/telescope -v; else echo 0; fi

  – If **0** is returned, the old Agent is used.
  – If other values are returned, the new Agent is used.

Procedure

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

   NOTE

   - To monitor the BMS software RAID metrics, log in to a BMS.
   - The examples in the following procedure are based on the GPU plug-in installation. The installation for the software RAID plug-in is similar.

2. Run the following command to go to the Agent installation path **/usr/local/telescope**:

   Old Agent:

   cd /usr/local/telescope

   New Agent:

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

3. Run the following command to create the **plugins** folder:

   mkdir plugins

4. Run the following command to enter the **plugins** folder:

   cd plugins

5. To download the script of the GPU metric collection plug-in, run the following command:

   wget *https://telescope.obs.cn-north-1.myhuaweicloud.com/gpu_collector*

Table 4-9 Obtaining the plug-in installation package

Name	Download Path
Linux 64-bit installation package of the GPU metric collection plug-in	CN North-Beijing1: **https://obs.cn-north-1.myhuaweicloud.com/uniagent-cn-north-1/extension/gpu/gpu_collector** CN North-Beijing4: **https://obs.cn-north-4.myhuaweicloud.com/uniagent-cn-north-4/extension/gpu/gpu_collector** CN South-Guangzhou: **https://obs.cn-south-1.myhuaweicloud.com/uniagent-cn-south-1/extension/gpu/gpu_collector** CN East-Shanghai2: **https://obs.cn-east-2.myhuaweicloud.com/uniagent-cn-east-2/extension/gpu/gpu_collector** AP-Hong-Kong: **https://obs.ap-southeast-1.myhuaweicloud.com/uniagent-ap-southeast-1/extension/gpu/gpu_collector** AP-Bangkok: **https://obs.ap-southeast-2.myhuaweicloud.com/uniagent-ap-southeast-2/extension/gpu/gpu_collector** AP-Bangkok: **https://obs.ap-southeast-3.myhuaweicloud.com/uniagent-ap-southeast-3/extension/gpu/gpu_collector**

Name	Download Path
Linux 64-bit installation package of the RAID metric collection plug-in	CN North-Beijing1: **https://obs.cn-north-1.myhuaweicloud.com/uniagent-cn-north-1/extension/raid/raid_monitor.sh** CN North-Beijing4: **https://obs.cn-north-4.myhuaweicloud.com/uniagent-cn-north-4/extension/raid/raid_monitor.sh** CN South-Guangzhou: **https://obs.cn-south-1.myhuaweicloud.com/uniagent-cn-south-1/extension/raid/raid_monitor.sh** CN East-Shanghai2: **https://obs.cn-east-2.myhuaweicloud.com/uniagent-cn-east-2/extension/raid/raid_monitor.sh** AP-Hong-Kong: **https://obs.ap-southeast-1.myhuaweicloud.com/uniagent-ap-southeast-1/extension/raid/raid_monitor.sh** AP-Bangkok: **https://obs.ap-southeast-2.myhuaweicloud.com/uniagent-ap-southeast-2/extension/raid/raid_monitor.sh**

6. Run the following command to add the script execution permissions:
   chmod 755 gpu_collector
7. Run the following command to create the **conf.json** file, add the configuration content, and configure the plug-in path and metric collection period **crontime**, which is measured in seconds:
   vi conf.json
   Configuring the GPU metric plug-in old Telescope

```
{
  "plugins": [
   {
     "path": "/usr/local/telescope/plugins/gpu_collector",
     "crontime": 60
   }
 ]
}
```

   Configuring the GPU metric plug-in (new Telescope)

```
{
  "plugins": [
   {
     "path": "/usr/local/uniagent/extension/install/telescope/plugins/gpu_collector",
     "crontime": 60
   }
 ]
}
```

   Configuring the RAID metric plug-in (old Telescope)

```
{
  "plugins": [
   {
     "path": "/usr/local/telescope/plugins/raid_monitor.sh",
     "crontime": 60
   }
 ]
}
```

Configuring the RAID metric plug-in (new Telescope)

```
{
  "plugins": [
   {
     "path": "/usr/local/uniagent/extension/install/telescope/plugins/raid_monitor.sh",
     "crontime": 60
   }
  ]
}
```

NOTE

- The parameters **gpu_collector** and **raid_monitor.sh** indicate the GPU plug-in and RAID plug-in configuration.
- The collection period of the plug-in is 60 seconds. If the collection period is incorrectly configured, the metric collection will be abnormal.
- Do not change the plug-in path without permission. Otherwise, the GPU metric collection will be abnormal.

8. Open the **conf_ces.json** file in the **/usr/local/telescope/bin** directory. Add **"EnablePlugin": true** to the file to enable the metric collection function of the plug-in.

   NOTE

   The path of the new Telescope is **/usr/local/uniagent/extension/install/telescope/bin**.

```
{
   "Endpoint": "Region address. Retain the default value.",
   "EnablePlugin": true
}
```

9. Restart the Agent:

   Old Telescope:

   /usr/local/telescope/telescoped restart

   New Telescope:

   ps -ef | grep telescope | grep -v grep | awk '{print $2}' | xargs kill -9

4.9 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-ins support only the Linux OS. ECSs where the plug-ins are to be installed must be in the same VPC as the connection.

Prerequisites

- You have installed the Cloud Eye Agent. For details, see **Agent Installation and Configuration**.
- The plug-ins have been restored. For details, see **Restoring the Agent Configurations (Linux)**.
- 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 HUAWEI CLOUD regions, you can use the one-click installation script to configure the plug-ins. **Table 4-11** lists the supported regions.

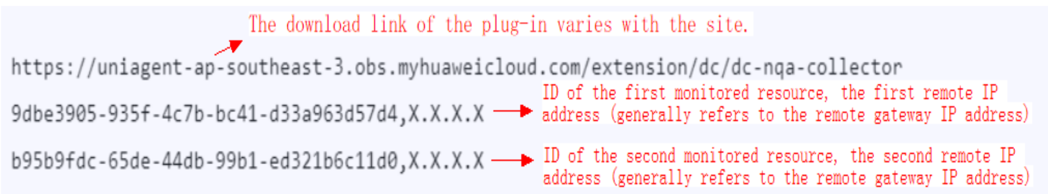
1. Log in to an ECS as user **root**.
2. Run the following command to create the **user.txt** file in the **usr/local/** directory and add user information, including the plug-in download link, monitored resource ID, and remote IP address:

   cd usr/local/

   vi user.txt

   user.txt is in the following format:

   Figure 4-11 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 4-10**.

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

- **Resource ID**: The value 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 plug-in is installed, if you want to add resources to be monitored, you only need to edit the **user.txt** file and add the corresponding ID and IP address in sequence.

Table 4-10 Obtaining the plug-in installation package

Name	Download Path
dc-nqa-collector installation package	CN North-Beijing4: **https://uniagent-cn-north-4.obs.myhuaweicloud.com/extension/dc/dc-nqa-collector** CN North-Beijing1: **https://uniagent-cn-north-1.obs.myhuaweicloud.com/extension/dc/dc-nqa-collector** CN East-Shanghai1: **https://uniagent-cn-east-3.obs.myhuaweicloud.com/extension/dc/dc-nqa-collector** CN East-Shanghai2: **https://uniagent-cn-east-2.obs.myhuaweicloud.com/extension/dc/dc-nqa-collector** CN South-Guangzhou: **https://uniagent-cn-south-1.obs.myhuaweicloud.com/extension/dc/dc-nqa-collector** CN Southwest-Guiyang1: **https://uniagent-cn-southwest-2.obs.myhuaweicloud.com/extension/dc/dc-nqa-collector** AP-Hong-Kong: **https://uniagent-ap-southeast-1.obs.myhuaweicloud.com/extension/dc/dc-nqa-collector** AP-Bangkok: **https://uniagent-ap-southeast-2.obs.myhuaweicloud.com/extension/dc/dc-nqa-collector** AP-Singapore: **https://uniagent-ap-southeast-3.obs.myhuaweicloud.com/extension/dc/dc-nqa-collector** Africa-Johannesburg: **https://uniagent-af-south-1.obs.myhuaweicloud.com/extension/dc/dc-nqa-collector** LA-Sao Paulo1: **https://uniagent-sa-brazil-1.obs.myhuaweicloud.com/extension/dc/dc-nqa-collector** LA-Santiago: **https://uniagent-la-south-2.obs.myhuaweicloud.com/extension/dc/dc-nqa-collector** LA-Mexico City 1: **https://uniagent-na-mexico-1.obs.myhuaweicloud.com/extension/dc/dc-nqa-collector**

Name	Download Path
history-dc-nqa-collector installation package	CN North-Beijing4: **https://uniagent-cn-north-4.obs.myhuaweicloud.com/extension/dc/history-dc-nqa-collector** CN North-Beijing1: **https://uniagent-cn-north-1.obs.myhuaweicloud.com/extension/dc/history-dc-nqa-collector** CN East-Shanghai1: **https://uniagent-cn-east-3.obs.myhuaweicloud.com/extension/dc/history-dc-nqa-collector** CN East-Shanghai2: **https://uniagent-cn-east-2.obs.myhuaweicloud.com/extension/dc/history-dc-nqa-collector** CN South-Guangzhou: **https://uniagent-cn-south-1.obs.myhuaweicloud.com/extension/dc/history-dc-nqa-collector** CN Southwest-Guiyang1: **https://uniagent-cn-southwest-2.obs.myhuaweicloud.com/extension/dc/history-dc-nqa-collector** AP-Hong-Kong: **https://uniagent-ap-southeast-1.obs.myhuaweicloud.com/extension/dc/history-dc-nqa-collector** AP-Bangkok: **https://uniagent-ap-southeast-2.obs.myhuaweicloud.com/extension/dc/history-dc-nqa-collector** AP-Singapore: **https://uniagent-ap-southeast-3.obs.myhuaweicloud.com/extension/dc/history-dc-nqa-collector** Africa-Johannesburg: **https://uniagent-af-south-1.obs.myhuaweicloud.com/extension/dc/history-dc-nqa-collector** LA-Sao Paulo1: **https://uniagent-sa-brazil-1.obs.myhuaweicloud.com/extension/dc/history-dc-nqa-collector** LA-Santiago: **https://uniagent-la-south-2.obs.myhuaweicloud.com/extension/dc/history-dc-nqa-collector** LA-Mexico City 1: **https://uniagent-na-mexico-1.obs.myhuaweicloud.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 4-11 One-click installation script of the Direct Connect plug-ins

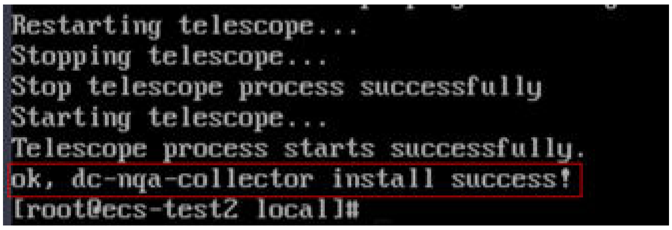
Region	Download Path
CN North-Beijing4	**https://uniagent-cn-north-4.obs.myhuaweicloud.com/extension/dc/dc-installer.sh**
CN North-Beijing1	**https://uniagent-cn-north-1.obs.myhuaweicloud.com/extension/dc/dc-installer.sh**
CN East-Shanghai1	**https://uniagent-cn-east-3.obs.myhuaweicloud.com/extension/dc/dc-installer.sh**
CN East-Shanghai2	**https://uniagent-cn-east-2.obs.myhuaweicloud.com/extension/dc/dc-installer.sh**
CN South-Guangzhou	**https://uniagent-cn-south-1.obs.myhuaweicloud.com/extension/dc/dc-installer.sh**
CN Southwest-Guiyang1	**https://uniagent-cn-southwest-2.obs.myhuaweicloud.com/extension/dc/dc-installer.sh**
AP-Hong-Kong	**https://uniagent-ap-southeast-1.obs.myhuaweicloud.com/extension/dc/dc-installer.sh**
AP-Bangkok	**https://uniagent-ap-southeast-2.obs.myhuaweicloud.com/extension/dc/dc-installer.sh**
AP-Singapore	**https://uniagent-ap-southeast-3.obs.myhuaweicloud.com/extension/dc/dc-installer.sh**
AF-Johannesburg	**https://uniagent-af-south-1.obs.myhuaweicloud.com/extension/dc/dc-installer.sh**
LA-Sao Paulo1	**https://uniagent-sa-brazil-1.obs.myhuaweicloud.com/extension/dc/dc-installer.sh**
LA-Santiago	**https://uniagent-la-south-2.obs.myhuaweicloud.com/extension/dc/dc-installer.sh**
LA-Mexico City1	**https://uniagent-na-mexico-1.obs.myhuaweicloud.com/extension/dc/dc-installer.sh**

4. Run the following command to run the one-click installation script of the plug-in.

If the installation is successful, the information shown in **Figure 4-12** is displayed.

bash dc-installer.sh

Figure 4-12 Successful installation



5. After the Agent is installed, wait for about 1 minute, log in to the management console, and view the Direct Connect monitoring data.

   Under **Management & Deployment**, 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 4-13 Network latency and packet loss rate

4.10 Process Monitoring

4.10.1 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, you need to 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. Under **Management & Deployment**, 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 4-12** describes the metrics of system processes.

Table 4-12 System process metrics

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

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

Viewing the Running Data of Top CPU Processes

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

NOTE

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

To query information about processes top CPU usages

1. Log in to the management console.
2. Under **Management & Deployment**, 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 4-13** lists **Process Monitoring** metrics.

Figure 4-14 Process Monitoring

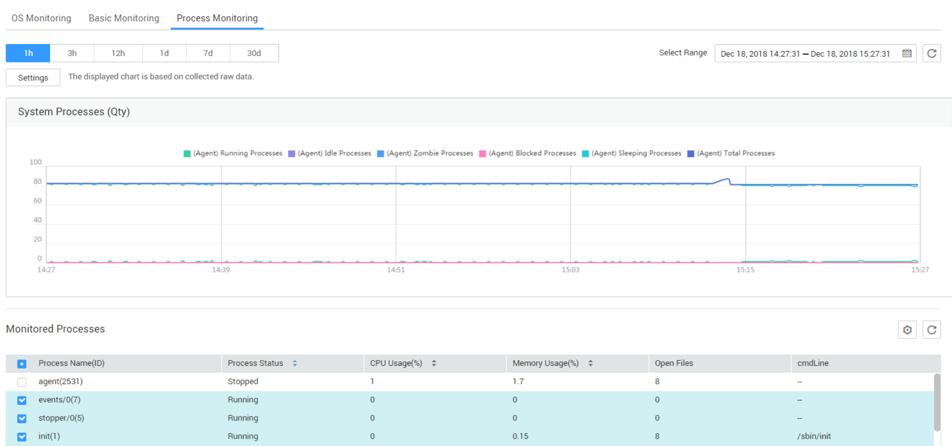
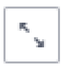


Table 4-13 Process Monitoring metrics

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**. You can also view historical monitoring data for any period during the last six months by customizing the monitoring period.

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

4.10.2 Adding Process Monitoring

Process monitoring is used to monitor active processes on a host. By default, the Agent collects active process information such as CPU usage, memory usage, and the number of files opened. The customized process monitoring function can collect the number of key processes and obtain the status of key processes at any time.

NOTE

Customized process monitoring is supported only in the CN North-Beijing1 (**cn-north-1**), CN North-Beijing4 (**cn-north-4**), CN South–Guangzhou (**cn-south-1**), and CN East–Shanghai2 (**cn-east-2**) regions. If you want to use this function in other regions, contact customer service.

Monitoring Specified Processes

Assume that the following processes are running on a server:

```
/usr/bin/java
/usr/bin/ntpd
/telescope
/usr/bin/python
```

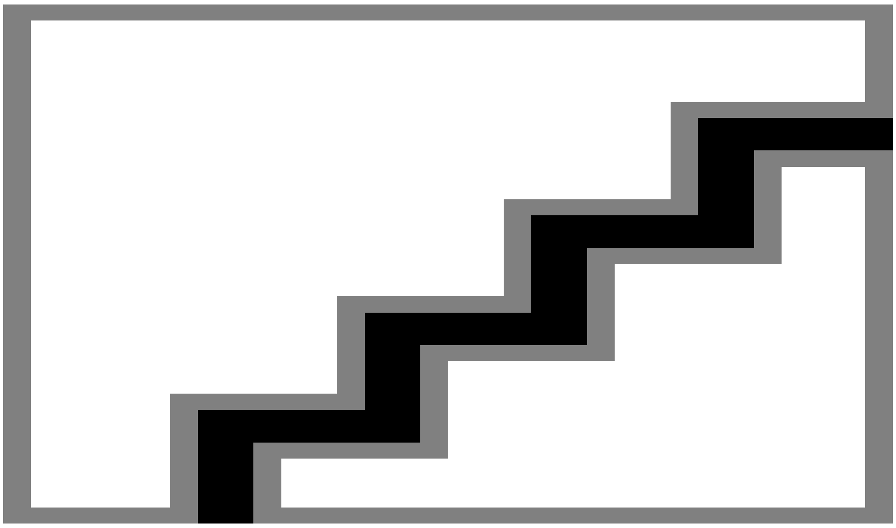
Three keywords are configured, and the collection results are as follows:

- Key word: Java, number of processes: 1
- Key word: telescope, number of processes: 1
- Key word: /usr/bin, number of processes: 3

Add specified processes.

1. Log in to the management console.
2. Under **Management & Deployment**, 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. On the **Process Monitoring** page, click **Configure** on the right of the **Custom Processes** area. On the **Configure Monitoring for Custom Process** page, configure the process name or keyword.

Figure 4-15 Configure Monitoring for Custom Process



NOTE

You do not need to configure the **Processes** column. After you set the process name, the system will return the number of matched processes.

After the configuration is complete, you can view the number of custom processes in the **Custom Processes** area on the **Process Monitoring** tab.

Enabling Alarm Notification for Custom Process Monitoring

You can configure the alarm notification function. When the number of processes decreases or increases, Cloud Eye will notify you immediately.

To enable alarm notifications custom processes, perform the following steps:

1. Log in to the management console.
2. Under **Management & Deployment**, 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. On the **Process Monitoring** page, click **Configure** on the right of the **Custom Processes** area.

   The **Configure Monitoring for Custom Process** box is displayed.
7. Locate the desired process and click **Create Alarm Rule**.
8. Configure alarm rule information and set **Alarm Policy** to **(Agent) Specifies Processes**. **Creating an Alarm Rule for an ECS or BMS (Agent) XX Metric** lists the parameters to be configured.

4.11 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 (Windows)**.

Procedure

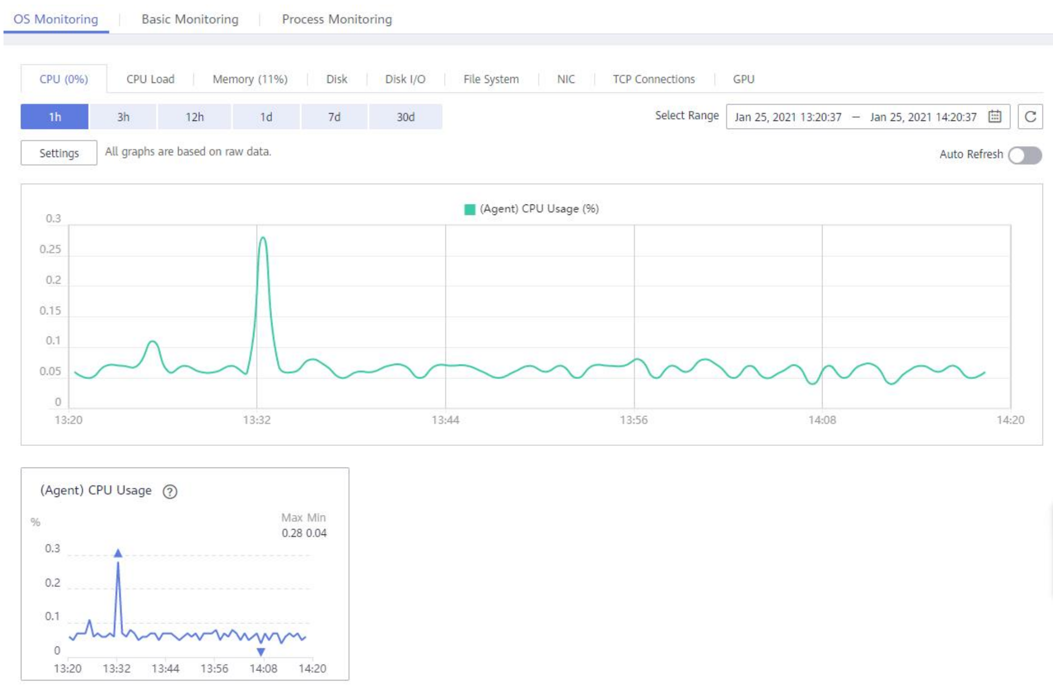
1. Log in to the management console.
2. Under **Management & Deployment**, select **Cloud Eye**.
3. View ECS or BMS metrics.

   NOTE

   For services that support enterprise projects, the system displays, by default, the host list of the enterprise projects on which you have permissions. **Enterprise Project** is available only in region **CN East-Shanghai1**.

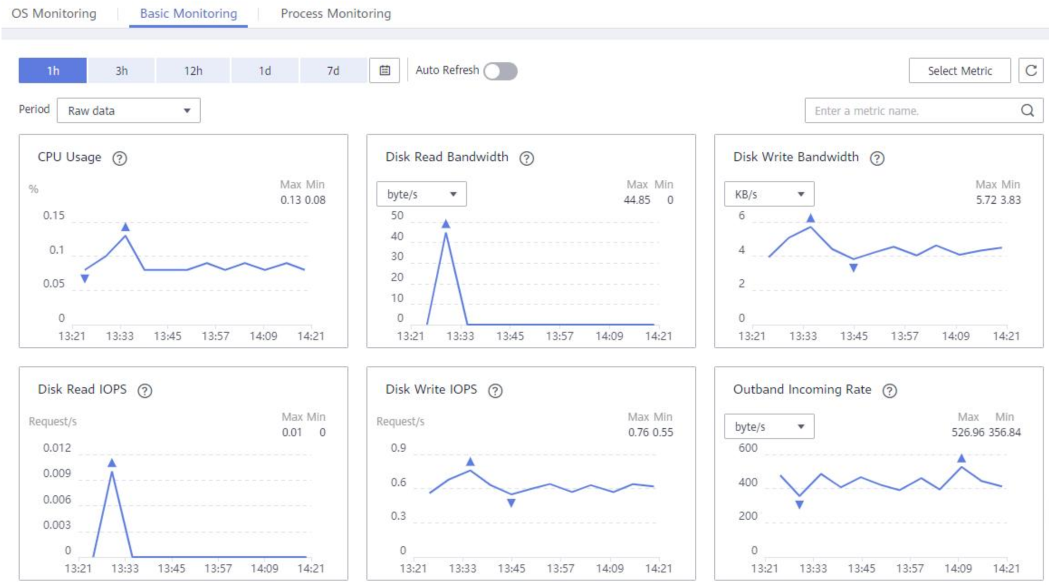
   – To view OS monitoring metrics of an ECS, choose **Elastic Cloud Server**, and click **View Metric** in the **Operation** column.

Figure 4-16 OS Monitoring



– To view basic monitoring metrics of an ECS, choose **Elastic Cloud Server**. Click **View Metric** in the **Operation** column and click **Basic Monitoring**.

Figure 4-17 Basic Monitoring



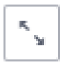
– To view OS monitoring metrics of a BMS, choose **Bare Metal Server**, and click **View Metric** in the **Operation** column.

– To view processing monitoring metrics, choose **Elastic Cloud Server**, and click **View Metric** in the **Operation** column. On the displayed page, click **Process Monitoring**.

4. View metrics.

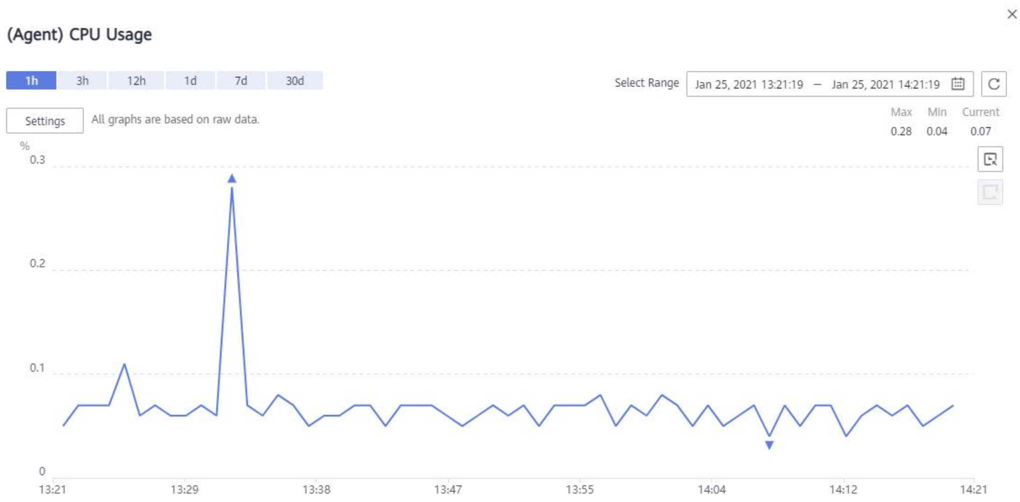
   In the upper part of the **OS Monitoring** page, different metric types, such as CPU, memory, and disk metrics are displayed.

   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 4-18 (Agent) CPU Usage



6. In the upper left corner of the graph, click **Settings** to 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.
   - The GPU metric data in **1h**, **3h**, **12h**, and **1d** is the raw data collected in the collection period set in **7**.
   - After clicking the zoom in icon in the upper right of an enlarged graph, you can drag the mouse to customize the time range.

4.12 Creating an Alarm Rule for an ECS or BMS (Agent) *XX* Metric

Scenarios

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

Procedure

1. Log in to the management console.
2. In the upper left corner, select a region and project.
3. Under **Management & Deployment**, 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 set the parameters.
   a. Set the alarm rule name, description, and associated enterprise project.

Table 4-14 Parameter description

Parameter	Description
Name	Specifies the alarm rule name. The system generates a random name, which you can modify.
Description	(Optional) Provides supplementary information about the alarm rule.
Enterprise Project	Specifies the enterprise project the alarm rule belongs to. Only users with the enterprise project permissions can view and manage the alarm rule.

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

Figure 4-19 Configuring the alarm content

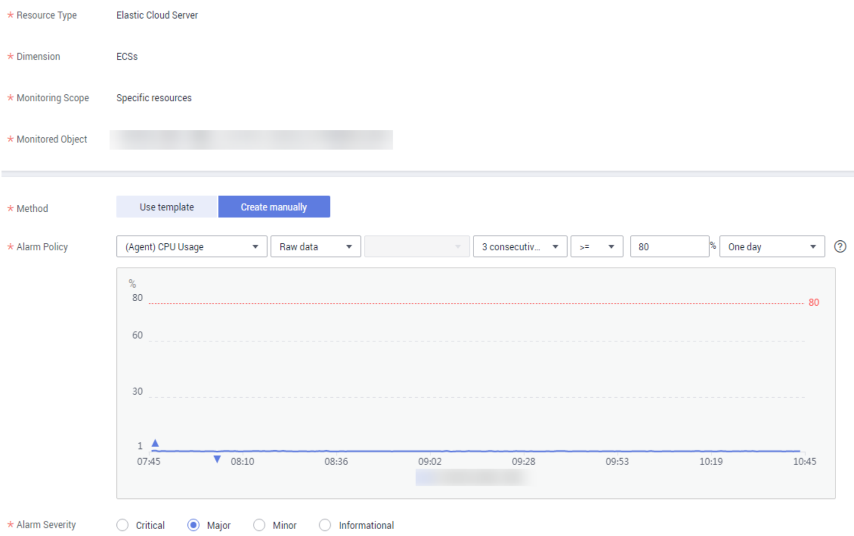


Table 4-15 Parameter description

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

Parameter	Description	Example Value
Threshold Type	For ECSs, you can select **Static** or **Dynamic**. The feature is only available in region CN South-Guangzhou. ● **Static**: Indicates the fixed value set in an alarm rule. If the fixed value is reached, an alarm is triggered. ● **Dynamic**: Indicates the predicative value range calculated based on historical data. If the current metric data deviates from the predicted value range, an alarm is triggered.	Static
Method	There are two options: **Use template** or **Create manually**.	Create manually
Template	Specifies the template to be used.	N/A
Alarm Policy	Specifies the policy for triggering an alarm. For example, an alarm is triggered if the average CPU usage of the monitored object is 80% or more for three consecutive 5-minute periods. Cloud Eye triggers an alarm every one hour again if the alarm persists. For details about basic and OS monitoring metrics, see **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.	N/A
Alarm Severity	Specifies the severity of the alarm. Valid values are **Critical**, **Major**, **Minor**, and **Informational**.	Major

c. Configure the alarm notification.

Figure 4-20 Alarm Notification

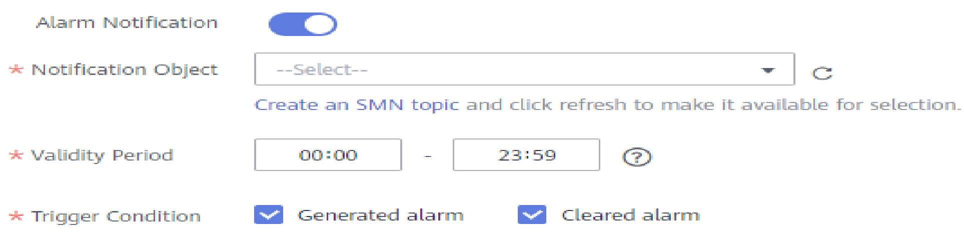


Table 4-16 Parameter description

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 that receives alarm notifications. You can select the account contact or a topic. ● **Account contact** is the mobile phone number and email address of the registered account. ● 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 **HTTP/HTTPS Messages**.
Validity Period	Cloud Eye sends notifications only within the validity period specified in the alarm rule. If **Validity Period** is set to **08:00-20:00**, Cloud Eye sends notifications only within 08:00-20:00.
Trigger Condition	Specifies the condition for triggering the alarm notification. You can select **Generated alarm** (when an alarm is generated), **Cleared alarm** (when an alarm is cleared), or both.

d. Click **Create**.

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

5 Custom Monitoring

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

Viewing Custom Monitoring

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

   NOTE

   - Only after you add monitoring data through APIs, will those data be displayed on the Cloud Eye console.
   - For details about how to add monitoring data, see **Adding Monitoring Data (RESTful API)**, **Adding Monitoring Data (Java SDK)**, and **Adding Monitoring Data (Python SDK)**.
4. Locate the row that contains the cloud service resource to be viewed, and click **View Metric**.

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

Creating an Alarm Rule

1. Log in to the management console.
2. Under **Management & Deployment**, 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 set the parameters. For details, see **Table 3-2** and **Table 3-4**.

6. Click **Create**.

6 Website Monitoring

6.1 Introduction to Website Monitoring

Scenarios

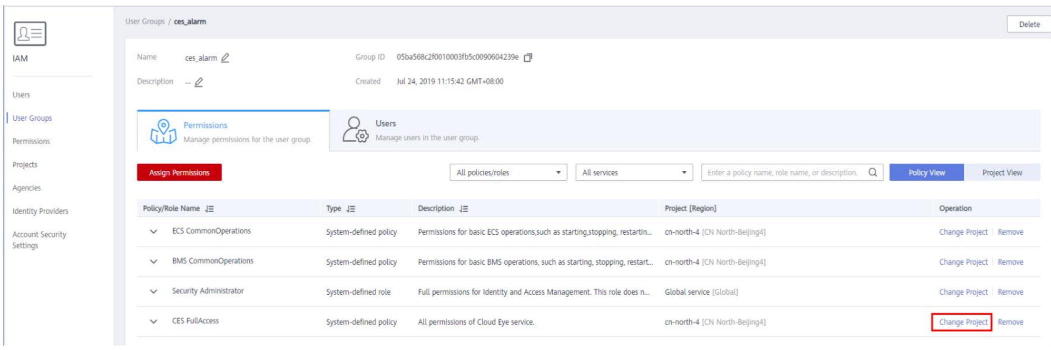
Website monitoring is used to simulate users' access to remote servers and continuously monitor the remote server status, such as availability and connectivity.

Checkpoint locations in North China (Langfang), East China (Shanghai), South China (Guangzhou), Southwest China (Guiyang), and South China (Shenzhen) are supported. More checkpoint locations will be available soon.

NOTE

- Website monitoring is free.
- The website monitoring function is available in the **CN North-Beijing1** region. If you want to use this function in other regions, the user group that you belong to must be assigned permissions for **cn-north-1 [CN North-Beijing1]** through IAM.

Figure 6-1 Change Object



Advantages

- You can create, modify, disable, enable, or delete monitors.

- The configuration is simple and quick, allowing you to improve efficiency and save resources that you would otherwise use to configure complex open source products.
- You receive notifications of website exceptions in real time.

Metrics

Table 6-1 Website monitoring metrics

Metric	Description
Response Time	The time taken by a website to respond to a request (from the time when the connection between the monitoring location and the website is established to the time when the monitoring location receives the first byte of the response message) Unit: ms
Availability	Availability data is collected hourly. The Availability graph can be viewed one hour after the creation of a monitor. Availability = (Number of the total detections per hour – Number of exception detections per hour)/Number of total detections per hour x 100%
Packet Loss Ratio	Ratio of the number of lost packets to the total number of packets transmitted
HTTP Response Code	Response status reported by the server
Available Monitoring Locations	Number of available monitoring locations
Available Monitoring Location Percentage	Percentage of available monitoring locations Available Monitoring Location Percentage = Number of available monitoring locations/Number of all monitoring locations x 100%

NOTE

- **Response Time**, **Availability**, **Available Monitoring Locations**, and **Available Monitoring Location Percentage** are applicable to HTTP(S), Transmission Control Protocol (TCP), User data protocol (UDP), and Packet Internet Groper (PING). **Packet Loss Ratio** applies only to PING. **HTTP Response Code** applies only to HTTP(S).
- Standard network protocols, such as Post Office Protocol version 3 (POP3), Simple Mail Transfer Protocol (SMTP), Domain Name System (DNS), and File Transfer Protocol (FTP), will be supported later to detect Internet service availability.

Protocols Supported

Table 6-2 Protocol description

Protocol	Description
HTTP(S)	Used to perform HTTP(S) detection on the specified URL or IP address. Three request methods: GET, POST, and HEAD are supported. In **Advanced Settings**, you can specify **HTTP Request Header** and **Request Cookies** of the above request methods.
PING	Used to test connectivity to a specified URL.
TCP	Used to perform TCP detection on the specified port. In **Advanced Settings**, you can specify **TCP Request Content** and its response content can be matched.
UDP	Used to perform UDP detection on the specified port. In **Advanced Settings**, you can specify **UDP Request Content** and its response content can be matched.

6.2 Creating a Monitor

Scenarios

This topic describes how to create a monitor to monitor and analyze network quality and performance.

NOTE

An account can create a maximum of 20 monitors.

Procedure

1. Log in to the management console.
2. Under **Management & Deployment**, select **Cloud Eye**.
3. On the **Website Monitoring** page, click **Create Monitor** in the upper right corner.
4. (For initial configuration) Select the region where the website monitoring data is stored.

   NOTE

   You can change the region that stores your website monitoring data, including your alarm rules, graphs, and exported monitoring data.
5. In the displayed **Create Monitor** dialog box, set parameters as prompted.

Figure 6-2 Create Monitor

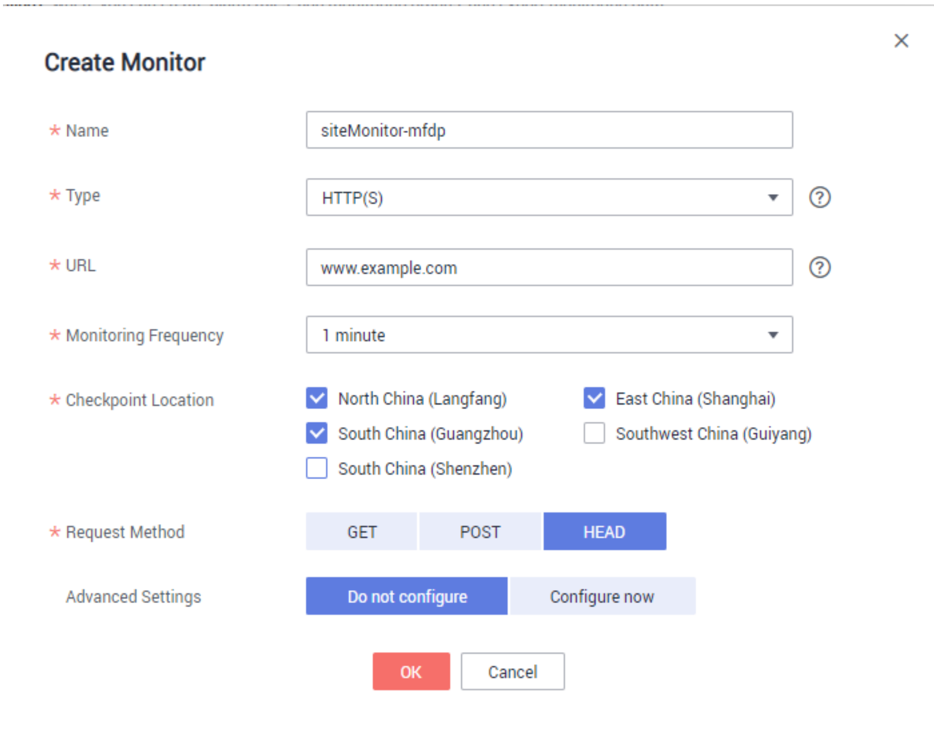


Table 6-3 Parameter description

Parameter	Description	Example Value
Name	Specifies the monitor name.	siteMonitor-mfdp
Type	Currently, the following protocols are supported: HTTP(S), PING, TCP, and UDP. More monitor types are being deployed.	HTTP(S)
URL	Specifies the address to be monitored. **NOTE** • To monitor an HTTPS website, enter the protocol header **https://**. • Website monitoring does not support IP addresses in the following private IP address segments: 10.0.0.0–10.255.255.255 172.16.0.0–172.31.255.255 192.168.0.0–192.168.255.255 127.0.0.0–127.255.255.255	www.example.com
Monitoring Frequency	Specifies the interval for the website monitoring detection engine to detect once. **NOTE** **Monitoring Frequency** can be set to **1 minute**, **5 minutes**, or **20 minutes**.	1 minute

Parameter	Description	Example Value
Checkpoint Location	Currently, website monitoring supports the following checkpoint locations: North China (Langfang), East China (Shanghai), South China (Guangzhou), Southwest China (Guiyang), and South China (Shenzhen).	North China (Langfang), East China (Shanghai), and South China (Guangzhou)
Request Method	This parameter is available when **Monitor Type** is set to **HTTP(S)**. Standard HTTP(S) request methods include GET, POST, and HEAD. The POST method can be used to submit content.	HEAD
Port Number	This parameter is available when **Monitor Type** is set to **TCP** or **UDP**.	8080
Advanced Settings	Different monitor types have different advanced settings. ● If **Type** is **HTTP(S)**, see **Table 6-4**. ● If **Monitor Type** is **TCP**, see **Table 6-5**. ● If **Monitor Type** is **UDP**, see **Table 6-6**.	N/A

Table 6-4 HTTP(S) advanced parameters

Parameter	Description	Example Value
HTTP Request Header	Specifies the HTTP header required to detect the target website. Each header must be on a separate line. **NOTE** If the submitted content is in the key=value format, the value of **HTTP Request Header** must be **Content-Type: application/x-www-form-urlencoded**.	key1=value1
Request Cookies	Specifies the cookie required to detect the target website. Each cookie must be on a separate line.	key1=value1
String Match	● Yes: If the response body contains the specified matched string, the detection succeeds. ● No: If the response body does not contain the specified matched string, the detection succeeds.	Yes
Matched String	Specifies the expected HTTP response content.	-

Table 6-5 TCP advanced parameters

Parameter	Description	Example Value
Request Content Format	The value can be in hexadecimal or text format.	Hexadecimal
TCP Request Content	Specifies the preset TCP request content.	0xcf
Matched String Format	The value can be in hexadecimal or text format.	Hexadecimal
Matched String	Specifies the expected TCP response content.	N/A

Table 6-6 UDP advanced parameters

Parameter	Description	Example Value
Request Content Format	The value can be in hexadecimal or text format.	Hexadecimal
UDP Request Content	Specifies the preset UDP request content.	0xcf
Matched String Format	The value can be in hexadecimal or text format.	Hexadecimal
Matched String	Specifies the expected UDP response content.	N/A

6. Click **OK**.

6.3 Creating an Alarm Rule for a Monitor

Scenarios

This topic describes how to create an alarm rule for a created monitor.

Prerequisites

A monitor has been created.

Procedure

1. Log in to the management console.
2. Under **Management & Deployment**, select **Cloud Eye**.
3. In the navigation pane on the left, choose **Website Monitoring**.
4. On the **Website Monitoring** page, locate the row that contains the target monitor. In the **Operation** column, click **Create Alarm Rule** under **More**.
5. On the **Create Alarm Rule** page, follow the prompts to set the parameters.
   a. Set the alarm rule name, description, and associated enterprise project.

Table 6-7 Parameters

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.
Enterprise Project	Specifies the enterprise project the alarm rule belongs to. Only users with the enterprise project permissions can view and manage the alarm rule.

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

Figure 6-3 Configuring the alarm content

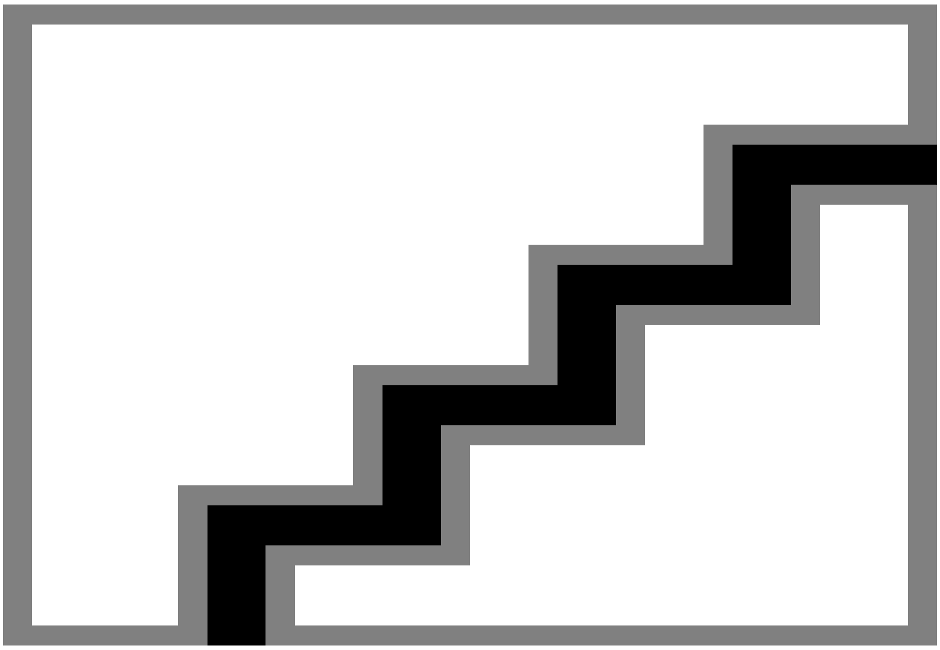


Table 6-8 Parameter description

Parameter	Description
Alarm Policy	Specifies the policy for triggering an alarm. For example, Cloud Eye triggers an alarm every one hour if availability is 90% or less for three consecutive periods. That is, if the alarm is not cleared after it is generated, an alarm notification is sent, once every hour.
Checkpoint Location	Checkpoint locations in North China (Langfang), East China (Shanghai), and South China (Guangzhou) are supported. If **Metric** is set to **Availability**, **Packet Loss Ratio**, **Response Time**, or **HTTP Response Code**, one or more checkpoint locations can be selected.
Alarm Severity	Specifies the alarm severity. Valid values are **Critical**, **Major**, **Minor**, and **Informational**.

NOTE

For parameters that are not mentioned in **Table 6-8**, retain their default values.

c. Set **Alarm Notification** parameters.

Figure 6-4 Alarm Notification

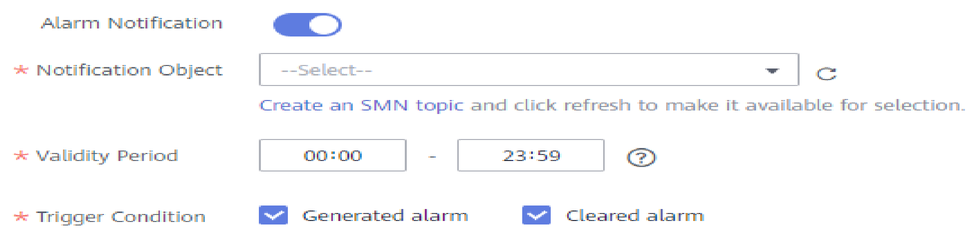


Table 6-9 Parameter description

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.

Parameter	Description
Notification Object	Specifies the object that receives alarm notifications. You can select the account contact or a topic. ● **Account contact** is the mobile phone number and email address of the registered account. ● 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**.
Validity Period	Cloud Eye sends notifications only within the validity period specified in the alarm rule. If **Validity Period** is set to **08:00-20:00**, Cloud Eye sends notifications only within 08:00-20:00.
Trigger Condition	Specifies the condition for triggering the alarm notification. You can select **Generated alarm** (when an alarm is generated), **Cleared alarm** (when an alarm is cleared), or both.

d. Click **Create**.

When the monitored website is abnormal (for example, the availability is 90% or less), Cloud Eye notifies you of the exception immediately to avoid service loss.

6.4 Viewing Website Monitoring Data

Scenarios

This topic describes how to view the website monitoring data, including availability, response time, and available monitoring location, to understand the website access.

Procedure

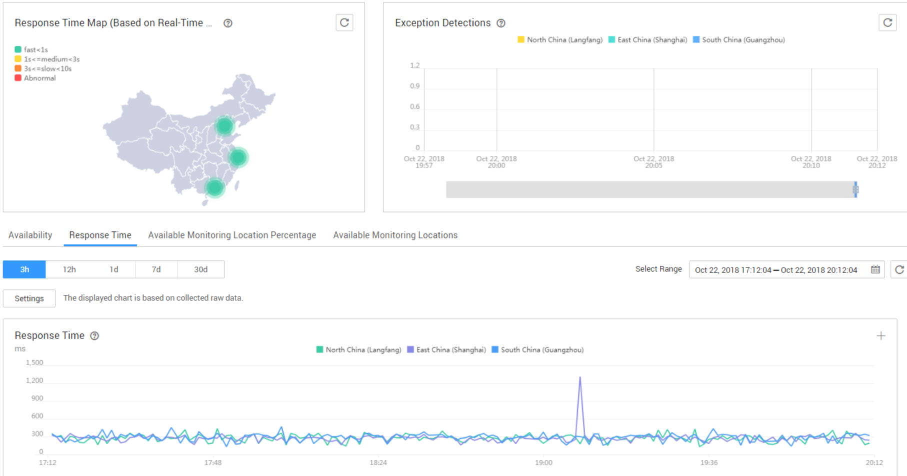
1. Log in to the management console.
2. Under **Management & Deployment**, select **Cloud Eye**.
3. In the navigation pane on the left, choose **Website Monitoring**.

   The overview of all monitors is displayed on the **Website Monitoring** page.

   You can check the name, URL, type, monitoring frequency, available monitoring location percentage, and average response time.
4. Locate the row containing the target monitor, and click **View Graph** in the **Operation** column.

   The monitoring graphs page is displayed. On the displayed page, you can view the original monitoring data curves of the monitor in the last 3 hours, last 12 hours, and last 24 hours.

Figure 6-5 Viewing graphs



NOTE

- If the metric is Availability, the average value in an hour is displayed in the monitoring graph.
- If the rollup period of Availability is longer than one hour, its data averaged based on the rollup period is displayed.

6.5 Managing Monitors

Scenarios

This topic describes how to modify, disable, enable, or delete monitors when services change or the alarm rules configured for website monitoring do not meet your service requirements.

Modifying a Monitor

1. Log in to the management console.
2. Under **Management & Deployment**, select **Cloud Eye**.
3. In the navigation pane on the left, choose **Website Monitoring**.
4. Locate the row containing the target monitor. In the **Operation** column, click **More**, and choose **Modify Monitor**.

   The **Modify Monitor** dialog box is displayed.
5. Configure the parameters based on **Table 6-3**.

   NOTE

   Values of **Monitor Type** and **URL** cannot be changed. Data may be lost after the change because advanced settings of different monitor types are different.

Disabling a Monitor

On the **Website Monitoring** page, locate the row that contains the target monitor. In the **Operation** column, click **Disable Monitor** under **More**. In the displayed **Disable Monitor** dialog box, click **Yes**.

Enabling a Monitor

On the **Website Monitoring** page, locate the row that contains the target monitor. In the **Operation** column, click **Enable Monitor** under **More**. In the displayed **Enable Monitor** dialog box, click **Yes**.

Deleting a Monitor

On the **Website Monitoring** page, locate the row that contains the target monitor. In the **Operation** column, click **Delete Monitor** under **More**. In the displayed **Delete Monitor** dialog box, click **Yes**.

7 Log Monitoring

7.1 Introduction to Log Monitoring

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

NOTE

Log monitoring is only launched in the CN North-Beijing1, CN East-Shanghai2, and CN South-Guangzhou regions.

7.2 Specifying a Custom Metric Filter

LTS extracts specified keywords from logs, so that you can use Cloud Eye to monitor key metrics in logs.

Prerequisites

- LTS has been used, a filter has been created in LTS, and the log monitoring data can be viewed.
- A log group and a log topic have been created. For details, see **Creating a Log Group** and **Creating a Log Topic**.
- You have interconnected with resources and configured log collection setting. For details, see **Configuring Log Collection Settings**.

Procedure

1. Log in to the management console. Under **Management & Deployment**, select **Log Tank Service**.
2. In the navigation pane on the left, choose **Log Management**.
3. In the log group list, click the name of the target log group.

   The log topic list page is displayed.

4. In the **Operation** column, click **More** and choose **Create Custom Counter Filter**.

   Set the parameters based on **Table 7-1**.

Table 7-1 Custom metric filter parameters

Parameter	Description
Filter Name	Specifies the name of the filter you set.
Filter Keyword	Specifies the specified keywords extracted from the log, for example, **Error**. ● Only filtering by a single keyword is supported. ● Filtering is case-sensitive and only logs meeting a certain condition can be filtered, such as Error or Warning.
Example Log	You are advised to paste a complete log to match the filter keywords.
Metric Name	You are advised to specify the metric name for each filter keyword. Example: **Error_metric**

5. Click **OK**.

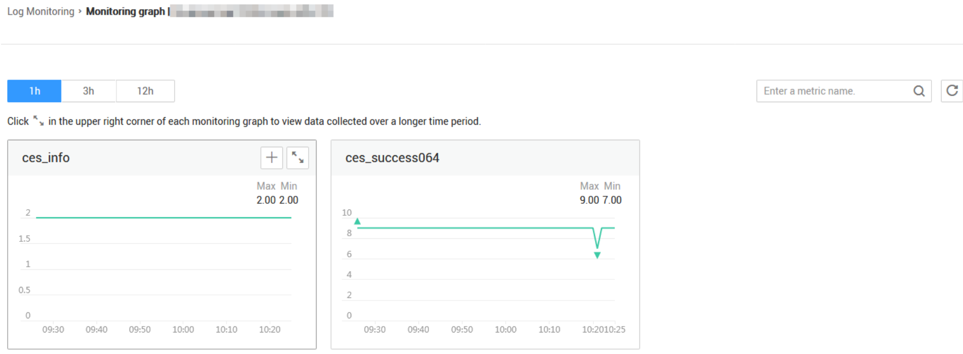
7.3 Viewing Log Monitoring Data

Procedure

1. Log in to the management console.
2. Under **Management & Deployment**, select **Cloud Eye**.
3. In the navigation pane on the left, choose **Log Monitoring**.
4. Locate the row containing the target log group, and click **View Metric** in the **Operation** column.

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

Figure 7-1 Viewing graphs



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.

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. For details, see **Events Supported by Event Monitoring**.

Event monitoring is enabled by default.

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. Under **Management & Deployment**, select **Cloud Eye**.
3. In the navigation pane on the left, choose **Event Monitoring**.

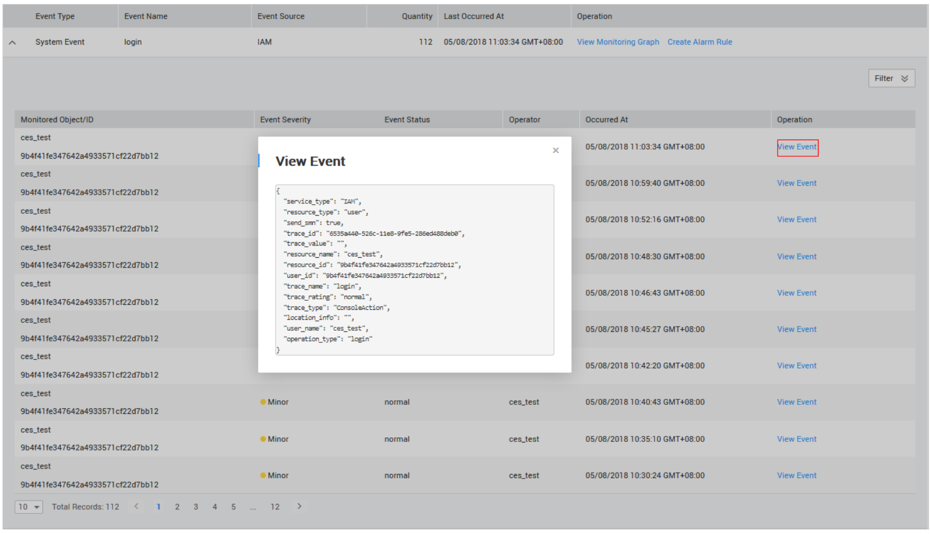
   On the displayed **Event Monitoring** page, all system events generated in the last 24 hours are displayed by default.

   You can also click **1h**, **3h**, **12h**, **1d**, **7d**, or **30d** to view 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 View Event



8.3 Creating an Alarm Rule to Monitor an Event

Scenarios

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

Procedure

1. Log in to the management console.
2. Under **Management & Deployment**, 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, set the parameters.
   a. Set the alarm rule name and description.

Table 8-1 Parameter description

Parameter	Description
Name	Specifies the alarm rule name. The system generates a random name, which you can modify.
Description	(Optional) Provides supplementary information about the alarm rule.
Enterprise Project	Specifies the enterprise project the alarm rule belongs to. Only users with the enterprise project permissions can view and manage the alarm rule.

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

Figure 8-3 Configuring parameters

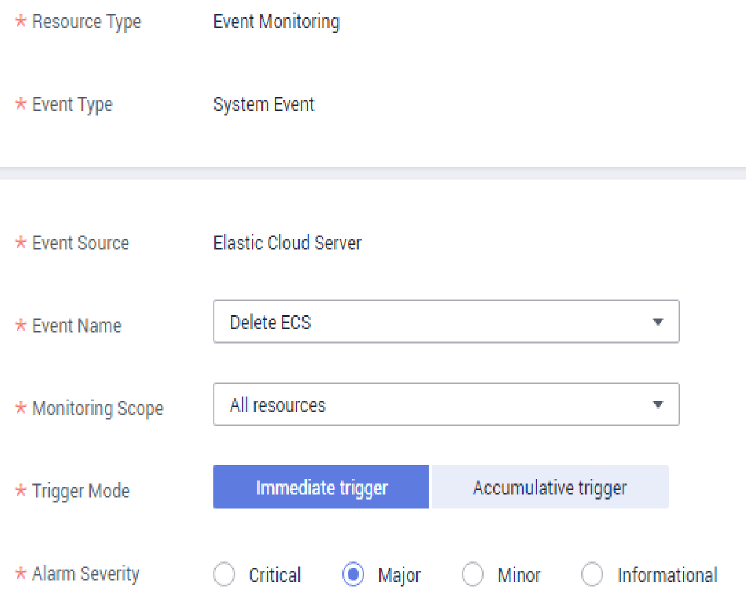


Table 8-2 Parameter description

Parameter	Description
Resource Type	Specifies the type of the resource the alarm rule is created for.
Dimension	Specifies the metric dimension of the selected resource type. Example value: **System event**

Parameter	Description
Method	Specifies the means you use to create the alarm rule.
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**.
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**
Monitoring Scope	Specifies the monitoring scope for event monitoring. Example value: **All resources**
Monitored Object	Specifies the object to be monitored. This parameter is mandatory if you set **Monitoring Scope** to **Specific resources**.
Trigger Mode	You can select immediate trigger or accumulative trigger based on the operation severity. Example value: **Immediate trigger**
Alarm Severity	Specifies the alarm severity. Valid values are **Critical**, **Major**, **Minor**, and **Informational**. Example value: **Major**

c. Set **Alarm Notification** parameters.

Figure 8-4 Alarm Notification

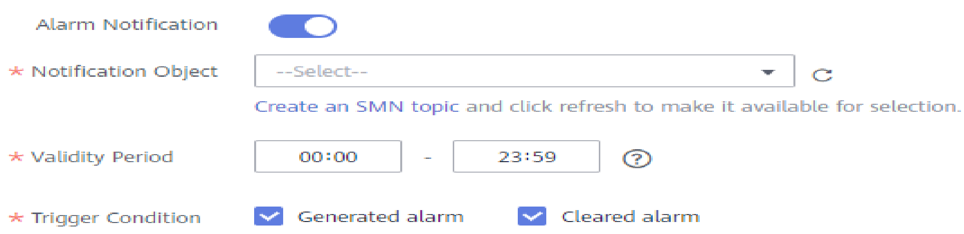


Table 8-3 Parameter description

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.

Parameter	Description
Notification Object	Specifies the object that receives alarm notifications. You can select the account contact or a topic. ● **Account contact** is the mobile phone number and email address of the registered account. ● 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**.
Validity Period	Cloud Eye sends notifications only within the validity period specified in the alarm rule. If **Validity Period** is set to **08:00-20:00**, Cloud Eye sends notifications only within 08:00-20:00.
Trigger Condition	Specifies the condition for triggering the alarm notification. You can select **Generated alarm** (when an alarm is generated), **Cleared alarm** (when an alarm is cleared), or both.

d. Click **Create**.

8.4 Events Supported by Event Monitoring

Table 8-4 ECS

Event Source	Event Name	Event Severity	Description	Solution	Impact
ECS	Start auto recovery	Major	If a host is faulty, ECSs on the host will be automatically migrated to another properly-running host. During the migration, the ECSs will be restarted.	Wait for the event to end and check whether services are affected.	Services may be interrupted.

Event Source	Event Name	Event Severity	Description	Solution	Impact
	Stop auto recovery	Major	After the automatic migration is complete, the ECS will be restored.	This event indicates that the ECS has restored to normal and is working properly.	No impact.
	Auto recovery timeout (being processed on the backend)	Major	The operation of migrating the ECS to a normal host times out.	Migrate services to other ECSs.	Services are interrupted.
	GPU link fault	Critical	The GPU of the host running the ECS is faulty or is 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	Critical	The FPGA of the host running the ECS is faulty or is 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 Severity	Description	Solution	Impact
	Improper ECS running	Major	The ECS is faulty, or the NIC is abnormal, causing the ECS to run abnormally.	Deploy service applications in HA mode. After the fault is rectified, check whether services recover.	Services are interrupted.
	Improper ECS running recovered	Major	The ECS has restored to the normal status.	Wait for the ECS status to become normal and check whether services are affected.	No impact.
	Delete ECS	Major	The ECS is deleted ● on the management console ● by calling APIs	Check whether the deletion was performed intentionally by a user.	Services are interrupted.

Event Source	Event Name	Event Severity	Description	Solution	Impact
	Reboot ECS	Minor	The ECS is 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.
	Stop ECS	Minor	The ECS is stopped ● on the management console ● by calling APIs	● Check whether the stop operation was performed intentionally by a user. ● Deploy service applications in HA mode. ● After the ECS is started, check whether services recover.	Services are interrupted.

Event Source	Event Name	Event Severity	Description	Solution	Impact
	Delete NIC	Major	The ECS NIC is 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 Severity	Description	Solution	Impact
	Modify ECS specifications	Minor	The ECS specifications have been modified • on the management console • by calling APIs	• Check whether the operation is performed by a user. • Deploy service applications in HA mode. • After the specifications are modified, check whether services have recovered.	Services are interrupted.

NOTE

Once a physical host running ECSs breaks down, the ECSs automatically migrate to a functional physical host. The ECSs will restart during the migration.

Table 8-5 BMS

Event Source	Event Name	Event Severity	Description	Solution	Impact
BMS	Reboot BMS	Major	The BMS is 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.
	Unexpected restart	Major	The BMS restarts unexpectedly, which may be caused by ● OS fault ● Hardware fault	● Deploy service applications in HA mode. ● After the BMS is restarted, check whether services recover.	Services are interrupted.
	Stop BMS	Major	The BMS is stopped ● on the management console ● by calling APIs	● Deploy service applications in HA mode. ● After the BMS is started, check whether services recover.	Services are interrupted.
	Unexpected shutdown	Major	The BMS stops unexpectedly, which may be caused by ● unexpected power-off ● hardware fault	● Deploy service applications in HA mode. ● After the BMS is started, check whether services recover.	Services are interrupted.

Event Source	Event Name	Event Severity	Description	Solution	Impact
	Network interruption	Major	The BMS network is interrupted, which may because ● The BMS is unexpectedly stopped or restarted. ● The switch is faulty. ● The gateway is faulty.	● Deploy service applications in HA mode. ● After the BMS is started, check whether services recover.	Services are interrupted.
	PCIe error	Major	The PCIe device or main board on the BMS is faulty.	● Deploy service applications in HA mode. ● After the BMS is recovered, check whether services recover.	The network or disk read/write services are affected.
	Disk fault	Major	The disk backplane or the disk on the BMS is 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.

Event Source	Event Name	Event Severity	Description	Solution	Impact
	EVS error	Major	The BMS fails to connect to the EVS disk, which may because ● The SDI interface is faulty. ● The remote storage device is 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.

Table 8-6 EIP

Event Source	Event Name	Event Severity	Description	Solution	Impact
EIP	EIP bandwidth overflow	Major	The required bandwidth exceeds the purchased bandwidth, which may slow down the network or cause packet loss. **NOTE** EIP bandwidth overflow is only launched in the CN North-Beijing1, CN East-Shanghai1, CN East-Shanghai2, and CN South-Guangzhou regions.	Check whether the EIP bandwidth keeps increasing and whether services are normal. Expand capacity if necessary.	The network becomes slow or packets are lost.
	Release EIP	Minor	The EIP is deleted.	Check whether the resource is deleted by mistake.	The server cannot access the Internet.

Event Source	Event Name	Event Severity	Description	Solution	Impact
	EIP blocked	Critical	If the required bandwidth exceeds 5 GB, packets will be discarded. It 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	Critical	The EIP has been unblocked.	Use the original EIP again.	No impact.

Table 8-7 CBR

Event Source	Event Name	Event Severity	Description	Solution	Impact
CBR	Backup failed	Critical	Failed to create the backup.	Manually create a backup or contact customer service.	Data loss may occur.
	Restoration failed	Critical	Failed to restore the resource using a backup.	Use other backups to restore the resource or contact customer service.	Data loss may occur.
	Backup deletion failed	Critical	Failed to delete the backup.	Try again later or contact customer service.	Charging may be abnormal.
	Vault deletion failed	Critical	Failed to delete the vault.	Try again later or contact customer service.	Charging may be abnormal.

Event Source	Event Name	Event Severity	Description	Solution	Impact
	Replication failed	Critical	Failed to replicate the backup.	Try again later or contact customer service.	Data loss may occur.
	Backup succeeded	Major	The backup is created successfully.	None	No impact.
	Restoration succeeded	Major	Resource restoration using a backup succeeded.	Check whether the data is successfully restored.	No impact.
	Backup deletion succeeded	Major	The backup is deleted successfully.	None	No impact.
	Vault deletion succeeded	Major	The vault is deleted successfully.	None	No impact.
	Replication succeeded	Major	The backup is replicated successfully.	None	No impact.

Table 8-8 RDS — resource exception

Event Source	Event Name	Event Severity	Description	Solution	Impact
RDS	DB instance creation failure	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.

Event Source	Event Name	Event Severity	Description	Solution	Impact
	Full backup failure	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.
	Primary/secondary switchover failure	Major	The standby DB instance does not take over services from the primary DB instance due to network or server failures. The original primary DB instance continues to provide services within a short time.	Check whether the connection between the application and the database is re-established.	No impact.

Event Source	Event Name	Event Severity	Description	Solution	Impact
	Abnormal replication status	Major	The possible causes are as follows: 1. The replication delay between the primary and standby DB instances is too long (usually occurs when a large amount of data is written to databases or a large transaction is performed). During peak hours, data may be blocked. 2. The network between the primary and secondary DB instances is disconnected.	Submit a service ticket.	This event does not interrupt data read and write of the DB instance, and your applications are not affected.
	Replication status recovered	Major	The replication delay between the primary and standby DB instances is within the normal range, or the network connection between them has restored.	No action is required.	No impact.
	Faulty DB instance	Major	A single or primary DB instance is faulty due to a disaster or a server failure.	Check whether an automatic backup policy has been configured for the DB instance and submit a service ticket.	The database service may be unavailable.

Event Source	Event Name	Event Severity	Description	Solution	Impact
	DB instance recovered	Major	RDS uses high availability tools to rebuild the standby DB instance for disaster recovery. After the recovery, this event will be reported.	No action is required.	No impact.
	Changing to primary/ secondary DB instances failure	Major	A fault occurs when you create the standby DB instance or configure synchronization between the primary and standby DN instances. The fault may because resources are insufficient in the data center where the standby DB instance is located.	Submit a service ticket.	This event does not interrupt data read and write of the DB instance, and your applications are not affected.

Table 8-9 RDS — operations

Event Source	Event Name	Event Severity
RDS	Reset administrator password	Major
	Operate DB instance	Major
	Delete DB instance	Minor
	Modify backup policy	Minor
	Change parameter group	Minor
	Delete parameter group	Minor

Event Source	Event Name	Event Severity
	Reset parameter group	Minor
	Change database port	Major

Table 8-10 DDS

Event Source	Event Name	Event Severity	Description	Solution	Impact
DDS	DB instance creation failure	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.

Event Source	Event Name	Event Severity	Description	Solution	Impact
	Abnormal replication status	Major	The possible causes are as follows: 1. The replication delay between the primary and standby DB instances is too long (usually occurs when a large amount of data is written to databases or a large transaction is performed). During off-peak hours, the replication delay between the primary and standby DB instances gradually decreases. 2. The network between the primary and secondary DB instances is disconnected.	Submit a service ticket.	This event does not interrupt data read and write of the DB instance, and your applications are not affected.
	Replication status recovered	Major	The replication delay between the primary and standby DB instances is within the normal range, or the network connection between them has restored.	No action is required.	No impact.

Event Source	Event Name	Event Severity	Description	Solution	Impact
	Faulty DB instance	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	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.	No impact.
	Faulty node	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	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.	No impact.
	Primary/ standby switchover or failover	Major	This event is reported when a primary/standby switchover or a failover is triggered.	No action is required.	No impact.

Table 8-11 GaussDB NoSQL

Event Source	Event Name	Event Severity	Description	Solution	Impact
NoSQL	Failed to create a DB instance	Major	The DB 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 upper limit.	DB instances cannot be created.
	Failed to modify the specifications	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.
	Failed to add a node	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 fails to be added and add a new node.	No impact.
	Failed to delete a node	Major	The underlying resources fail to be released.	Delete the node again.	No impact.

Event Source	Event Name	Event Severity	Description	Solution	Impact
	Failed to scale up the storage space	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.
	Failed to reset the password	Major	Resetting the password times out.	Reset the password again.	No impact.
	Failed to modify a parameter group	Major	Modifying a parameter group times out.	Modify the parameter group again.	No impact.
	Failed to set the backup policy	Major	The database connection is abnormal.	Set the backup policy again.	No impact.
	Failed to create a manual backup	Major	The backup files fail to be exported or uploaded.	Submit a service ticket to the O&M personnel.	Data cannot be backed up.
	Failed to create an automated backup	Major	The backup files fail to be exported or uploaded.	Submit a service ticket to the O&M personnel.	Data cannot be backed up.
	Faulty DB instance	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.

Event Source	Event Name	Event Severity	Description	Solution	Impact
	DB instance recovered	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.	No impact.
	Faulty node	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	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.	No impact.
	Primary/ standby switchover or failover	Major	This event is reported when a primary/standby switchover or a failover is triggered.	No action is required.	No impact.

Event Source	Event Name	Event Severity	Description	Solution	Impact
	HotKeyOccurs	Major	Objectively, the primary key is improperly set. As a result, hotspot data is distributed in one partition. The improper application design, which 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 firstly.	The service request success rate is affected, and the cluster performance and stability also be affected.
	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.

Table 8-12 GaussDB(for MySQL)

Event Source	Event Name	Event Severity	Description	Solution	Impact
GaussDB (for MySQL)	Failed to create a DB instance	Major	DB instances fail to be created because the quota is insufficient or underlying resources are exhausted.	Check the DB instance quota. Release resources and create DB instances again.	DB instances cannot be created.

Event Source	Event Name	Event Severity	Description	Solution	Impact
	Read replica promotion failure	Major	The read replica fails to be promoted to the primary DB instance due to network or server failures. The original primary DB instance takes over services within a short time.	Submit a service ticket.	The read replica fails to be promoted to the primary DB instance.
	Read replica creation failure	Major	Read replicas fail to be created because the quota is insufficient or underlying resources are exhausted.	Check the read replica quota. Release resources and create DB instances again.	Read replicas fail to be created.
	Instance class change failure	Major	DB instance classes fail to be changed because the quota is insufficient or underlying resources are exhausted.	Submit a service ticket.	DB instance classes fail to be changed.

Table 8-13 GaussDB(for openGauss)

Event Source	Event Name	Event Severity	Description	Solution	Impact
GaussDB (for openGauss)	Process Status Alarm	Major	Key processes exit, including: CMS/CMA, ETCD, GTM, CN or DN process.	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.
	Component Status Alarm	Major	Key components do not respond, including: CMA, ETCD, GTM, CN or 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.

Event Source	Event Name	Event Severity	Description	Solution	Impact
	Cluster Status Alarm	Major	The cluster is abnormal, such as: The cluster is read-only. Majority of ETCDs are faulty. The cluster resources are unevenly distributed.	Contact SRE engineers.	If the cluster is read-only, only read-only requests are processed. If the majority of ETCDs are fault, the cluster is unavailable. If the cluster resources are unevenly distributed, the cluster performance and reliability deteriorate.
	Hardware Resource Alarm	Major	A major hardware fault occurs in the cluster, such as: A disk is damaged, causing the GTM network communication fault.	Contact SRE engineers.	Some or all services are affected.
	Status Transition Alarm	Major	The following events occur in the cluster: DN build failed. Forcible DN promotion. Primary/ standby DN switchover/ failover 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.

Event Source	Event Name	Event Severity	Description	Solution	Impact
	Other Abnormal Alarm	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.

Table 8-14 VPC

Event Source	Event Name	Event Severity
VPC	Delete VPC	Major
	Modify VPC	Minor
	Delete subnet	Minor
	Modify subnet	Minor
	Modify bandwidth	Minor
	Delete VPN	Major
	Modify VPN	Minor

Table 8-15 EVS

Event Source	Event Name	Event Severity
EVS	Update disk	Minor
	Expand disk	Minor
	Delete disk	Major

Table 8-16 IAM

Event Source	Event Name	Event Severity
IAM	Login	Minor
	Logout	Minor
	Change password	Major

Event Source	Event Name	Event Severity
	Create user	Minor
	Delete user	Major
	Update user	Minor
	Create user group	Minor
	Delete user group	Major
	Update user group	Minor
	Create identity provider	Minor
	Delete identity provider	Major
	Update identity provider	Minor
	Update metadata	Minor
	Update security policy	Major
	Add credential	Major
	Delete credential	Major
	Create project	Minor
	Update project	Minor
	Suspend project	Major

Table 8-17 KMS

Event Source	Event Name	Event Severity
KMS	Disable key	Major
	Schedule key deletion	Minor
	Retire grant	Major
	Revoke grant	Major

Table 8-18 OBS

Event Source	Event Name	Event Severity
OBS	Delete bucket	Major
	Delete bucket policy	Major

Event Source	Event Name	Event Severity
	Set bucket ACL	Minor
	Set bucket policy	Minor

9 Viewing Alarm History

9.1 Configuring OBS Data Storage

Scenarios

On Cloud Eye, the raw data retention period for each metric is two days. Raw data with a retention period of more than two days will not be saved. After enabling Object Storage Service (OBS), you can save raw data for a longer period of time by synchronizing them to OBS.

This topic describes how to configure data storage.

Prerequisites

- A cloud service is enabled.
- OBS has been enabled.

Procedure

1. Log in to the management console.
2. Under **Management & Deployment**, select **Cloud Eye**.
3. In the navigation pane on the left, choose **Cloud Service Monitoring**. Locate the target resource and click **Configure Data Storage** in the **Operation** column.

   Alternatively, in the navigation pane on the left, choose **Server Monitoring**. Locate the target ECS. In the **Operation** column, click **Configure Data Storage**.
4. (Optional) Configure data storage in batches.

   On the **Cloud Service Monitoring** page, select the target cloud service resources and click **Configure Data Storage**.

   Alternatively, on the **Server Monitoring** page, select the target ECSs and click **Configure Data Storage**.
5. In the displayed **Configure Data Storage** window, set parameters based on **Table 9-1**:

Table 9-1 Parameters for **Configure Data Storage**

Parameter	Description	Example Value
Transfer Trace to OBS	Specifies whether to transfer trace to OBS. Its value can be **Configure** or **Not required**.	Configure
Create OBS Bucket	If an OBS bucket exists, you do not need to create another buckets.	Yes
OBS Bucket for Storing Traces	If there is no OBS bucket, enter the name of the OBS bucket to be created. If there are OBS buckets, select one.	ecs-0615
File Prefix	The metric data file prefix enables you to distinguish Cloud Eye data files from other files in the OBS bucket.	ecs-0615

NOTE

- OBS will grant read and write permissions to Cloud Eye for the selected bucket. Exercise caution when modifying the bucket policy to prevent data transfer failures.
- For security purposes, set **Storage Class** to **Standard** and **Bucket Policy** to **Private**.
- If the configured dump policy is disabled for more than 7 days, it will be cleared by default. If you need to use the dump policy, reconfigure it.
- If the user account is frozen for more than two hours, the function of transferring data to OBS is disabled. If you want to use this function, unfreeze the account and enable the function again.

6. Click **OK**.

   After the configuration, the system automatically dumps monitoring data to the OBS bucket every two hours, for example, 00:00 and 02:00.

9.2 Viewing Raw Data

Scenarios

This topic describes how to view the monitoring data saved in the OBS bucket by downloading metric data files.

Prerequisites

- You have successfully configured data storage on Cloud Eye. For details, see **Configuring OBS Data Storage**.
- You have installed Java and configured environment variables.

- You have downloaded the format conversion tool metric-transfer-merge.jar from the download address **https://metric-json-trans-csv.obs.myhuaweicloud.com/metric-transfer-merge.jar**.

Procedure

1. Log in to the management console.
2. Under **Management & Deployment**, select **Cloud Eye**.
3. In the navigation pane on the left, choose **Cloud Service Monitoring**. Locate the target resource and select the specified OBS bucket in the **Permanent Data Storage** column.

   Alternatively, in the navigation pane on the left, choose **Server Monitoring**. Locate the target ECS, and select the specified OBS bucket in the **Permanent Data Storage** column.
4. Select the metric data file you want to view in the OBS bucket. Based on the storage path of the metric data file, select *OBS bucket name* > *CloudEye* > *Region* > *Year* > *Month* > *Day* > *Service type directory* > *Resource type directory*. Click **Download** in the **Operation** column to download the file to the default path. To download the metric data file to a customized path, click **Download As**.

   The metric data file is named in the following format:

   *Metric data file prefix*_CloudEye_*Region*_*Time when the log was uploaded to the OBS: year-month-day*T*hour-minute-second*Z_*Randomly generated character*.json.gz

   Example: *File Prefix*_CloudEye_region_2016-05-30T16-20-56Z_21d36ced8c8af71e.json

   NOTE

   - The OBS bucket name and trace file prefix are user-defined, and other parameters are automatically generated.
   - Original metric data files are segment files of time granularity. The files include all metric data of a resource under the time segment. The metric data is stored in the JSON format.
   - To facilitate your operations, Cloud Eye provides the format conversion and content combination tool. Using this tool, you can combine the files of several time slices in a specific resource into a time-staged file in the chronological order in the .csv format. In addition, you can use the tool to generate an independent time splice file for every metric of the resource in the .csv format.
5. Access the cmd tool in the Windows system. Go to the folder where **metric-transfer-merge.jar** is located, run the **java -jar metric-transfer-merge.jar j2c inputDirectory outputDirectory mergFileName** command.

   In the Linux system, run the **java-jar metric-transfer-merge.jar inputDirectory outputDirectory mergFileName** command in the shell command line.

NOTE

- **j2c** is the command to convert JSON into CSV.
- **inputDirectory** is the directory to store the downloaded JSON files.
- **outputDirectory** is the directory to store the generated files.
- **mergFileName** is the name of the specified combined file for users. This parameter can be ignored because the tool will name the combined file as **mergeResult.csv** by default.

After running the java command, you can view the converted files in the **outputDirectory** directory. Each file corresponds to the data of one metric at all time points. **mergeResult.csv** is a large file generated by combining the data of all metrics. **Figure 9-1** shows the content of the converted file.

Figure 9-1 Metric data

```
Timestamp,Time,VPC.Upstream Bandwidth.Bandwidth:c36e6dd0-ddab-4658-a4f4-48c3e0d14743-(Byte/s)
1511272645257,2017-11-21 21:57:25,0.0
1511272705257,2017-11-21 21:58:25,0.0
1511272765257,2017-11-21 21:59:25,0.0
1511272825257,2017-11-21 22:00:25,0.0
1511272885259,2017-11-21 22:01:25,0.0
1511272945258,2017-11-21 22:02:25,0.0
1511273005257,2017-11-21 22:03:25,0.0
1511273065257,2017-11-21 22:04:25,0.0
1511273125257,2017-11-21 22:05:25,0.0
1511273185257,2017-11-21 22:06:25,0.0
1511273245257,2017-11-21 22:07:25,0.0
1511273305257,2017-11-21 22:08:25,0.0
1511273365257,2017-11-21 22:09:25,0.0
1511273425258,2017-11-21 22:10:25,0.0
1511273485257,2017-11-21 22:11:25,0.0
1511273545257,2017-11-21 22:12:25,0.0
1511273605257,2017-11-21 22:13:25,0.0
1511273665257,2017-11-21 22:14:25,0.0
1511273725257,2017-11-21 22:15:25,0.0
1511273785257,2017-11-21 22:16:25,0.0
1511273845259,2017-11-21 22:17:25,0.0
1511273905258,2017-11-21 22:18:25,0.0
1511273965257,2017-11-21 22:19:25,0.0
1511274025257,2017-11-21 22:20:25,0.0
1511274085257,2017-11-21 22:21:25,0.0
1511274145257,2017-11-21 22:22:25,0.0
1511274205257,2017-11-21 22:23:25,0.0
1511274265257,2017-11-21 22:24:25,0.0
```

10 Auditing Operation Records on Cloud Eye

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

10.1 Key Cloud Eye Operations

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

Operation	Resource Type	Event 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	Event Name
Creating a monitoring panel	dashboard	createDashboard
Deleting a monitoring panel	dashboard	deleteDashboard
Modifying a monitoring panel	dashboard	updateDashboard
Adding monitoring data	metric	addMetricData
Exporting monitoring data	metric	downloadMetricsReport
Configuring OBS dump	obs_transfer	createObsTransfer
Modifying OBS dump	obs_transfer	updateObsTransfer
Configuring OBS dump in batches	obs_transfer	batchCreateObsTransfer
Creating a monitor	remote_check	createRemoteMonitoring-Rules
Deleting a monitor	remote_check	deleteRemoteMonitoring-Rules
Modifying a monitor	remote_check	updateRemoteMonitoring-Rule
Enabling or disabling one-click monitoring	one_click_alarm	updateOneClickAlarm

10.2 Viewing Cloud Eye Logs

Scenarios

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

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

Procedure

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

– **Trace Source**, **Resource Type**, and **Search By**

  Select a filter from the drop-down list.

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

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

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

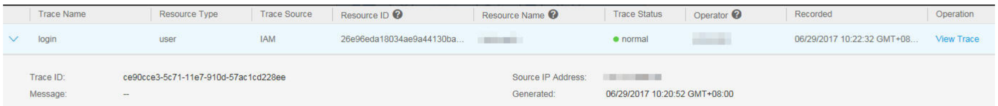
– **Operator**: Select a specific operator.

– **Trace Status**: Select one of **All trace statuses**, **Normal**, **Warning**, and **Incident**.

– Time range: You can select start and end time to query traces generated during a time range of the last seven days.

6. Click  on the left of a trace to expand its details.

Figure 10-1 Expanding trace details



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

Figure 10-2 View Trace

11 Permissions Management

11.1 Creating a User and Granting Permissions

This topic describes how to use **IAM** to implement fine-grained permissions control for your Cloud Eye resources. With IAM, you can:

- 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 only the permissions required for users to perform a special task.
- Entrust a HUAWEI CLOUD account or cloud service to perform efficient O&M on your Cloud Eye resources.

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

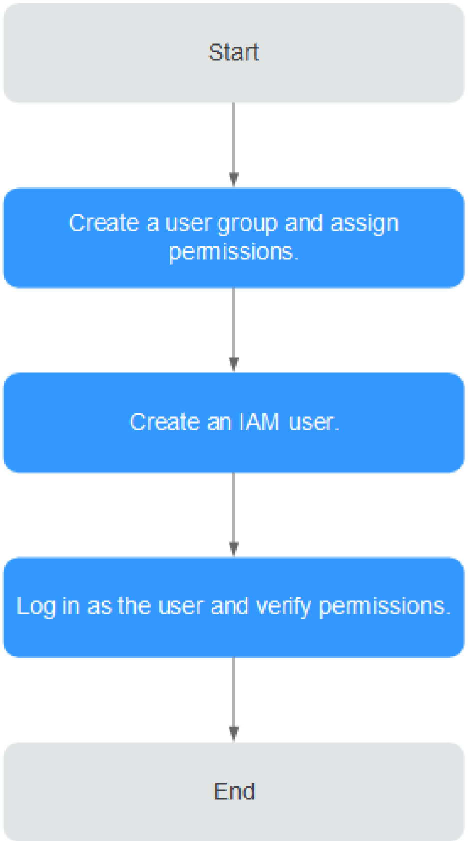
This topic describes the procedure for granting permissions (see **Figure 11-1**).

Prerequisites

- Learn about the system policies supported by Cloud Eye (see **System-defined policy summary**) and choose policies according to your requirements. For the permissions of other services, see **System Permissions**.

Process Flow

Figure 11-1 Process for granting Cloud Eye permissions



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

   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.
   - To grant more refined Cloud Eye permissions to user groups, see **System-defined policy summary**.

2. **Create an IAM user**.

   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.

11.2 Cloud Eye Custom Policies

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

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

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

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

Example Custom Policies

- Example 1: Allowing users to modify alarm rules

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

- Example 2: Denying alarm rule deletion

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

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

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

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

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


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

12 Quota Adjustment

What Is Quota?

Quotas are enforced for service resources on the platform to prevent unforeseen spikes in resource usage. 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.

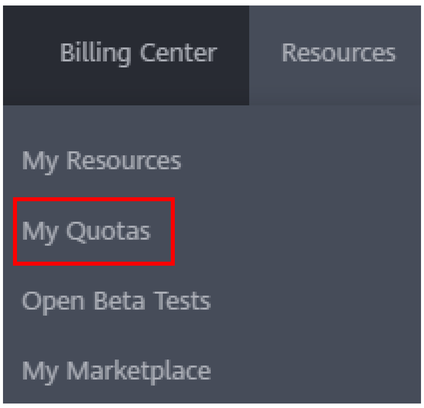
If the existing resource quota cannot meet your service requirements, you can apply for a higher quota.

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, choose **Resources** > **My Quotas**.

   The **Service Quota** page is displayed.

   Figure 12-1 My Quotas

4. View the used and total quota of each type of resources on the displayed page.

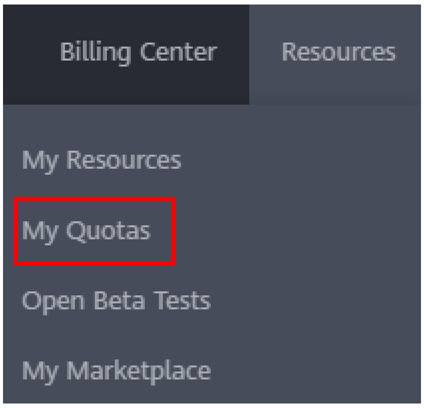
   If a quota cannot meet service requirements, apply for a higher quota.

How Do I Apply for a Higher Quota?

1. Log in to the management console.
2. In the upper right corner of the page, choose **Resources** > **My Quotas**.

   The **Service Quota** page is displayed.

   Figure 12-2 My Quotas

3. Click **Increase Quota**.
4. On the **Create Service Ticket** page, configure parameters as required.

   In **Problem Description** area, fill in the content and reason for adjustment.
5. After all necessary parameters are configured, select **I have read and agree to the Tenant Authorization Letter and Privacy Statement** and click **Submit**.

13 Services Interconnected with Cloud Eye

Category	Service	Namespace	Dimension	Reference
Compute	Elastic Cloud Server	SYS.ECS	Key: instance_id Value: ECS ID	**ECS metrics**
	ECS OS Monitoring	AGT.ECS	Key: instance_id Value: ECS ID	**OS Monitoring Metrics Supported by ECSs with the Agent Installed and Using Simplified Monitoring Metrics**
	ECS OS Monitoring (Latin America region)	AGT.ECS	Key: instance_id Value: ECS ID	**OS Monitoring Metrics Supported by ECSs with the Agent Installed**
	Bare Metal Server	SERVICE.BMS	Key: instance_id Value: BMS ID	**Supported Monitoring Metrics (with Agent Installed and Simplified Metrics)**
	BMS (Latin America)	SERVICE.BMS	Key: instance_id Value: BMS ID	**Supported Monitoring Metrics (with Agent Installed)**
	Auto Scaling	SYS.AS	Key: AutoScalingGroup Value: AS group ID	**AS metrics**

Category	Service	Namespace	Dimension	Reference
	Cloud Phone	SYS.CPH	• Key: instance_id Value: server ID • Key: cph_id Value: cloud phone ID • Key: disk_name Value: disk name • Key: gpu_index Value: GPU name	**Cloud Phone metrics**
	FunctionGraph	SYS.FunctionGraph	Key: package-functionname Value: app name-function name	**FunctionGraph metrics**
Storage	Elastic Volume Service (attached to an ECS or BMS)	SYS.EVS	Key: disk_name Value: server ID-drive letter (sda is the drive letter.)	**EVS metrics**
	Object Storage Service	SYS.OBS	Key: bucket_name Value: bucket name	**OBS metrics**
	Scalable File Service	SYS.SFS	Key: share_id Value: SFS file system	**SFS metrics**
	SFS Turbo	SYS.EFS	Key: efs_instance_id Value: instance	**SFS Turbo metrics**
Network	Elastic IP and bandwidth	SYS.VPC	• Key: publicip_id Value: EIP ID • Key: bandwidth_id Value: bandwidth ID	**VPC metrics**

Category	Service	Namespace	Dimension	Reference
	Elastic Load Balance	SYS.ELB	• Key: lb_instance_id Value: ID of a classic load balancer • Key: lbaas_instance_id Value: ID of a shared load balancer • Key: lbaas_listener_id Value: ID of a shared load balancer listener	**ELB metrics**
	Direct Connect	SYS.DCAAS	• Key: direct_connect_id Value: connection • Key: history_direct_connect_id Value: historical connection	**Direct Connect metrics**
	Virtual Private Network	SYS.VPN	Key: connection_id Value: VPN connection	**VPN metrics**
	NAT Gateway	SYS.NAT	Key: nat_gateway_id Value: NAT gateway ID	**NAT Gateway metrics**

Category	Service	Namespace	Dimension	Reference
	Cloud Connect	SYS.CC	• Key: cloud_connect_id Value: cloud connection ID • Key: bwp_id Value: bandwidth package ID • Key: region_bandwidth_id Value: inter-region bandwidth ID	**Cloud Connect metrics**
Application	Distributed Message Service	SYS.DMS	For details, see the information in the right column.	**DMS metrics** **DMS Kafka metrics** **DMS RabbitMQ instance metrics**
	API Gateway	SYS.APIG	Key: api_id Value: API	**API Gateway metrics**

Category	Service	Namespace	Dimension	Reference
	Distributed Cache Service	SYS.DCS	• Key: dcs_instance_id Value: DCS Redis instance • Key: dcs_cluster_redis_node Value: Redis Server • Key: dcs_cluster_proxy_node Value: Proxy in a Proxy Cluster DCS Redis 3.0 instance • Key: dcs_cluster_proxy2_node Value: Proxy in a Proxy Cluster DCS Redis 4.0 or 5.0 instance • Key: dcs_memcached_instance_id Value: DCS Memcached instance	**DCS metrics**
	ROMA	SYS.ROMA	For details, see **ROMA metrics**.	**ROMA metrics**
Database	Relational Database Service	SYS.RDS	For details, see the information in the right column.	**RDS for MySQL metrics** **RDS for PostgreSQL metrics** **RDS for SQL Server metrics**

Category	Service	Namespace	Dimension	Reference
	Document Database Service	SYS.DDS	• Key: mongodb_node_id Value: DDS node ID • Key: mongodb_instance_id Value: DDS DB instance ID	**DDS metrics**
	Distributed Database Middleware	SYS.DDM	Key: ddm_node_id Value: DDM node	**DDM metrics**
	GaussDB NoSQL	SYS.NoSQL	For details, see the information in the right column.	**GaussDB(for Cassandra) metrics** **GaussDB(for Mongo) metrics** **GaussDB(for Influx) metrics** **GaussDB(for Redis) metrics**
Migration	Cloud Data Migration	SYS.CDM	Key: instance_id Value: CDM instance	**CDM metrics**
Enterprise Intelligence	Data Warehouse Service	SYS.DWS	• Key: datastore_id Value: data warehouse cluster ID • Key: dws_instance_id Value: data warehouse node ID	**DWS metrics**
	ModelArts	SYS.ModelArts	• Key: service_id Value: real-time service ID • Key: model_id Value: model ID	**ModelArts metrics**
	Cloud Search Service	SYS.ES	Key: cluster_id Value: CSS cluster	**CSS metrics**

Category	Service	Namespace	Dimension	Reference
	ImageSearch	SYS.IS	Key: instanceName Value: instance name	**ImageSearch metrics**
	Image Recognition	SYS.IRS	Key: call_of_interface Value: API	**Image Recognition metrics**
	Content Moderation	SYS.MODERATION	Key: call_of_interface Value: API	**Content Moderation metrics**
	Face Recognition	SYS.FRS	• Key: call_of_api Value: API • Key: face_set Value: facial image library	**Face Recognition metrics**
	Natural Language Processing	SYS.NLP	Key: call_of_interface Value: API	**NLP metrics**
	Optical Character Recognition	SYS.OCR	Key: call_of_interface Value: API	**OCR metrics**
	Graph Engine Service	SYS.GES	Key: instance_id Value: GES instance	**GES metrics**
	Data Lake Insight	SYS.DLI	• Key: queue_id Value: queue instance • Key: flink_job_id Value: Flink job	**DLI metrics**

14 Troubleshooting

14.1 One-Click Agent Restoration Fails

Symptom

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

Possible Cause

Check the following items to troubleshoot the fault:

1. DNS configuration
2. IAM agency configuration
3. User permissions

Solution

Step 1 Check the DNS configuration.

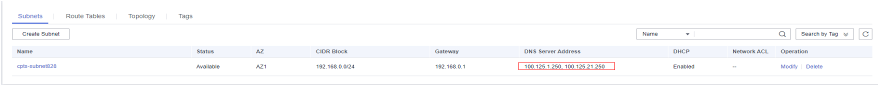
1. Log in to the management console.
2. Under **Computing**, select **Elastic Cloud Server**.
3. Click the name of the ECS.

   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)**.

Figure 14-1 DNS server address



Step 2 Check the IAM agency configuration.

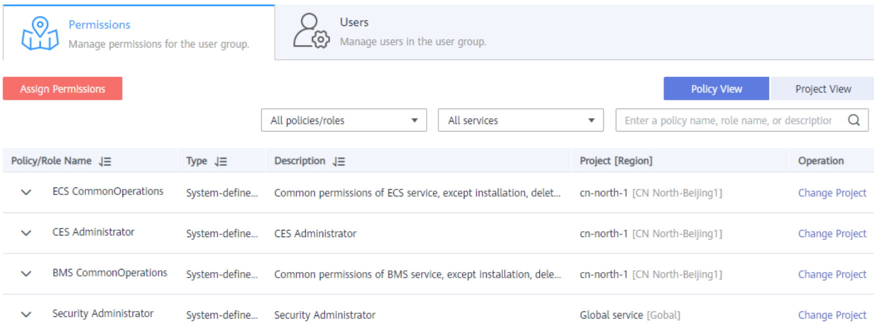
1. Log in to the management console.
2. Hover your mouse on the username and click **Identity and Access Management**.
3. On the IAM console, choose **Agencies**.
4. Check whether there is an agency named **CESAgentAutoConfigAgency**.

   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. Hover your mouse on the username and click **Identity and Access Management**.
3. In the navigation pane on the left, click **User Groups**.
4. Locate your user group and click **Assign Permissions** 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

Figure 14-2 User permissions required for installing the Agent



----End

14.2 What Can I Do If No Monitoring Data Is Displayed After One-Click Agent Restoration? (Old Agent)

Symptoms

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

Possible Causes

If no OS monitoring data is available for an ECS or BMS with 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.

Check the Agent version.

1. Log in to an ECS as user **root**.
2. Run the following command to check the Agent version:

   if [[-f /usr/local/uniagent/extension/install/telescope/bin/telescope]]; then /usr/local/uniagent/extension/install/telescope/bin/telescope -v; else echo 0; fi

   – If **0** is returned, the old Agent is used.

   – If other values are returned, the new Agent is used.

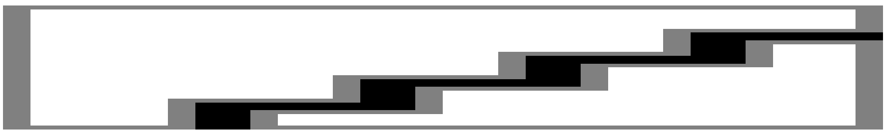
Troubleshooting for Linux

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

   The following information indicates that the telescope process is normal.

   Figure 14-3 Viewing the telescope processes

   – If yes, go to **4**.

   – If no, go to **3**.
3. Run the following command to start the Agent process:

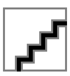
   /usr/local/telescope/telescoped start
4. Run the following command to check whether an agency has been created for the server:

   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 14-4 Failing to obtain the AK/SK

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 14-5 Abnormal 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.

   Figure 14-6 Querying the telescope endpoint

```
[root@hss log]# cat /usr/local/telescope/bin/conf_ces.json
{
"Endpoint": "https://ces.cn-south-1.myhuaweicloud.com"
}[root@hss log]#
```

10. Run the following command to check whether the DNS service is normal:
   ping *ces.cn-south-1.myhuaweicloud.com*
   – If the network is normal, no further action is required.
   – Otherwise, modify the **DNS server** 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.

Processes in **Figure 14-7** and **Figure 14-8** indicate that the telescope process is running.

Figure 14-7 agent process (Windows)

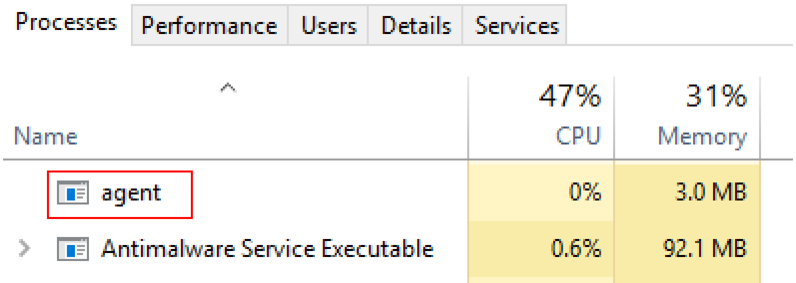
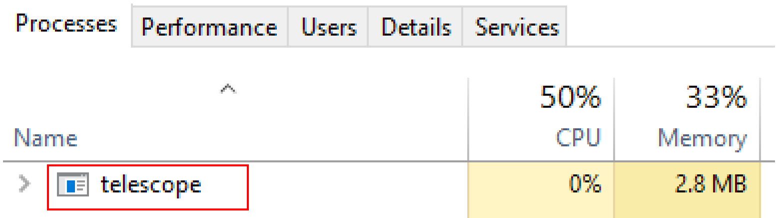


Figure 14-8 telescope process (Windows)



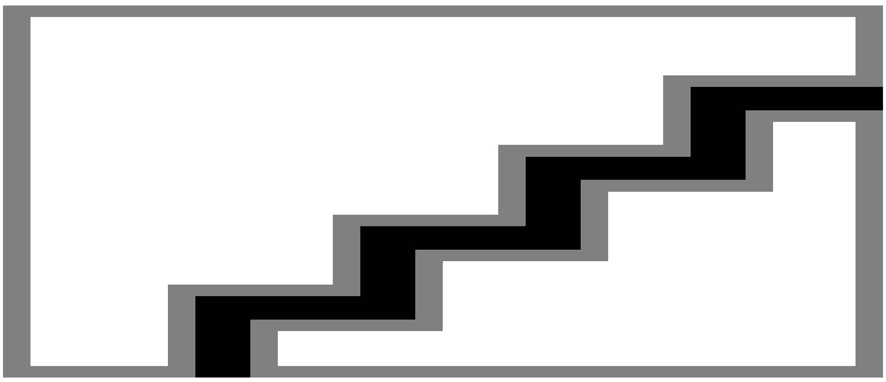
   – If yes, go to **4**.
   – If no, go to **3**.

3. Double-click **start.bat** to start the Agent.
4. Access **http://169.254.169.254/openstack/latest/meta_data.json** and 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 14-9 Abnormal route configuration-Windows



   – 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 configuration file.

   {"Endpoint":"https://ces.cn-north-4.myhuaweicloud.com"}
9. Run the following command to check whether the DNS service is normal:

   ping *ces.cn-south-14.myhuaweicloud.com*
   – If the network is normal, no further action is required.
   – Otherwise, modify the **DNS server** or the Cloud Eye endpoint.

     NOTE

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

A Change History

Released On	Description
2020-05-30	This issue is the forty-eighth official release. ● Added the enterprise project function in **Creating a Resource Group** and **Creating an Alarm Rule**.
2020-04-10	This issue is the forty-seventh official release. ● Added **Installing the Direct Connect Metric Collection Plug-ins**.
2020-01-20	This issue is the forty-sixth official release. ● Updated **Cloud Eye Custom Policies** and deleted "syntax of fine-grained policies" in **Cloud Eye Custom Policies**.
2020-01-15	This issue is the forty-fifth official release. ● Added information about the CN Southwest-Guiyang1 region in **Server Monitoring**.
2019-12-30	This issue is the forty-fourth official release. ● Added the procedure for manually configuring the Agent in the CN East-Shanghai1 region in **(Optional) Manually Configuring the Agent (Linux)** and **(Optional) Manually Configuring the Agent (Windows)**.
2019-12-04	This issue is the forty-third official release. ● Added description about the visual editor in **Creating a User and Granting Permissions** and **Cloud Eye Custom Policies**.
2019-11-15	This is the forty-second official release. ● Added **Services Interconnected with Cloud Eye**.

Released On	Description
2019-09-30	This is the forty-first official release. ● Added information about the CN East-Shanghai1 region in **Server Monitoring**.
2019-09-19	This issue is the fortieth official release. ● Optimized content in **Events Supported by Event Monitoring**.
2019-09-06	This issue is the thirty-ninth official release. ● Added fine-grained authorization and syntax of fine-grained policies in **Cloud Eye Custom Policies**.
2019-07-31	This issue is the thirty-eighth official release, which incorporates the following changes: ● Added **Why Is the Monitoring Data Not Displayed on the Cloud Eye Console?** ● Added **How do I Query the Current Agent Version?** ● Added "GES Metrics" in **Services Interconnected with Cloud Eye**.
2019-06-12	This issue is the thirty-fifth official release, which incorporates the following changes: ● Added the content of permissions management. ● Launched the one-click monitoring function. ● Added "DCS Metrics" in **Services Interconnected with Cloud Eye**. ● Added "SFS Turbo Metrics" in **Services Interconnected with Cloud Eye**. ● Added "SFS Metrics" in **Services Interconnected with Cloud Eye**. ● Added "NLP Metrics" in **Services Interconnected with Cloud Eye**.
2019-04-30	This issue is the thirty-sixth official release, which incorporates the following changes: ● Optimized the procedure for installing the Agent. ● Added application scenarios to the product introduction. ● Interconnected with Elastic File Service (EFS). ● Interconnected with Database Security Service (DBSS).

Released On	Description
2019-03-30	This issue is the thirty-fifth official release, which incorporates the following changes: ● Changed **Virtual Private Cloud** to **Elastic IP and Bandwidth** under **Cloud Service Monitoring** on the Cloud Eye console. ● Optimized the Distributed Message Service (DMS) metrics.
2019-03-14	This issue is the thirty-fourth official release, which incorporates the following changes: ● Optimized the procedure for adding security group rules. ● Added Distributed Cache Service (DCS) metrics. ● Interconnected with Face Recognition. ● Optimized Relational Database Service (RDS) metrics.
2019-02-21	This issue is the thirty-third official release, which incorporates the following changes: ● Added "Quota Adjustment". ● Supported server monitoring in region **CN North-Beijing4**. ● Interconnected with Conversational Bot Service (CBS).
2019-01-17	This issue is the thirty-second official release, which incorporates the following changes: ● Optimized the names of Elastic Cloud Server (ECS) and Elastic Volume Service (EVS) disk metrics. ● Optimized the names of two Relational Database Service (RDS) metrics.
2018-12-30	This issue is the thirty-first official release, which incorporates the following changes: ● Added Distributed Message Service (DMS) metrics. ● Added Cloud Search Service (CSS) metrics.
2018-11-30	This issue is the thirtieth official release, which incorporates the following changes: ● Added FunctionGraph metrics. ● Added Elastic Load Balance (ELB) metrics.
2018-11-15	This issue is the twenty-ninth official release, which incorporates the following changes: ● Launched custom monitoring for processes. ● Added Cloud Assistant. ● Added Relational Database Service (RDS) metrics.

<table>
<tr><th>Released On</th><th>Description</th></tr>
<tr><td>2018-10-30</td><td>This issue is the twenty-eighth official release, which incorporates the following changes:
Added validity time in the alarm rule creation.
Users can create alarm rules for one resource in a resource group or for the whole resource group.
Interconnected with Automatic Speech Recognition (ASR), Image Recognition, Content Moderation, and Text To Speech (TTS).</td></tr>
<tr><td>2018-09-30</td><td>This issue is the twenty-seventh official release, which incorporates the following changes:
Added Distributed Database Middleware (DDM) metrics.
Added Elastic Load Balance (ELB) metrics.
Added Direct Connect metrics.
Optimized the Create Alarm Rule window.
Added Distributed Message Service (DMS) metrics.</td></tr>
<tr><td>2018-08-30</td><td>This issue is the twenty-sixth official release, which incorporates the following changes:
Added Distributed Database Middleware (DDM) metrics.
Added OS Monitoring metrics.
Optimized the procedure for installing the Agent.</td></tr>
<tr><td>2018-07-30</td><td>This issue is the twenty-fifth official release, which incorporates the following changes:
Added ECS automatic recovery for Event Monitoring.
Resource groups support BMSs.
The Agent can be installed to a specified directory.
Added descriptions about specifying ports for the Agent.
Added Elastic Volume Service (EVS) metrics.</td></tr>
<tr><td>2018-06-30</td><td>This issue is the twenty-fourth official release, which incorporates the following changes:
Added the function of configuring data storage in bathes.
Added the function of restoring the Agent configurations for ECSs.
Added Elasticsearch metrics.
Added Relational Database Service (RDS) metrics.
Added Virtual Private Cloud (VPC) traffic metrics.</td></tr>
</table>

Released On	Description
2018-05-30	This issue is the twenty-third official release, which incorporates the following changes: ● **OS Monitoring** supports process metrics. ● **OS Monitoring** supports the Windows OSs. ● Added the auto refresh button to the monitoring panels.
2018-04-30	This issue is the twenty-second official release, which incorporates the following changes: ● Interconnected with NAT Gateway. ● Optimized the strings for alarm rule creation. ● Launched the **Event Monitoring** function. ● Changed the **ECS Monitoring** page.
2018-03-30	This issue is the twenty-first official release, which incorporates the following changes: ● Added Distributed Cache Service (DCS) metrics. ● Interconnected with UPredict. ● Interconnected with ElasticSearch. ● **OS Monitoring** supports GPU metrics. ● Launched the **Resource Groups** function. ● Launched the **Log Monitoring** function.
2018-02-28	This issue is the twentieth official release, which incorporates the following changes: ● Added Artificial Intelligence Service (AIS) metrics. ● Interconnected with Cloud Data Migration (CDM). ● Added the **Availability** feature to the website monitoring function. ● **OS Monitoring** supports load metrics.
2018-01-30	This issue is the nineteenth official release, which incorporates the following changes: ● Launched the **Custom Monitoring** function. ● Added Artificial Intelligence Service (AIS) metrics. ● Launched the **Website Monitoring** function.
2018-01-26	This issue is the eighteenth official release, which incorporates the following changes: ● Launched the **Process Monitoring** function. ● **OS Monitoring** supports NIC metrics. ● Added the metric sorting function. ● Interconnected with Object Storage Service (OBS).

Released On	Description
2017-12-30	This issue is the seventeenth official release, which incorporates the following changes: ● Interconnected with API Gateway. ● Interconnected with Document Database Service (DDS). ● Interconnected with CloudTable. ● Added Distributed Cache Service (DCS) metrics. ● Added Artificial Intelligence Service (AIS) metrics.
2017-11-30	This issue is the sixteenth official release, which incorporates the following changes: ● Interconnected with Distributed Database Middleware (DDM). ● Added Artificial Intelligence Service (AIS) metrics. ● Added Auto Scaling (AS) metrics. ● Added the content of using Cloud-Init to automatically install and configure the Agent. ● Added the function of **Metric Data Transfer to OBS**.
2017-10-30	This issue is the fifteenth official release, which incorporates the following changes: ● Launched the **Advanced Monitoring** function. ● Optimized the descriptions of Distributed Message Service (DMS) metrics. ● When you create a topic, the page jumps from the Cloud Eye console to the SMN console.
2017-09-30	This issue is the fourteenth official release, which incorporates the following changes: ● Added the **Custom Alarm Templates** function. ● Added **Monitoring Overview**. ● Added FunctionGraph metrics. ● Added Scalable File Service (SFS) metrics.
2017-08-30	This issue is the thirteenth official release, which incorporates the following changes: ● Added the alarm template. ● Updated the process of adding alarm rules.
2017-07-30	This issue is the twelfth official release, which incorporates the following changes: ● Added Artificial Intelligence Service (AIS) metrics. ● Added an FAQ: Under What Circumstances Will an Alarm Rule Trigger "Insufficient data"?

Released On	Description
2017-06-30	This issue is the eleventh official release, which incorporates the following change: Optimized the **Instance Monitoring** page and supported tiled display of multiple metrics.
2017-05-26	This issue is the tenth official release, which incorporates the following changes: ● Added Distributed Message Service (DMS) metrics. ● Added **Metric Quantity** description. ● Added **Sum** as a rollup method.
2017-04-28	This issue is the ninth official release, which incorporates the following changes: ● Added Machine Learning Service (MLS) metrics. ● Added WEB Tamper Protection (WTP) metrics. ● Added Data Warehouse Service (DWS) metrics. ● Added Virtual Private Cloud (VPC) traffic metric.
2017-03-30	This issue is the eighth official release, which incorporates the following changes: ● Added Workspace metrics. ● Added Relational Database Service (RDS) metrics. ● Added an Elastic Cloud Server (ECS) metric that can recover ECSs.
2017-02-27	This issue is the seventh official release, which incorporates the following changes: ● Added the operation of creating a monitoring panel. ● Added the Cloud Eye data rollup mechanism.
2017-01-19	This issue is the sixth official release, which incorporates the following change: Added the rollup methods supported by Cloud Eye.
2016-12-30	This issue is the fifth official release, which incorporates the following change: Added the metric customization function.
2016-11-24	This issue is the fourth official release, which incorporates the following change: Added the alarm history viewing function.
2016-10-19	This issue is the third official release, which incorporates the following change: Deleted Resource Template Service (RTS) metrics.

Released On	Description
2016-07-15	This issue is the second official release, which incorporates the following change: Added Relational Database Service (RDS) metrics.
2016-03-14	This issue is the first official release.

