

Cloud Eye

User Guide

Issue 01
Date 2024-04-15



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

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

Trademarks and Permissions



HUAWEI and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

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

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

Huawei Technologies Co., Ltd.

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

Website: <https://www.huawei.com>

Email: support@huawei.com

Security Declaration

Vulnerability

Huawei's regulations on product vulnerability management are subject to the *Vul. Response Process*. For details about this process, visit the following web page:

<https://www.huawei.com/en/psirt/vul-response-process>

For vulnerability information, enterprise customers can visit the following web page:

<https://securitybulletin.huawei.com/enterprise/en/security-advisory>

Contents

1 Product Introduction.....	1
1.1 What Is Cloud Eye?.....	1
1.2 Advantages.....	2
1.3 Application Scenarios.....	2
1.4 Cloud Eye and Other Services.....	3
1.5 Basic Concepts.....	4
1.6 Constraints.....	5
1.7 Region and AZ.....	5
1.8 Permissions.....	6
2 Getting Started.....	14
2.1 Checking the Status of a Cloud Platform.....	14
2.2 Querying Metrics of a Cloud Service.....	14
2.3 Using Server Monitoring.....	16
2.4 Using Event Monitoring.....	17
2.5 Creating an Alarm Rule.....	17
3 Dashboards.....	19
3.1 Introduction to Dashboards.....	19
3.2 Creating a Dashboard.....	19
3.3 Adding a Graph.....	19
3.4 Viewing a Graph.....	20
3.5 Configuring a Graph.....	21
3.6 Deleting a Graph.....	21
3.7 Deleting a Dashboard.....	21
4 Resource Groups.....	23
4.1 Introduction to Resource Groups.....	23
4.2 Creating a Resource Group.....	23
4.3 Viewing Resource Groups.....	24
4.3.1 Resource Group List.....	24
4.3.2 Resource Overview.....	25
4.3.3 Unhealthy Resources.....	25
4.3.4 Alarm Rules.....	25
4.3.5 Alarm Records.....	25

4.4 Managing Resource Groups.....	26
4.4.1 Modifying a Resource Group.....	26
4.4.2 Deleting a Resource Group.....	26
5 Using the Alarm Function.....	27
5.1 Introduction to the Alarm Function.....	27
5.2 Creating Alarm Notification Topics.....	27
5.2.1 Creating a Topic.....	27
5.2.2 Adding Subscriptions.....	28
5.3 Creating Alarm Rules.....	29
5.3.1 Introduction to Alarm Rules.....	29
5.3.2 Creating an Alarm Rule by Using an Alarm Template.....	30
5.3.3 Creating an Alarm Rule for a Specific Metric.....	31
5.4 Viewing Alarm Records.....	34
5.5 One-Click Monitoring.....	34
5.6 Alarm Rule Management.....	35
5.6.1 Modifying an Alarm Rule.....	35
5.6.2 Disabling Alarm Rules.....	36
5.6.3 Enabling Alarm Rules.....	37
5.6.4 Deleting Alarm Rules.....	37
5.7 Alarm Templates.....	37
5.7.1 Viewing Alarm Templates.....	37
5.7.2 Creating a Custom Template.....	37
5.7.3 Modifying a Custom Template.....	38
5.7.4 Deleting a Custom Template.....	39
6 Server Monitoring.....	40
6.1 Introduction to Server Monitoring.....	40
6.2 Agent Installation and Configuration.....	41
6.3 Installing and Configuring the Agent on a Linux ECS.....	41
6.3.1 Modifying the DNS Server Address and Adding Security Group Rules (Linux).....	41
6.3.2 Installing the Agent on a Linux Server.....	43
6.3.3 Restoring the Agent Configurations on a Linux Server.....	44
6.3.4 (Optional) Manually Configuring the Agent (Linux).....	45
6.4 Installing and Configuring the Agent on a Windows ECS.....	48
6.4.1 Modifying the DNS Server Address and Adding Security Group Rules (Windows).....	48
6.4.2 Installing and Configuring the Agent on a Windows Server.....	50
6.4.3 (Optional) Manually Configuring the Agent on a Windows Server.....	51
6.5 Installing the Agents in Batches on Linux ECSs.....	53
6.6 Managing the Agent.....	54
6.6.1 Managing the Agent (Linux).....	54
6.6.2 Managing the Agent (Windows).....	55
6.7 Process Monitoring.....	56
6.7.1 Viewing Process Monitoring.....	56

6.8 Viewing Server Monitoring Metrics.....	61
6.9 Creating an Alarm Rule to Monitor a Server.....	62
7 Custom Monitoring.....	64
8 Event Monitoring.....	65
8.1 Introduction to Event Monitoring.....	65
8.2 Viewing Event Monitoring Data.....	65
8.3 Creating an Alarm Rule to Monitor an Event.....	66
8.4 Events Supported by Event Monitoring.....	68
9 Cloud Service Monitoring.....	73
9.1 Introduction to Cloud Service Monitoring.....	73
9.2 Viewing Metrics.....	73
10 Permissions Management.....	75
10.1 Creating a User and Granting Permissions.....	75
10.2 Cloud Eye Custom Policies.....	77
11 Quota Adjustment.....	79
12 Services Interconnected with Cloud Eye.....	80
12.1 Computing.....	80
12.1.1 ECS Metrics.....	80
12.1.2 OS Monitoring Metrics Supported by ECSs with the Agent Installed.....	85
12.1.3 AS Metrics.....	106
12.2 Storage.....	108
12.2.1 EVS Metrics.....	108
12.3 Network.....	109
12.3.1 EIP and Bandwidth Metrics.....	109
12.3.2 ELB Metrics.....	110
12.3.3 NAT Gateway Metrics.....	114
13 FAQs.....	116
13.1 General Consulting.....	116
13.1.1 What Is Rollup?.....	116
13.1.2 How Long Is Metric Data Retained?.....	116
13.1.3 How Many Rollup Methods Does Cloud Eye Support?.....	117
13.1.4 How Can I Export Collected Data?.....	117
13.2 Server Monitoring.....	118
13.2.1 How Can I Quickly Restore the Agent Configuration?.....	118
13.2.2 What OSs Does the Agent Support?.....	118
13.2.3 How Do I Query the Current Agent Version?.....	120
13.2.4 What Should I Do If the Service Port Is Used by the Agent?.....	120
13.2.5 How Can I Create an Agency?.....	121
13.2.6 What Can't I Create Another Agency?.....	122
13.2.7 What Should I Do If Agency CESAgentAutoConfigAgency Failed to Be Automatically Created?.....	122

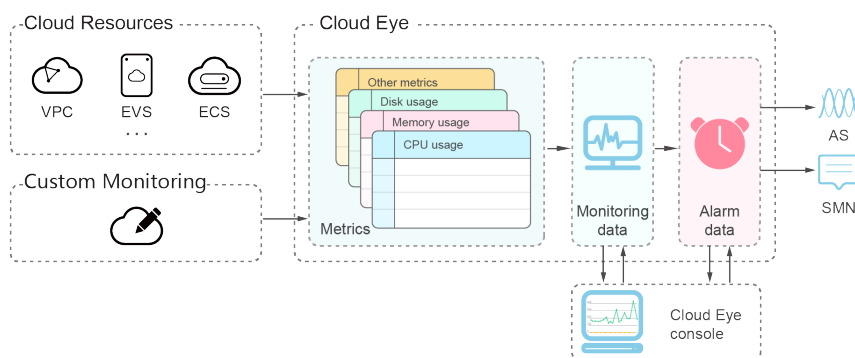
13.2.8 What Can I Do If Agency CESAgentAutoConfigAgency Is Invalid?.....	122
13.2.9 Will the Agent Affect the Server Performance?.....	122
13.2.10 What Should I Do If the Agent Status Is Faulty?.....	122
13.3 Alarm Notifications or False Alarms.....	123
13.3.1 What Is an Alarm Notification? How Many Types of Alarm Notifications Are There?.....	123
13.3.2 What Alarm Status Does Cloud Eye Support?.....	123
13.3.3 What Alarm Severities Does Cloud Eye Support?.....	124
13.4 Monitored Data Exceptions.....	124
13.4.1 Why Is the Monitoring Data Not Displayed on the Cloud Eye Console?.....	124
13.4.2 Why Are the Network Traffic Metric Values in Cloud Eye Different from Those Detected in ECS?.....	124
13.4.3 What Are the Impacts on ECS Metrics If Not Installed on ECSs?.....	125
13.5 User Permissions.....	125
13.5.1 What Should I Do If the IAM User Permissions Are Abnormal?.....	125
A Change History.....	126

1 Product Introduction

1.1 What Is Cloud Eye?

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

Figure 1-1 Cloud Eye architecture



Cloud Eye provides the following functions:

- **Automatic monitoring**
Monitoring starts automatically after you created resources such as Elastic Cloud Servers (ECSs). On the Cloud Eye console, you can view statuses of the resources and set alarm rules for them.
- **Flexible alarm rule configuration**
You can create alarm rules for multiple resources at the same time. After you create an alarm rule, you can modify, enable, disable, or delete it at any time.
- **Real-time notification**
You can enable **Alarm Notification** when creating alarm rules. When the cloud service status changes and metrics reach the thresholds specified in alarm rules, Cloud Eye notifies you by SMS messages, emails, or by sending

messages to server addresses, allowing you to monitor the cloud resource status and changes in real time.

- **Dashboard**

A dashboard enables you to view cross-service and cross-dimension monitoring data. It displays key metrics and provides an overview of the service status and monitoring details that you can use for troubleshooting.

- **Event monitoring**

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

1.2 Advantages

Automatic Provisioning

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

Reliable Real-time Monitoring

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

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

Visualized Monitoring

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

Multiple Notification Types

You can enable **Alarm Notification** when creating alarm rules. When a metric reaches the threshold specified in an alarm rule, Cloud Eye notifies you by emails or SMS messages, allowing you to keep track of the statuses of cloud services and enabling you to build smart alarm handling programs.

Batch Creation of Alarm Rules

You can use alarm templates to create alarm rules in batches for multiple cloud services.

1.3 Application Scenarios

Cloud Service Monitoring

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

Performance Issues

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

Capacity Expansion

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

Custom Monitoring

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

Event Monitoring

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

1.4 Cloud Eye and Other Services

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

Cloud Eye supports automatic monitoring of the following metrics:

Compute

- [ECS Metrics](#)
- [AS Metrics](#)

Storage

- [EVS Metrics](#)

Networking

- [EIP and Bandwidth Metrics](#)
- [ELB Metrics](#)
- [NAT Gateway Metrics](#)

1.5 Basic Concepts

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

- [Metrics](#)
- [Rollup](#)
- [Dashboards](#)
- [Topics](#)
- [Alarm Rules](#)
- [Alarm Templates](#)
- [Projects](#)

Metrics

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

Rollup

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

Dashboards

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

Topics

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

Alarm Rules

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

Alarm Templates

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

Projects

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

1.6 Constraints

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

Table 1-1 Resources and their default quotas

Resource	Default Quota
Alarm rules that can be created	100
Custom alarm templates that can be created	50
Alarm rules that can be added to an alarm template	20
Dashboards that can be created	20
Graphs that can be added to a dashboard	24
Time that the alarm history can be kept	720 hours
Topics that can be selected for receiving notifications	5

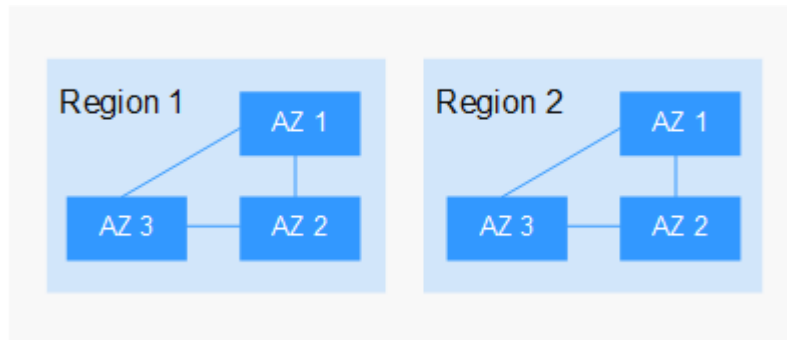
1.7 Region and AZ

Concept

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

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

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

Figure 1-2 Regions and AZs

Selecting a Region

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

Selecting an AZ

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

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

Regions and Endpoints

Before you use an API to call resources, specify its region and endpoint. For more details, see [Regions and Endpoints](#).

1.8 Permissions

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

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

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

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

Cloud Eye Permissions

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

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

You can grant users permissions by using roles and policies.

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

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

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

Table 1-2 System policies

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

Policy Name	Description	Dependency	Type
CES ReadOnlyAccess	Read-only permissions for Cloud Eye. Users granted these permissions can only view Cloud Eye data.	The Cloud Eye monitoring function involves querying resources of other cloud services, which requires the cloud services to support fine-grained authorization.	System-defined policy

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

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

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

Feature	Operation	CES Administrator (The Tenant Guest policy must be added at the same time.)	Tenant Guest	CES FullAccess	CES ReadOnlyAccess
	Adjusting the position of a graph	√	×	√	×
Resource Groups	Creating a resource group	√	×	√	×
	Viewing the resource group list	√	√	√	√
	Viewing resource groups (Resource Overview)	√	√	√	√
	Viewing resource groups (Alarm Rules)	√	√	√	√
	Viewing resource groups (Alarm Records)	√	√	√	√
	Modifying a resource group	√	×	√	×
	Deleting a resource group	√	×	√	×
Alarm Rules	Creating an alarm rule	√	×	√	×
	Modifying an alarm rule	√	×	√	×
	Enabling an alarm rule	√	×	√	×
	Disabling an alarm rule	√	×	√	×
	Deleting an alarm rule	√	×	√	×
	Querying the alarm rule list	√	√	√	√

Feature	Operation	CES Administrator (The Tenant Guest policy must be added at the same time.)	Tenant Guest	CES FullAccess	CES ReadOnlyAccess
	Viewing details of an alarm rule	√	√	√	√
	Viewing a graph	√	√	√	√
Alarm Records	Viewing alarm records	√	√	√	√
Alarm Templates	Viewing a default template	√	√	√	√
	Viewing a custom template	√	√	√	√
	Creating a custom template	√	×	√	×
	Modifying a custom template	√	×	√	×
	Deleting a custom template	√	×	√	×
Server Monitoring	Viewing the server list	√	√	√	√
	Viewing server monitoring metrics	√	√	√	√
	Installing the Agent	√ (You must have the ECS FullAccess permission.)	×	√ (You must have the ECS FullAccess permission.)	×

Feature	Operation	CES Administrator (The Tenant Guest policy must be added at the same time.)	Tenant Guest	CES FullAccess	CES ReadOnlyAccess
	Restoring the Agent configurations	√ (You must have the Security Administrator and ECS FullAccess permissions.)	×	√ (You must have the Security Administrator and ECS FullAccess permissions.)	×
	Uninstalling the Agent	√ (You must have the ECS FullAccess permission.)	×	√ (You must have the ECS FullAccess permission.)	×
	Configuring process monitoring	√	×	√	×
	Configuring monitoring for a process	√	×	√	×
Cloud Service Monitoring	Viewing the cloud service list	√	√	√ (Cloud services need to support fine-grained authorization.)	√ (Cloud services need to support fine-grained authorization.)

Feature	Operation	CES Administrator (The Tenant Guest policy must be added at the same time.)	Tenant Guest	CES FullAccess	CES ReadOnlyAccess
	Querying cloud service metrics	√	√	√	√
Custom Monitoring	Adding custom monitoring data	√	×	√	×
	Viewing the custom monitoring list	√	√	√	√
	Viewing custom monitoring data	√	√	√	√
Event Monitoring	Adding a custom event	√	×	√	×
	Viewing the event list	√	√	√	√
	Viewing details of an event	√	√	√	√
Data Dumping to DMS Kafka	Creating a dump task	√	×	√	×
	Querying data dumping tasks	√	√	√	√
	Querying a specified data dump task	√	√	√	√
	Modifying a data dump task	√	×	√	×
	Starting a data dump task	√	×	√	×
	Stopping a data dump task	√	×	√	×
	Deleting a data dump task	√	×	√	×

Feature	Operation	CES Administrator (The Tenant Guest policy must be added at the same time.)	Tenant Guest	CES FullAccess	CES ReadOnlyAccess
Others	Configuring data storage	√ (You must have the Tenant Administrator permission.)	×	√ (You must have the OBS Bucket Viewer permission.)	×
	Exporting monitoring data	√	×	√	×
	Sending an alarm notification	√	×	√	×

2 Getting Started

2.1 Checking the Status of a Cloud Platform

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

Viewing Monitored Object Statistics

1. Log in to the management console.
2. Click **Service List** in the upper left corner, and select **Cloud Eye**.
3. In the navigation pane on the left, choose **Dashboard > Monitoring Overview**, and you can view the service resource quantity in the **Monitored Object Statistics** area.

Resource Monitoring Preview (in the Alarm State)

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

Alarm Statistics

Alarm statistics display the number of critical, major, minor, and informational alarms. Click the number of one alarm severity, and you will be directed to the **Alarm Records** page displaying alarm rules of this severity.

2.2 Querying Metrics of a Cloud Service

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

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

Procedure

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

The cloud service page is displayed.


4. Locate the row that contains the cloud service resource you want to monitor and click **View Metric** in the **Operation** column.

The detailed monitoring page is displayed.

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

NOTE


- Metric units can be changed between byte or byte/s and GB or GB/s on graphs. When you are changing the unit, if the maximum value of a metric is smaller than $10^{(-5)}$, both the maximum value and the minimum value of this metric are 0. In addition, all data displayed on the graph is 0.
- If **Auto Refresh** is enabled, data is automatically refreshed every minute.
- You can search for a specific metric in the search box.
- Some cloud services allow you to view resource details. You can click **View Resource Details** in the upper part of the page to view details about monitored resources.

5. Hover your mouse over a graph and click  in the upper right corner.

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

NOTE

- If you select **1h**, **3h**, **12h**, or **1d**, raw data is displayed by default. Near the top left corner of the page, you can click **Settings** to change the rollup period of the monitoring data. For details about the rollup period, see [What Is Rollup?](#)
- If you select **7d** or **30d**, aggregated data is displayed by default. Near the top left corner of the page, you can click **Settings** to change the rollup period of the monitoring data.

6. In the upper right corner of the monitoring view, click  to create an alarm rule for a metric. For details about the parameters, see [Creating an Alarm Rule for a Specific Metric](#).
7. To export data, click **Export Data** on the **Cloud Service Monitoring** page, configure parameters as prompted, and click **Export**. For details, see [How Can I Export Collected Data?](#)

2.3 Using Server Monitoring

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

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

NOTE

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

Functions

- Various Metrics
Server monitoring provides more than 40 metrics, such as metrics for CPU, memory, disk, and network usage, meeting the basic monitoring and O&M requirements for servers.
- Fine-grained Monitoring
After the Agent is installed, the metrics collected by the Agent are reported every minute.
- Process Monitoring
CPU usage, memory usage, and number of opened files used by active processes are monitored to help you better understand the resource usages on ECSs and BMSs.

Using Server Monitoring

1. Log in to the management console.
2. Click **Service List** in the upper left corner, and select **Cloud Eye**.
3. In the navigation pane on the left, choose **Server Monitoring**.
4. Select the target ECS and install the Agent on it.
 - a. Change the DNS server address of and add security group rules to the target ECS. For details, see [Modifying the DNS Server Address and Adding Security Group Rules \(Linux\)](#) or [Modifying the DNS Server Address and Adding Security Group Rules \(Windows\)](#).
 - b. Install the Agent. For details, see [Installing the Agent on a Linux Server](#) or [Installing and Configuring the Agent on a Windows Server](#).
5. After 5 minutes, check whether the Agent status is **Running**.
If yes, the Agent has been installed successfully.
On the right of the ECS, click **View Metric** in the **Operation** column to view the monitoring data.

2.4 Using Event Monitoring

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

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

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

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

Viewing Event Monitoring Graphs

1. Log in to the management console.
2. Click **Service List** in the upper left corner, and select **Cloud Eye**.
3. In the navigation pane on the left, choose **Event Monitoring**.
On the page displayed, all system events and custom events of the last 24 hours are displayed by default.
4. Select an event and click **View Graph** in the **Operation** column.

Creating an Alarm Rule

1. Log in to the management console.
2. Click **Service List** in the upper left corner, and select **Cloud Eye**.
3. In the navigation pane on the left, choose **Event Monitoring**.
4. In the event list, locate the event and click **Create Alarm Rule** in the **Operation** column.
5. Configure the alarm rule name, alarm policy, and alarm notification as prompted.
After you create the alarm rule, if the metric data reaches the threshold, Cloud Eye immediately notifies you through SMN that an exception has occurred.

2.5 Creating an Alarm Rule

Scenarios

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

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

Functions

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

Procedure

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

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

3 Dashboards

3.1 Introduction to Dashboards

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

3.2 Creating a Dashboard

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

Procedure

1. Log in to the management console.
2. Click **Service List** in the upper left corner, and select **Cloud Eye**.
3. In the navigation pane on the left, choose **Overview > Dashboards** and click **Create Dashboard**.
The **Create Dashboard** dialog box is displayed.
4. Set the dashboard name.
Enter a maximum of 128 characters. Only letters, digits, hyphens (-), and underscores (_) are allowed.
5. Click **OK**.

3.3 Adding a Graph

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


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

Procedure

1. Log in to the management console.
2. Click **Service List** in the upper left corner, and select **Cloud Eye**.
3. Choose **Overview > Dashboards**, switch to the desired dashboard, and click **Add Graph**.
The **Add Graph** dialog box is displayed.
4. Set parameters based on [Table 3-1](#).

Table 3-1 Parameters

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

5. Click **OK**.
On the selected dashboard, you can view the trends of the new graph. If you hover your mouse on the graph and click , you can view detailed metric data comparison.

3.4 Viewing a Graph

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


Procedure

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

You can view all monitoring graphs on the current dashboard.

 **NOTE**

- You can sort graphs by dragging them.
- You can click **1h**, **3h**, **12h**, **1d**, or **7d** in the upper part of monitoring graphs to switch the monitoring periods of all graphs on the dashboard. By default, raw metric data is displayed for **1h**, and the aggregated metric data is displayed for other periods.

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

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

3.5 Configuring a Graph

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

Procedure

1. Log in to the management console.
2. Click **Service List** in the upper left corner, and select **Cloud Eye**.
3. In the navigation pane on the left, choose **Overview > Dashboards**. Select the target panel and graph, and click the configure icon.

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

 **NOTE**

You can add up to 20 metrics to a graph.

3.6 Deleting a Graph

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

3.7 Deleting a Dashboard

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

Procedure

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

4 Resource Groups

4.1 Introduction to Resource Groups

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

4.2 Creating a Resource Group

Scenarios

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

Restrictions

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

Procedure

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

 **NOTE**

8. Click **Create**.

4.3 Viewing Resource Groups

4.3.1 Resource Group List

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

Procedure

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

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

Table 4-1 Parameters of the resource group list

Parameter	Description
Name/ID	Specifies the resource group name and ID. NOTE The group name can contain a maximum of 128 characters. Only letters, digits, hyphens (-), and underscores (_) are allowed.
Health Status	<ul style="list-style-type: none">● 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.
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, 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, Total Resources is 4 .
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.

4.3.2 Resource Overview

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

Procedure

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

4.3.3 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 project.
3. Click **Service List** in the upper left corner, and select **Cloud Eye**.
4. In the navigation pane on the left, choose **Resource Groups**.
5. Click a resource group name to go to the **Resource Overview** page.
6. In the navigation pane on the left, choose **Unhealthy Resources** to view all resources in the resource group for which alarms have been triggered.

4.3.4 Alarm Rules

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

Procedure

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

4.3.5 Alarm Records

The **Alarm Records** page displays alarm records for all resources in a resource group.

Procedure

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

4.4 Managing Resource Groups

4.4.1 Modifying a Resource Group

When you need to add resources to or delete resources from a resource group, modify the resource group.

Procedure

1. Log in to the management console.
2. In the upper left corner, select a region and project.
3. Click **Service List** in the upper left corner, and select **Cloud Eye**.
4. In the navigation pane on the left, choose **Resource Groups**.
5. Locate the row containing the target resource group and click **Modify** in the **Operation** column.
6. On the displayed **Modify Resource Group** page, modify the resource group.
7. Click **Modify**.

4.4.2 Deleting a Resource Group

Procedure

1. Log in to the management console.
2. In the upper left corner, select a region and project.
3. Click **Service List** in the upper left corner, and select **Cloud Eye**.
4. In the navigation pane on the left, choose **Resource Groups**.
5. Locate the row containing the target resource group and click **Delete** in the **Operation** column.
6. In the displayed **Delete Resource Group** dialog box, click **Yes**.

5 Using the Alarm Function

5.1 Introduction to the Alarm Function

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

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

NOTE

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


5.2 Creating Alarm Notification Topics

5.2.1 Creating a Topic

Scenarios

A topic is a specified event to publish messages and subscribe to notifications. It serves as a message sending channel, where publishers and subscribers can interact with each other.

Creating a Topic

1. Log in to the management console.
2. Click  on the upper left to select the desired region and project.
3. In the service list, select **Simple Message Notification**.
The SMN console is displayed.

- In the navigation pane, choose **Topics**.
The **Topics** page is displayed.
- In the upper right corner, click **Create Topic**.
- Enter a topic name and display name.

Table 5-1 Information required for creating a topic

Parameter	Description
Topic Name	Topic name, which: <ul style="list-style-type: none">Contains only letters, digits, hyphens (-), and underscores (_), and must start with a letter or digit.Contain 1 to 255 characters.Must be unique and cannot be modified once the topic is created.
Display Name	Message sender name, which must be fewer than 192 characters. NOTE After you specify a display name, the sender in email messages will be presented as <i>Display name</i> <username@example.com>. Otherwise, the sender will be username@example.com .

- Click **OK**.
The topic you created is displayed in the topic list. The system generates a topic URN, which is the unique resource identifier of the topic and cannot be changed.
- Click the name of the topic to view its details, including the URN, display name, and subscriptions.

5.2.2 Adding Subscriptions

Scenarios

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

Adding a Subscription

- Log in to the management console.
- In the service list, select **Simple Message Notification**.
The SMN console is displayed.
- In the navigation tree on the left, choose **Topics**.
The **Topics** page is displayed.
- Click the topic name. The topic details are displayed.
- On the **Subscriptions** tab, query the subscription list.
- Click **Add Subscription** in the upper right of the subscription list.

- The **Add Subscription** page is displayed.
- Specify the subscription protocol and endpoint.

Table 5-2 Information required for adding a subscription

Parameter	Description
Topic Name	Provides the name of the topic to be subscribed to, which cannot be changed.
Protocol	Specifies the protocol the subscription endpoint supports. The available options include SMS , Email , HTTP , and HTTPS .
Endpoint	Specifies the subscription endpoint. You can enter up to 10 endpoints, with every two separated with a line break. <ul style="list-style-type: none">SMS: Enter one or more phone numbers. The phone number must be preceded by a plus sign (+) and the country code. For example: +8600000000000 +8600000000001Email: Enter one or more email addresses. For example: username@example.com username2@example.comHTTP or HTTPS: Enter one or more public network URLs. For example: http://example.com/notification/action http://example2.com/notification/action

- Click **OK**.

The subscription you added is displayed in the subscription list. SMN automatically sends a confirmation message to the subscription endpoint, and the subscriber must confirm the subscription within 48 hours so that they can receive notification messages. Otherwise, you need to send a new confirmation message to the subscriber.

5.3 Creating Alarm Rules

5.3.1 Introduction to Alarm Rules

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

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

5.3.2 Creating an Alarm Rule by Using an Alarm Template

Cloud Eye allows you to use alarm templates to create alarm rules, making it easy and convenient to add or modify alarm rules for resources or cloud services, especially for a large number of resources and cloud services.

This topic describes how to use a default alarm template to create an alarm rule for a cloud service resource.

Creating an Alarm Rule

1. Log in to the management console.
2. Click **Service List** in the upper left corner, and select **Cloud Eye**.
3. In the navigation pane on the left, choose **Alarm Management > Alarm Rules**.
4. Click **Create Alarm Rule** in the upper right corner.
5. On the **Create Alarm Rule** page, configure the parameters.
 - a. Select an object and configure other parameters listed in [Table 5-3](#). Click **Next**.

NOTE

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

Table 5-3 Parameters

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.
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
Monitoring Scope	Specifies the monitoring scope the alarm rule applies to. You can select Resource groups or Specific resources . NOTE <ul style="list-style-type: none">• If Resource groups is selected, an alarm is triggered when any resource in the group meets the alarm policy.• If Resource groups is selected, alarm rules cannot be created using templates.

Parameter	Description
Select Group	This parameter is mandatory when Monitoring Scope is set to Resource groups .

- b. If you select **Use template** for **Method**, you also need to specify the parameters listed in [Table 5-4](#).

Table 5-4 Parameters

Parameter	Description
Method	Specifies the means you use to create the alarm rule.
Template	Specifies the template to be used.
Alarm Notification	Specifies whether to notify users when alarms are triggered. Notifications can be sent by email or HTTP/HTTPS message.
Notification Object	Specifies the object to which alarm notifications will be sent. You can select the account contact or a topic. <ul style="list-style-type: none">• Account contact is the mobile number and email address of the registered account.• Topic: A topic is used to publish messages and subscribe to notifications. If the required topic is unavailable, create one first and add subscriptions to it. For details, see Creating a Topic and Adding Subscriptions.
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	You can select Generated alarm (when an alarm is generated), Cleared alarm (when an alarm is cleared), or both.

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

5.3.3 Creating an Alarm Rule for a Specific Metric

Cloud Eye enables you to create alarm rules for a metric of one or multiple cloud services, making it convenient for you to monitor the metric of your resources.

Adding an Alarm Rule

1. Log in to the management console.

2. Click **Service List** in the upper left corner, and select **Cloud Eye**.
3. In the navigation pane on the left, choose **Alarm Management > Alarm Rules**, and click **Create Alarm Rule** in the upper right corner.
4. On the **Create Alarm Rule** page, follow the prompts to configure the parameters.
 - a. Select an object and configure other parameters listed in [Table 5-5](#).

Table 5-5 Parameters

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.
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: EC2s
Monitoring Scope	Specifies the monitoring scope the alarm rule applies to. You can select Resource groups or Specific resources . NOTE <ul style="list-style-type: none"> • If Resource groups is selected and any resource in the group meets the alarm policy, an alarm is triggered. • If Resource groups is selected, alarm rules cannot be created using templates.
Monitored Object	Specifies the resource the alarm rule is created for. You can specify one or more resources.

- b. In the **Select Metric** step, select **Create manually** and configure parameters based on [Table 5-6](#).

Table 5-6 Parameters

Parameter	Description	Example Value
Method	Specifies the means you use to create the alarm rule.	Configure manually

Parameter	Description	Example Value
Metric	<p>For example:</p> <ul style="list-style-type: none"> • CPU Usage Indicates the CPU usage of the monitored object. The unit is percent. • Memory Usage Indicates the memory usage of the monitored object. The unit is percent. 	CPU Usage
Alarm Policy	<p>Specifies the policy for triggering an alarm.</p> <p>For example, an alarm is triggered if the average value of the monitored metric is 80% or more for three consecutive 5-minute periods.</p>	N/A
Alarm Severity	<p>Specifies the alarm severity, which can be Critical, Major, Minor, or Informational.</p>	Major
Alarm Notification	<p>Specifies whether to notify users when alarms are triggered. Notifications can be sent by email, text message, or HTTP/HTTPS message.</p>	Enable
Notification Object	<p>Specifies the object to which alarm notifications will be sent. You can select the account contact or a topic.</p> <ul style="list-style-type: none"> • 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. 	N/A
Validity Period	<p>Cloud Eye sends notifications only within the validity period specified in the alarm rule.</p> <p>If Validity Period is set to 08:00-20:00, Cloud Eye sends notifications only within 08:00-20:00.</p>	N/A
Trigger Condition	<p>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.</p>	N/A

5.4 Viewing Alarm Records

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

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

Procedure

1. Log in to the management console.
2. Choose **Alarm Management** > **Alarm Records**.

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

NOTE

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

5.5 One-Click Monitoring

Scenarios

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

Constraints

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

Procedure

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

- Click the arrow on the left of the cloud service name to view the built-in alarm rules.

 **NOTE**

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

5.6 Alarm Rule Management

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

5.6.1 Modifying an Alarm Rule

Procedure

- Log in to the management console.
- Click **Service List** in the upper left corner, and select **Cloud Eye**.
- Choose **Alarm Management > Alarm Rules**.
- On the displayed **Alarm Rules** page, use either of the following two methods to modify an alarm rule:
 - Locate the row containing the alarm rule you want to modify, click **Modify** in the **Operation** column.
 - Click the name of the alarm rule you want to modify. On the page displayed, click **Modify** in the upper right corner.
- On the **Modify Alarm Rule** page, modify alarm rule parameters as needed.

Table 5-7 Parameters

Parameter	Description	Example Value
Name	Specifies the alarm rule name. The system generates a random name, which you can modify.	alarm-b6al
Description	(Optional) Provides supplementary information about the alarm rule.	N/A
Resource Type	Specifies the type of the resource the alarm rule is created for.	Elastic Cloud Server
Dimension	Specifies the metric dimension of the selected resource type.	ECSS
Monitoring Scope	Specifies the monitoring scope the alarm rule applies to.	Resource Groups
Group	This parameter is mandatory when Monitoring Scope is set to Resource groups .	N/A

Parameter	Description	Example Value
Method	There are two options: Associate template or Configure manually . NOTE After an associated template is modified, the policies contained in this alarm rule to be created will be modified accordingly.	Configure manually
Monitored Object	Specifies the resource the alarm rule is created for. You can specify one or more resources.	N/A
Monitored Object ID	Specifies the resource ID.	N/A
Metric	For example: <ul style="list-style-type: none">• CPU Usage Indicates the CPU usage of the monitored object in percent.• Memory Usage Indicates the memory usage of the monitored object in percent.	CPU Usage
Alarm Policy	Specifies the policy for triggering an alarm. For example, an alarm is triggered if the average value of the monitored metric is 80% or more for three consecutive 5-minute periods.	N/A
Alarm Severity	Specifies the alarm severity, which can be Critical , Major , Minor , or Informational .	Major
Alarm Notification	Specifies whether to notify users by sending emails or SMS messages, or by sending HTTP/HTTPS messages to servers.	N/A
Trigger Condition	Specifies the condition for triggering the alarm notification. You can select Generated alarm (when an alarm is generated), Cleared alarm (when an alarm is cleared), or both.	N/A

6. Click **OK**.

5.6.2 Disabling Alarm Rules

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

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

5.6.3 Enabling Alarm Rules

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

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

5.6.4 Deleting Alarm Rules

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

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

5.7 Alarm Templates

5.7.1 Viewing Alarm Templates

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

Procedure

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

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

5.7.2 Creating a Custom Template

1. On the **Alarm Templates** page, click **Create Custom Template**.
2. On the **Create Custom Template** page, configure parameters by referring to [Table 5-8](#).

Table 5-8 Parameters

Parameter	Description
Name	Specifies the alarm rule name. The system generates a random name, which you can modify. Example value: alarmTemplate-c6ft
Description	(Optional) Provides supplementary information about the custom template.
Method	You can select Using existing template or Configure manually . <ul style="list-style-type: none">● Using existing template: Select an existing template for Template. The default alarm rules in the template are automatically added.● Configure manually: You can customize alarm policies as required.
Add Resource Type	Specifies the type of the resource the alarm rule is created for. Example value: Elastic Cloud Server
Metric Name	For example: <ul style="list-style-type: none">● CPU Usage Indicates the CPU usage of the monitored object in percent.● Memory Usage Indicates the memory usage of the monitored object in percent.
Alarm Policy	Specifies the policy for triggering an alarm. For example, an alarm is triggered if the average value of the monitored metric is 80% or more for three consecutive 5-minute periods.
Alarm Severity	Specifies the alarm severity, which can be Critical , Major , Minor , or Informational .
Operation	You can copy or delete an added alarm policy.

3. Click **Create**.

5.7.3 Modifying a Custom Template

1. In the navigation pane on the left, choose **Alarm Management > Alarm Templates** and click **Custom Templates**. Locate the template you want to modify and click **Modify** in the **Operation** column.
2. On the **Modify Custom Template** page, modify the configured parameters by referring to [Table 5-8](#).
3. Click **Modify**.

5.7.4 Deleting a Custom Template

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

6 Server Monitoring

6.1 Introduction to Server Monitoring

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

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

NOTE

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

Scenarios

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

Monitoring Capabilities

Server monitoring provides multiple metrics, such as metrics for CPU, memory, disk, and network usage, meeting the basic monitoring and O&M requirements for servers. For details about metrics, see [ECS Metrics](#).

Resource Usage

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

6.2 Agent Installation and Configuration

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

Scenario	Supported Service	Reference
Installing the Agent on a Linux server	ECS	Installing and Configuring the Agent on a Linux ECS
Installing the Agent on a Windows server	ECS	Installing and Configuring the Agent on a Windows ECS

Agent installation and configuration description:

- To successfully install the Agent, ensure that both DNS and security group rules are correctly configured.
- After you install the Agent, you can click **Restore Agent Configurations** on the Cloud Eye console to complete the agency and Agent configuration.
- If the Agent fails to be configured by clicking **Restore Agent Configurations** or due to other reasons, manually configure it.
- For details about the OSs that support the Agent, see [What OSs Does the Agent Support?](#)

6.3 Installing and Configuring the Agent on a Linux ECS

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

Scenarios

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

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

 **NOTE**

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

Modifying the DNS Server Address (Command Lines)

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

To use the management console, see [Modifying the DNS Server Address \(Management Console\)](#).

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

 **NOTE**

`X.X.X.X` indicates the DNS server address. You can obtain it from the administrator.

Modifying the DNS Server Address (Management Console)

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

1. In the upper left corner, select a region and project.
2. Click **Service List** in the upper left corner. Under **Compute**, select **Elastic Cloud Server**.
On the ECS console, click the name of the target ECS to view its details.
3. Click the VPC name on the right of **VPC** to go to the VPC console.
4. In the VPC list, click **vpc-328c**.
5. In the subnet list, click **subnet-328d** and click **Modify**.

In the displayed **Modify Subnet** dialog box, change **DNS Server Address 1** to the correct DNS server IP address.

 **NOTE**

subnet-328d is the ECS subnet.

6. Click **OK**.

 **NOTE**

The new DNS server address takes effect after the ECS 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.

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

- The security group list is displayed.
- Click the security group name.
 - Click **Modify Security Group Rule**.
- The security group details page is displayed.

NOTE

Procedure for BMS:

- Click the security group ID on the upper left.
 - Click **Manage Rule** in the **Operation** column of the security group.
- Click the **Outbound Rules** tab, and click **Add Rule**.
 - Add rules based on [Table 6-1](#).

Table 6-1 Security group rules

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

6.3.2 Installing the Agent on a Linux Server

Scenarios

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

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 as user **root**.
2. Run the following command to install the Agent:

```
cd /usr/local && wget --no-check-certificate https://obs.xx.xx.com/telescope-xx/scripts/agentInstall.sh && chmod 755 agentInstall.sh && ./agentInstall.sh
```

NOTE

The italic part in the command is the address of the Agent package, which can be obtained from the administrator.

Figure 6-1 Successful installation

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

3. Configure the Agent by referring to [Restoring the Agent Configurations on a Linux Server](#) or [\(Optional\) Manually Configuring the Agent \(Linux\)](#).

NOTE

- [Restoring Agent Configurations](#) allows you to configure **AK/SK**, **RegionID**, and **ProjectId** in just a few clicks. You can also modify related configuration files by referring to [\(Optional\) Manually Configuring the Agent \(Linux\)](#).

6.3.3 Restoring the Agent Configurations on a Linux Server

Scenarios

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

 NOTE

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

Restoring the Agent Configurations

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

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

6.3.4 (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.

Prerequisites

The Agent has been installed.

Procedure

1. Log in to an ECS as user **root**.
2. Run the following command to go to the Agent installation path **bin**:
cd /usr/local/uniagent/extension/install/telescope/bin
3. Modify configuration file **conf.json**.
 - a. Run the following command to open **conf.json**:
vi conf.json
 - b. Modify the parameters in the file. For details, see [Table 6-2](#).

ECS parameters

```
{
  "InstanceId": "XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX",
  "ProjectId": "XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX",
  "AccessKey": "XXXXXXXXXXXXXXXXXXXX",
  "SecretKey": "XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX",
  "RegionId": "xx-xx-xx",
  "ClientPort": 0,
  "PortNum": 200
}
```

BMS parameters

```
{
  "InstanceId": "XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX",
  "ProjectId": "XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX",
  "AccessKey": "XXXXXXXXXXXXXXXXXXXX",
  "SecretKey": "XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX",
  "RegionId": "xx-xx-xx",
  "ClientPort": 0,
  "PortNum": 200,
  "BmsFlag": true
}
```

Table 6-2 Public parameters

Parameter	Description
InstanceId	<p>(Optional) Specifies the ECS ID. You can log in to the management console and view the ECS ID in the ECS list.</p> <p>NOTE</p> <p>If you do not configure InstanceId, retain "InstanceId":"".</p> <p>If you configure it, ensure that the following two requirements are met:</p> <ul style="list-style-type: none"> The ECS ID must be unique at all sites, that is, in the same region, InstanceId used by the Agent cannot be the same. Otherwise, errors may occur. The InstanceId value must be consistent with the actual ECS ID. Otherwise, you cannot see the OS monitoring data on Cloud Eye.
ProjectId	<p>(Optional) Specifies the project ID.</p> <p>If you do not configure ProjectId, retain "ProjectId":"".</p> <p>If you configure it, perform the following operations:</p> <ol style="list-style-type: none"> 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 is located.

Parameter	Description
AccessKey / SecretKey	<p>To obtain the AK and SK, perform the following operations:</p> <p>Log in to the Cloud Eye console, click the username in the upper right corner, and choose My Credentials, and choose Access Keys.</p> <ul style="list-style-type: none"> 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. <p>NOTICE</p> <ul style="list-style-type: none"> For security purposes, it is recommended that the user be an IAM user with the CES Administrator permissions only.
RegionId	Specifies the region ID. Contact the administrator to obtain it.
ClientPort	<p>Specifies the start port number used by the Agent.</p> <p>NOTE</p> <p>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.</p>
PortNum	<p>Specifies the number of ports configured for the Agent.</p> <p>NOTE</p> <p>The default value is 200. If ClientPort is 5000, the port range will be 5000 to 5199.</p>

4. Modify configuration file **conf_ces.json** for the Cloud Eye metric collection module.
 - a. Run the following command to open public configuration file **conf_ces.json**:
vi conf_ces.json
 - b. Modify the endpoint in **conf_ces.json**, and save the **conf_ces.json** file. For details, see [Table 6-3](#).

```
{
  "Endpoint": "https://ces.xx-xx-xx.xxx.com"
}
```

Table 6-3 Parameter setting of the metric collection module

Parameter	Description
Endpoint	Specifies the Cloud Eye URL in the region the ECS belongs to. Contact the administrator to obtain it.

 NOTE

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

6.4 Installing and Configuring the Agent on a Windows ECS

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

Scenarios

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

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

 NOTE

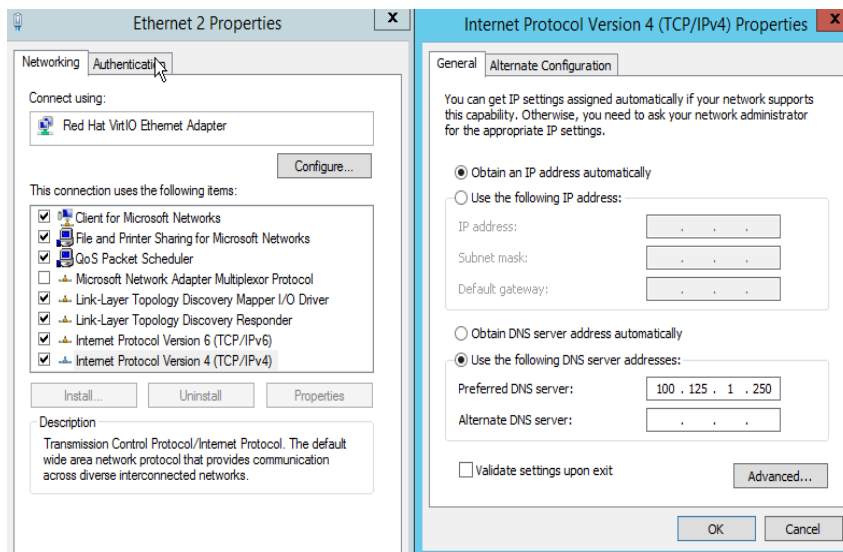
DNS and security group configuration are intended for the primary NIC.

Modifying the DNS Server Address (Windows GUI)

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

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

Figure 6-2 Adding the DNS server address (Windows)



NOTE

100.125.1.250 is an example. For DNS details, contact the administrator.

Modifying the ECS Security Group Rules (Management Console)

The following describes how to modify security group rules for an ECS on the management console.

1. On the ECS details page, click the **Security Groups** tab.
The security group list is displayed.
2. Click the security group name.
3. Click **Modify Security Group Rule**.
The security group details page is displayed.

NOTE

Procedure for BMS:

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

Table 6-4 Security group rules

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

6.4.2 Installing and Configuring the Agent on a Windows Server

Scenarios

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

Constraints

The Agent cannot be installed on Windows BMSs.

Prerequisites

- You have performed operations described in [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.
- The Agent installation package (Windows) has been obtained from the administrator.

Procedure

1. Log in to the Windows ECS as an administrator.

2. Open a browser, and enter the address of the Agent installation package in the address box to download and save the installation package.
3. Create a directory for storing the installation package (for example, **D:\Agent**) and decompress the package to this directory.
4. Double-click the **install.bat** script to install and start the Agent.
If **Install service success** is displayed, the Agent is successfully installed and started.

NOTE

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

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

The Agent configuration is completed.

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

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

Scenarios

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

Constraints

The Agent cannot be installed on Windows BMSs.

Prerequisites

The Agent has been installed.

Procedure

1. Log in to the ECS.
2. Open the **conf.json** file in the **telescope_windows_amd64\bin** directory.
3. Configure the following parameters. For details, see [Table 6-5](#).

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

Table 6-5 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: <ul style="list-style-type: none">• The ECS ID must be unique at all sites, that is, in the same region, InstanceId used by the Agent cannot be the same. Otherwise, errors may occur.• The InstanceId value must be consistent with the actual ECS ID. Otherwise, you cannot see the OS monitoring data on Cloud Eye.
ProjectId	Specifies the project ID. You do not need to configure ProjectId . Retain " ProjectId ":"". If you wish to configure it, perform the following operations: <ol style="list-style-type: none">1. Log in to the Cloud Eye console, click the username in the upper right corner, and choose My Credentials.2. Under Projects, obtain the project ID for the region where the ECS is located.
AccessKey/ SecretKey	To obtain the AK and SK, perform the following operations: Log in to the Cloud Eye console, click the username in the upper right corner, and choose My Credentials , and choose Access Keys . <ul style="list-style-type: none">• 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.
RegionId	Specifies the region ID. Contact the administrator to obtain it.
ClientPort	Specifies the start port number used by the Agent. NOTE The default value is 0 , indicating that the Agent will randomly use any port. Ports 1 to 1023 are reserved. You are advised not to specify a port in this range for the Agent.
PortNum	Specifies the number of ports configured for the Agent. NOTE The default value is 200 . If ClientPort is 5000 , the port range will be 5000 to 5199.

4. Wait for a few minutes.

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

6.5 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](#) to ensure that data collection is normal. Use the ECS as a jump server and run scripts in batches to copy, decompress, and install the Agent package and configuration file to other ECSs.

NOTICE

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

Prerequisites

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

NOTE

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

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

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

Procedure

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

```
cd /usr/local && wget http://obs.xx-xx-xx.xx.com/telescope-xx-xx-xx/scripts/agentBatchPackage.sh && chmod 755 agentBatchPackage.sh && ./agentBatchPackage.sh
```

NOTE

The italic part in the command is an example. Contact the administrator to obtain the address of the Agent package.

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

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

NOTICE

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

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

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

 **NOTE**

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

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

```
cd /usr/lib/python2.7/site-packages
rm pexpect-3.2-py2.7.egg-info -f
rm ptyprocess-0.5.2-py2.7.egg-info -f
rm pexpect -rf
rm ptyprocess -rf
```

6.6 Managing the Agent

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

6.6.1 Managing the Agent (Linux)

 **NOTE**

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

Checking the Agent Status

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

```
service telescoped status
```

The following message indicates that the Agent is running properly:

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

Starting the Agent

```
/usr/local/telescope/telescoped start
```

Restarting the Agent

```
/usr/local/telescope/telescoped restart
```

Stopping the Agent

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

```
service telescoped stop
```

NOTE

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

```
/usr/local/telescope/telescoped stop
```

Uninstalling the Agent

Run the following command to uninstall the Agent:

```
/usr/local/telescope/uninstall.sh
```

NOTICE

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

6.6.2 Managing the Agent (Windows)

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

Checking the Agent Status

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

Starting the Agent

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

Stopping the Agent

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

Uninstalling the Agent

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

NOTICE

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

6.7 Process Monitoring

6.7.1 Viewing Process Monitoring

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

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

NOTE

To view the process monitoring information, install the Agent.

Querying the System Processes

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

To query the number of processes

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

NOTE

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

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

In the **System Processes** area, the process information is displayed. [Table 6-6](#) describes the metrics of system processes.

Table 6-6 System process metrics

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

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


Viewing the Running Data of Top CPU Processes

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

NOTE

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

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

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

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


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

You can click **CPU Usage**, **Memory Usage**, or **Open Files** above the graph to view the curves of different metrics of the currently displayed process. [Table 6-7](#) lists **Process Monitoring** metrics.

Table 6-7 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.

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

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

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

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

6.8 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 about basic monitoring metrics, see [ECS Metrics](#).

For details about OS monitoring metrics, see [OS Monitoring Metrics Supported by ECSs with the Agent Installed](#).

Prerequisites

You have installed the Agent. For details, see [Installing and Configuring the Agent on a Linux ECS](#) and [Installing and Configuring the Agent on a Windows Server](#).


Procedure

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

4. View metrics.

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

View metric graphs based on raw data from the last 1 hour, last 3 hours, last 12 hours, last 1 day, last 7 days, or last 30 days. Cloud Eye provides the **Auto Refresh** function at 60-second intervals.

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

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

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

6.9 Creating an Alarm Rule to Monitor a Server

Scenarios

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

Procedure

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

Table 6-8 Alarm rule Name and Description

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

- b. You do not need to set the monitored object because it is the current ECS.
- c. In the **Select Metric** step, select **Create manually** and configure parameters based on [Table 6-9](#).

Table 6-9 Parameters

Parameter	Description	Example Value
Method	Specifies the means you use to create the alarm rule.	Create manually
Metric	For details about basic monitoring metrics, see ECS Metrics . For details about OS monitoring metrics, see OS Monitoring Metrics Supported by ECSs with the Agent Installed .	N/A

Parameter	Description	Example Value
Mount Point or Disk	This parameter is mandatory when the metric is a fine-grained disk metric. For the Windows OS, enter a drive letter, such as C , D , or E . For the Linux OS, enter a mount point, such as /dev or /opt .	/dev
Alarm Policy	Specifies the policy for triggering an alarm. For example, an alarm is triggered if the average value of the monitored metric is 80% or more for three consecutive 5-minute periods.	N/A
Alarm Severity	Specifies the alarm severity, which can be Critical , Major , Minor , or Informational .	Major
Alarm Notification	Specifies whether to notify users 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
Topic	Specifies the name of the topic the alarm notification is to be sent to. If you have enabled Alarm Notification , select a topic. If no desirable topics are available, create one first, whereupon the SMN service is invoked. For details about how to create a topic, see the <i>Simple Message Notification User Guide</i> .	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

d. Click **Create**.

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

7 Custom Monitoring

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

Viewing Custom Monitoring

1. Log in to the management console.
2. Click **Service List** in the upper left corner, and select **Cloud Eye**.
3. In the navigation pane on the left, choose **Custom Monitoring**.
4. On the **Custom Monitoring** page, view the data reported by yourself through API requests, including custom services and metrics.

NOTE

Only after you add monitoring data through APIs, will those data be displayed on the Cloud Eye console. For details about how to add monitoring data, see section "Adding Monitoring Data" in *Cloud Eye API Reference*.

5. Locate the row that contains the cloud resource to be viewed, and click **View Graph**.

On the page displayed, you can view graphs based on raw data collected in **1h**, **3h**, **12h**, **1d**, and **7d**. In the upper right corner of each graph, the maximum and minimum values of the metric in the corresponding time periods are dynamically displayed.

Creating an Alarm Rule

1. Log in to the management console.
2. Click **Service List** in the upper left corner, and select **Cloud Eye**.
3. In the navigation pane on the left, choose **Custom Monitoring**.
4. On the **Custom Monitoring** page, locate the target resource and click **Create Alarm Rule** in the **Operation** column.
5. On the **Create Alarm Rule** page, follow the prompts to configure the parameters. For details, see [Table 5-6](#).
6. Click **Create**.

8 Event Monitoring

8.1 Introduction to Event Monitoring

In event monitoring, you can query system events that are automatically reported to Cloud Eye and custom events reported to Cloud Eye through the API. You can create alarm rules for both system events and custom events. When specific events occur, Cloud Eye generates alarms for you. Event monitoring does not depend on the Agent.

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

Event monitoring is enabled by default. For details, see [Events Supported by Event Monitoring](#).

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

8.2 Viewing Event Monitoring Data

Scenarios

This topic describes how to view the event monitoring data.

Procedure

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

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

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

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

8.3 Creating an Alarm Rule to Monitor an Event

Scenarios

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

Procedure

- Log in to the management console.
- Click **Service List** in the upper left corner, and select **Cloud Eye**.
- In the navigation pane on the left, choose **Event Monitoring**.
- On the event list page, click **Create Alarm Rule** in the upper right corner.
- Follow the prompts to configure the following parameters.

Table 8-1 Parameters

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
Event Name	Specifies the operations on system resources performed by users, such as login and logout. For events supported by event monitoring, see Events Supported by Event Monitoring . Example value: Start auto recovery
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 Policy	Specifies the policy for triggering an alarm. For example, an alarm is triggered if the event occurred for three consecutive periods of 5 minutes. NOTE This parameter is mandatory when Triggering Mode is set to Accumulative Trigger .

Parameter	Description
Alarm Severity	Specifies the alarm severity, which can be Critical , Major , Minor , or Informational . Example value: Major
Alarm Notification	Specifies whether to notify users when alarms are triggered. Notifications can be sent by email, text message, or HTTP/HTTPS message.
Topic	Specifies the name of the topic the alarm notification is to be sent to. If you enable this function, select a topic. If the required topic is unavailable, create one first. For details about how to create a topic, see the <i>Simple Message Notification User Guide</i> .
Trigger Condition	If you enable Alarm Notification , Generated alarm is mandatory for Trigger Condition . Example value: Generated alarm

- In the **Specify Rule Name** step, configure the parameters. Click **Finish**.

Table 8-2 Parameter description

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

8.4 Events Supported by Event Monitoring

Table 8-3 Elastic Cloud Server (ECS)

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
ECS	ECS restarted	rebootServer	Minor	The ECS was restarted <ul style="list-style-type: none"> on the management console. by calling APIs. 	Check whether the restart was performed intentionally by a user. <ul style="list-style-type: none"> Deploy service applications in HA mode. After the ECS starts up, check whether services recover. 	Services are interrupted.
	Restart triggered due to hardware fault	startAutoRecovery	Major	ECSs on a faulty host would be automatically migrated to another properly-running host. During the migration, the ECSs was restarted.	Wait for the event to end and check whether services are affected.	Services may be interrupted.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Restart completed due to hardware failure	endAutoRecovery	Major	The ECS was restored to be normal after the automatic migration.	This event indicates that the ECS has recovered and been working properly.	None
	Auto recovery timeout (being processed on the backend)	faultAutoRecovery	Major	Migrating the ECS to a normal host timed out.	Migrate services to other ECSs.	Services are interrupted.
	Startup failure	faultPowerOn	Major	The ECS failed to start.	Start the ECS again. If the problem persists, contact O&M personnel.	The ECS cannot start.
	GPU link fault	GPULinkFault	Critical	The GPU of the host running the ECS was faulty or was recovering from a fault.	Deploy service applications in HA mode. After the GPU fault is rectified, check whether services are restored.	Services are interrupted.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	FPGA link fault	FPGALinkFault	Critical	The FPGA of the host running the ECS was faulty or was recovering from a fault.	Deploy service applications in HA mode. After the FPGA fault is rectified, check whether services are restored.	Services are interrupted.
	Improper ECS running	vmIsRunningImproperly	Major	The ECS was faulty or the ECS NIC was abnormal.	Deploy service applications in HA mode. After the fault is rectified, check whether services recover.	Services are interrupted.
	Improper ECS running recovered	vmIsRunningImproperlyRecovery	Major	The ECS was restored to the normal status.	Wait for the ECS status to become normal and check whether services are affected.	None
	VM faults caused by host process exceptions	VMFaultsByHostProcessExceptions	Critical	The processes of the host accommodating the ECS were abnormal.	Contact O&M personnel.	The ECS is faulty.

 NOTE

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

Table 8-4 Cloud Backup and Recovery (CBR)

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
CBR	Failed to create the backup.	backupFailed	Critical	The backup failed to be created.	Manually create a backup or contact customer service.	Data loss may occur.
	Failed to restore the resource using a backup.	restoreFailed	Critical	The resource failed to be restored using a backup.	Restore the resource using another backup or contact customer service.	Data loss may occur.
	Failed to delete the backup.	backupDeleteFailed	Critical	The backup failed to be deleted.	Try again later or contact customer service.	Charging may be abnormal.
	Failed to delete the vault.	vaultDeleteFailed	Critical	The vault failed to be deleted.	Try again later or contact technical support.	Charging may be abnormal.
	Replication failure	replicationFailed	Critical	The backup failed to be replicated.	Try again later or contact technical support.	Data loss may occur.
	The backup is created successfully.	backupSucceeded	Major	The backup was created.	None	None

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Resource restoration using a backup succeeded.	restorationSucceeded	Major	The resource was restored using a backup.	Check whether the data is successfully restored.	None
	The backup is deleted successfully.	backupDeletionSucceeded	Major	The backup was deleted.	None	None
	The vault is deleted successfully.	vaultDeletionSucceeded	Major	The vault was deleted.	None	None
	Replication success	replicationSucceeded	Major	The backup was replicated successfully.	None	None
	Client offline	agentOffline	Critical	The backup client was offline.	Ensure that the Agent status is normal and the backup client can be connected to .	Backup tasks may fail.
	Client online	agentOnline	Major	The backup client was online.	None	None

9 Cloud Service Monitoring

9.1 Introduction to Cloud Service Monitoring

Scenarios

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


What You Can Do with Cloud Service Monitoring

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


9.2 Viewing Metrics

1. Log in to the management console.
2. Click **Service List** in the upper left corner, and select **Cloud Eye**.
3. In the navigation pane on the left, choose **Cloud Service Monitoring** and select the cloud service whose resources you want to view.
4. Locate the target cloud service resource, in the **Operation** column, click **View Metric**.

 NOTE

- You can sort graphs by dragging them based on service requirements.
 - If **Auto Refresh** is enabled, data is automatically refreshed every minute.
 - Some cloud services allow you to view resource details. You can click **View Resource Details** in the upper part of the page to view details about monitored resources.
 - You can search for a specific metric in the search box.
5. Hover your mouse over a graph. In the upper right corner, click  to view monitoring details on an enlarged graph. You can select a time period or customize a time range to view the metric trend in a specific monitoring interval.

 NOTE

- If you select **1h**, **3h**, **12h**, or **1d**, raw data is displayed by default. You can set **Period** and **Statistic** to change the rollup period of monitoring data. For details about rollup periods, see [What Is Rollup?](#)
 - If you select **7d** or **30d**, aggregated data is displayed by default. Near the top left corner of the page, you can click **Settings** to change the rollup period of the monitoring data.
6. In the upper right corner of the monitoring graph, click  to create alarm rules for the metric. For details about the parameters, see [Creating an Alarm Rule by Using an Alarm Template](#).

10 Permissions Management

10.1 Creating a User and Granting Permissions

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

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

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

This topic describes the procedure for granting permissions (see [Figure 10-1](#)).

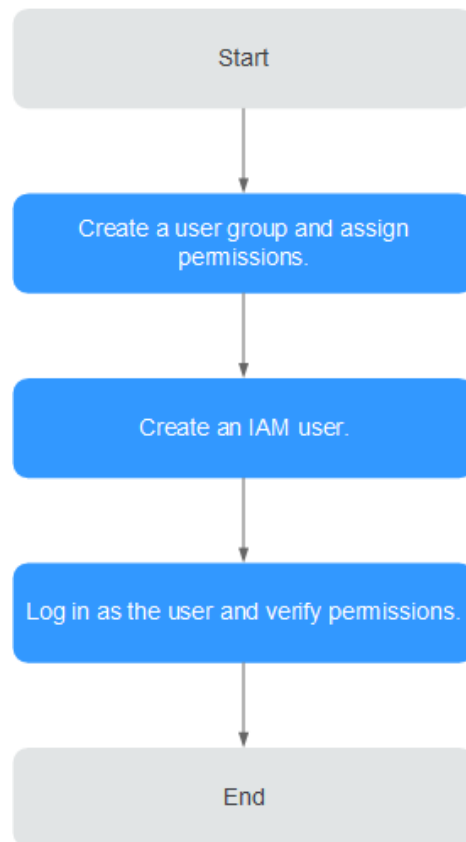
Prerequisites

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

For details about the system policies supported by Cloud Eye and the comparison between these policies, see [Permissions](#).

Process Flow

Figure 10-1 Process for granting Cloud Eye permissions



1. Create a user group and assign permissions.

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

NOTE

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

10.2 Cloud Eye Custom Policies

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

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

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

For details, see section "Creating a Custom Policy" in *Identity and Access Management User Guide*. 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 create, modify, query, and delete 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"
    }
  ]
}
```


11 Quota Adjustment

What Is Quota?

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

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

How Do I View My Quotas?

1. Log in to the management console.
2. In the upper right corner of the page, click  .
The **Service Quota** page is displayed.
3. 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?

The system does not support online quota adjustment. If you need to adjust a quota, contact the operations administrator.

Before contacting the operations administrator, make sure that the following information has been obtained:

- Account name, which can be obtained by performing the following operations:
Log in to the management console using the cloud account, click the username in the upper right corner, select **My Credentials** from the drop-down list, and obtain the account name on the **My Credentials** page.
- Quota information, which includes service name, quota type, and required quota

12 Services Interconnected with Cloud Eye

12.1 Computing

12.1.1 ECS Metrics

You do not need to install the Agent for the basic monitoring metrics of ECSs. You can view the basic monitoring metrics after you have created ECSs and the ECSs have been running for several minutes.

Basic monitoring metric data is reported every 5 minutes.

ECS metrics vary depending on ECS OSs and types. For details, see [Table 12-1](#). ✓ indicates that the metric is supported, and x indicates that the metric is not supported.

Table 12-1 Supported ECS metrics

Metric	Windows ECS	Linux ECS
CPU Usage	✓	✓
Memory Usage	✓	x
Disk Usage	✓	x
Disk Read Bandwidth	✓	✓
Disk Write Bandwidth	✓	✓
Disk Read IOPS	✓	✓
Disk Write IOPS	✓	✓
Inband Incoming Rate	✓	x
Inband Outgoing Rate	✓	x

Metric	Windows ECS	Linux ECS
Outband Incoming Rate	√	√
Outband Outgoing Rate	√	√

 NOTE

[Table 12-2](#) describes these ECS metrics.

Table 12-2 Basic metric description

Metric ID	Parameter	Description	Value Range	Monitored Object & Dimension	Monitoring Interval (Raw Metrics and KVM Only)
cpu_util	CPU Usage	CPU usage of an ECS Unit: Percent Formula: CPU usage of an ECS/Number of vCPUs in the ECS	≥ 0	ECS	5 minutes
mem_util	Memory Usage	Memory usage of an ECS This metric is unavailable if the image has no UVP VMTools installed. Unit: Percent Formula: Used memory of an ECS/ Total memory of the ECS NOTE The memory usage of QingTian ECSs cannot be monitored.	≥ 0	ECS	5 minutes

Metric ID	Parameter	Description	Value Range	Monitored Object & Dimension	Monitoring Interval (Raw Metrics and KVM Only)
disk_util_inband	Disk Usage	Disk usage of an ECS This metric is unavailable if the image has no UVP VMTools installed. Unit: Percent Formula: Used capacity of an ECS-attached disk/Total capacity of the ECS-attached disk	≥ 0	ECS	5 minutes
disk_read_bytes_rate	Disk Read Bandwidth	Number of bytes read from an ECS-attached disk per second Unit: byte/s Formula: Total number of bytes read from an ECS-attached disk/ Monitoring interval $\text{byte_out} = (\text{rd_bytes} - \text{last_rd_bytes})/\text{Time difference}$	≥ 0	ECS	5 minutes
disk_write_bytes_rate	Disk Write Bandwidth	Number of bytes written to an ECS-attached disk per second Unit: byte/s Formula: Total number of bytes written to an ECS-attached disk/ Monitoring interval	≥ 0	ECS	5 minutes

Metric ID	Parameter	Description	Value Range	Monitored Object & Dimension	Monitoring Interval (Raw Metrics and KVM Only)
disk_read_requests_rate	Disk Read IOPS	Number of read requests sent to an ECS-attached disk per second Unit: request/s Formula: Total number of read requests sent to an ECS-attached disk/ Monitoring interval $req_out = (rd_req - last_rd_req) / \text{Time difference}$	≥ 0	ECS	5 minutes
disk_write_requests_rate	Disk Write IOPS	Number of write requests sent to an ECS-attached disk per second Unit: request/s Formula: Total number of write requests sent to an ECS-attached disk/ Monitoring interval $req_in = (wr_req - last_wr_req) / \text{Time difference}$	≥ 0	ECS	5 minutes
network_incoming_bytes_rate_inband	Inband Incoming Rate	Number of incoming bytes on an ECS per second Unit: byte/s Formula: Total number of inband incoming bytes on an ECS/ Monitoring interval	≥ 0	ECS	5 minutes

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

12.1.2 OS Monitoring Metrics Supported by ECSs with the Agent Installed

After [installing the Agent](#) on an ECS, you can view its OS monitoring metrics. Monitoring data is collected every 1 minute.

CPU, CPU load, memory, disk, disk I/O, file system, and NIC metrics can be monitored.

Table 12-3 CPU metrics

Metric	Metric	Metric Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
cpu_usage_idle	(Agent) Idle CPU Usage	Percentage of time that CPU is idle Unit: Percent <ul style="list-style-type: none"> Linux: Check the metric value changes in file /proc/stat in a collection period. Windows: Run the top command to check the %Cpu(s) id value. 	0-100%	ECSs	1 minute
cpu_usage_other	(Agent) Other Process CPU Usage	Percentage of time that the CPU is used by other processes Unit: Percent <ul style="list-style-type: none"> Linux: Other Process CPU Usage = 1 - Idle CPU Usage - Kernel Space CPU Usage - User Space CPU Usage Windows: Other Process CPU Usage = 1 - Idle CPU Usage - Kernel Space CPU Usage - User Space CPU Usage 	0-100%	ECSs	1 minute
cpu_usage_system	(Agent) Kernel Space CPU Usage	Percentage of time that the CPU is used by kernel space Unit: Percent <ul style="list-style-type: none"> Linux: Check the metric value changes in file /proc/stat in a collection period. Run the top command to check the %Cpu(s) sy value. Windows: Obtain the metric value using the Windows API GetSystemTimes. 	0-100%	ECSs	1 minute

Metric	Metric	Metric Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
cpu_usage_user	(Agent) User Space CPU Usage	Percentage of time that the CPU is used by user space Unit: Percent <ul style="list-style-type: none"> Linux: Check the metric value changes in file /proc/stat in a collection period. Run the top command to check the %Cpu(s) us value. Windows: Obtain the metric value using the Windows API GetSystemTimes. 	0-100%	ECSs	1 minute
cpu_usage	(Agent) CPU Usage	CPU usage of the monitored object Unit: Percent <ul style="list-style-type: none"> Linux: Check the metric value changes in file /proc/stat in a collection period. Run the top command to check the %Cpu(s) value. Windows: Obtain the metric value using the Windows API GetSystemTimes. 	0-100%	ECSs	1 minute
cpu_usage_nice	(Agent) Nice Process CPU Usage	Percentage of time that the CPU is in user mode with low-priority processes which can easily be interrupted by higher-priority processes Unit: Percent <ul style="list-style-type: none"> Linux: Check the metric value changes in file /proc/stat in a collection period. Run the top command to check the %Cpu(s) ni value. Windows is not supported. 	0-100%	ECSs	1 minute

Metric	Metric	Metric Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
cpu_usage_iowait	(Agent) iowait Process CPU Usage	Percentage of time that the CPU is waiting for I/O operations to complete Unit: Percent <ul style="list-style-type: none"> Linux: Check the metric value changes in file /proc/stat in a collection period. Run the top command to check the %Cpu(s) wa value. Windows is not supported. 	0-100%	ECSs	1 minute
cpu_usage_irq	(Agent) CPU Interrupt Time	Percentage of time that the CPU is servicing interrupts Unit: Percent <ul style="list-style-type: none"> Linux: Check the metric value changes in file /proc/stat in a collection period. Run the top command to check the %Cpu(s) hi value. Windows is not supported. 	0-100%	ECSs	1 minute
cpu_usage_softirq	(Agent) CPU Software Interrupt Time	Percentage of time that the CPU is servicing software interrupts Unit: Percent <ul style="list-style-type: none"> Linux: Check the metric value changes in file /proc/stat in a collection period. Run the top command to check the %Cpu(s) si value. Windows is not supported. 	0-100%	ECSs	1 minute

Table 12-4 CPU load metrics

Metric	Metric	Metric Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
load_average1	(Agent) 1-Minute Load Average	CPU load averaged from the last 1 minute Linux: Obtain the metric value from the number of logic CPUs in load1/ in file /proc/loadavg . Run the top command to check the load1 value.	≥0	ECSs	1 minute
load_average5	(Agent) 5-Minute Load Average	CPU load averaged from the last 5 minutes Linux: Obtain the metric value from the number of logic CPUs in load5/ in file /proc/loadavg . Run the top command to check the load5 value.	≥0	ECSs	1 minute
load_average15	(Agent) 15-Minute Load Average	CPU load averaged from the last 15 minutes Linux: Obtain the metric value from the number of logic CPUs in load15/ in file /proc/loadavg . Run the top command to check the load15 value.	≥0	ECSs	1 minute

 **NOTE**

The Windows OS does not support the CPU load metrics.

Table 12-5 Memory metrics

Metric	Metric	Metric Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
mem_available	(Agent) Available Memory	Amount of memory that is available and can be given instantly to processes Unit: GB <ul style="list-style-type: none"> Linux: Obtain the metric value from MemAvailable in file /proc/meminfo. If MemAvailable is not available in /proc/meminfo, it equals to MemFree+Buffers+Cached. Windows: It is calculated by available memory minuses used memory. The value is obtained by calling the Windows API <code>GlobalMemoryStatusEx</code>. 	≥ 0 GB	ECS	1 minute
mem_usedPercent	(Agent) Memory Usage	Memory usage of the instance Unit: Percent <ul style="list-style-type: none"> Linux: Obtain the metric value from the /proc/meminfo file (MemTotal-MemAvailable)/MemTotal. Windows: The calculation formula is as follows: Used memory size/Total memory size*100%. 	0-100%	ECS	1 minute
mem_free	(Agent) Idle Memory	Amount of memory that is not being used Unit: GB <ul style="list-style-type: none"> Linux: Obtain the metric value from /proc/meminfo. Windows is not supported. 	≥ 0 GB	ECS	1 minute

Metric	Metric	Metric Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
mem_buffers	(Agent) Buffer	<p>Amount of memory that is being used for buffers</p> <p>Unit: GB</p> <ul style="list-style-type: none"> Linux: Obtain the metric value from /proc/meminfo. Run the top command to check the KiB Mem:buffers value. Windows is not supported. 	≥ 0 GB	ECS	1 minute
mem_cached	(Agent) Cache	<p>Amount of memory that is being used for file caches</p> <p>Unit: GB</p> <ul style="list-style-type: none"> Linux: Obtain the metric value from /proc/meminfo. Run the top command to check the KiB Swap:cached Mem value. Windows is not supported. 	≥ 0 GB	ECS	1 minute

Table 12-6 Disk metrics

Metric	Metric	Metric Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
mountPointPrefix_disk_free	(Agent) Available Disk Space	<p>Free space on the disks Unit: GB</p> <ul style="list-style-type: none"> Linux: Run the df -h command to check the value in the Avail column. The path of the mount point prefix cannot exceed 64 characters. It must start with a letter, and contain only digits, letters, hyphens (-), periods (.), and swung dashes (~). Windows: Use the WMI interface to call GetDiskFreeSpaceExW API to obtain disk space data. The path of the mount point prefix cannot exceed 64 characters. It must start with a letter, and contain only digits, letters, hyphens (-), periods (.), and swung dashes (~). 	≥ 0 GB	ECSs	1 minute

Metric	Metric	Metric Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
mountPointPrefix_disk_total	(Agent) Disk Storage Capacity	<p>Total space on the disks, including used and free</p> <p>Unit: GB</p> <ul style="list-style-type: none"> Linux: Run the df -h command to check the value in the Size column. The path of the mount point prefix cannot exceed 64 characters. It must start with a letter, and contain only digits, lowercase letters, uppercase letters, hyphens (-), periods (.), and swung dashes (~). Windows: Use the WMI interface to call GetDiskFreeSpaceExW API to obtain disk space data. The path of the mount point prefix cannot exceed 64 characters. It must start with a letter, and contain only digits, letters, hyphens (-), periods (.), and swung dashes (~). 	≥ 0 GB	ECSs	1 minute

Metric	Metric	Metric Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
mountPointPrefix_disk_used	(Agent) Used Disk Space	<p>Used space on the disks Unit: GB</p> <ul style="list-style-type: none"> Linux: Run the df -h command to check the value in the Used column. The path of the mount point prefix cannot exceed 64 characters. It must start with a letter, and contain only digits, letters, hyphens (-), periods (.), and swung dashes (~). Windows: Use the WMI interface to call GetDiskFreeSpaceExW API to obtain disk space data. The path of the mount point prefix cannot exceed 64 characters. It must start with a letter, and contain only digits, letters, hyphens (-), periods (.), and swung dashes (~). 	≥ 0 GB	ECSs	1 minute

Metric	Metric	Metric Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
mountPointPrefix_disk_used_Percent	(Agent) Disk Usage	<p>Percentage of total disk space that is used. It is calculated as follows: Disk Usage = Used Disk Space/Disk Storage Capacity.</p> <p>Unit: Percent</p> <ul style="list-style-type: none"> Linux: It is calculated as follows: Used/Size. The path of the mount point prefix cannot exceed 64 characters. It must start with a letter, and contain only digits, letters, hyphens (-), periods (.), and swung dashes (~). Windows: Use the WMI interface to call GetDiskFreeSpaceExW API to obtain disk space data. The path of the mount point prefix cannot exceed 64 characters. It must start with a letter, and contain only digits, letters, hyphens (-), periods (.), and swung dashes (~). 	0-100%	ECSs	1 minute

Table 12-7 Disk I/O metrics

Metric	Metric	Metric Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
mountPointPrefix_disk_agt_read_bytes_rate	(Agent) Disks Read Rate	<p>Volume of data read from the instance per second</p> <p>Unit: byte/s</p> <ul style="list-style-type: none"> Linux: <p>The disk read rate is calculated by calculating the data changes in the sixth column of the corresponding device in file /proc/diskstats in a collection period.</p> <p>The path of the mount point prefix cannot exceed 64 characters. It must start with a letter, and contain only digits, letters, hyphens (-), periods (.), and swung dashes (~).</p> Windows: <ul style="list-style-type: none"> - Use Win32_PerfFormattedData_PerfDisk_LogicalDisk object in the WMI to obtain disk I/O data. - The path of the mount point prefix cannot exceed 64 characters. It must start with a letter, and contain only digits, letters, hyphens (-), periods (.), and swung dashes (~). - When the CPU usage is high, monitoring data obtaining timeout may occur and result in the failure of obtaining monitoring data. 	≥ 0 byte/s	ECS	1 minute

Metric	Metric	Metric Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
mountPointPrefix_disk_agt_read_requests_rate	(Agent) Disks Read Requests	<p>Number of read requests sent to the monitored disk per second</p> <p>Unit: Request/s</p> <ul style="list-style-type: none"> • Linux: <p>The disk read requests are calculated by calculating the data changes in the fourth column of the corresponding device in file /proc/diskstats in a collection period.</p> <p>The path of the mount point prefix cannot exceed 64 characters. It must start with a letter, and contain only digits, letters, hyphens (-), periods (.), and swung dashes (~).</p> • Windows: <ul style="list-style-type: none"> - Use Win32_PerfFormattedData_PerfDisk_LogicalDisk object in the WMI to obtain disk I/O data. - The path of the mount point prefix cannot exceed 64 characters. It must start with a letter, and contain only digits, letters, hyphens (-), periods (.), and swung dashes (~). - When the CPU usage is high, monitoring data obtaining timeout may occur and result in the failure of obtaining monitoring data. 	≥ 0 Request/s	ECS	1 minute

Metric	Metric	Metric Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
mountPointPrefix_disk_agent_write_bytes_rate	(Agent) Disks Write Rate	<p>Volume of data written to the instance per second Unit: byte/s</p> <ul style="list-style-type: none"> • Linux: The disk write rate is calculated by calculating the data changes in the tenth column of the corresponding device in file /proc/diskstats in a collection period. The path of the mount point prefix cannot exceed 64 characters. It must start with a letter, and contain only digits, letters, hyphens (-), periods (.), and swung dashes (~). • Windows: <ul style="list-style-type: none"> - Use Win32_PerfFormattedData_PerfDisk_LogicalDisk object in the WMI to obtain disk I/O data. - The path of the mount point prefix cannot exceed 64 characters. It must start with a letter, and contain only digits, letters, hyphens (-), periods (.), and swung dashes (~). - When the CPU usage is high, monitoring data obtaining timeout may occur and result in the failure of obtaining monitoring data. 	≥ 0 byte/s	ECS	1 minute

Metric	Metric	Metric Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
mountPointPrefix_disk_agt_write_requests_rate	(Agent) Disks Write Requests	<p>Number of write requests sent to the monitored disk per second</p> <p>Unit: Request/s</p> <ul style="list-style-type: none"> • Linux: <p>The disk write requests are calculated by calculating the data changes in the eighth column of the corresponding device in file /proc/diskstats in a collection period.</p> <p>The path of the mount point prefix cannot exceed 64 characters. It must start with a letter, and contain only digits, letters, hyphens (-), periods (.), and swung dashes (~).</p> • Windows: <ul style="list-style-type: none"> - Use Win32_PerfFormattedData_PerfDisk_LogicalDisk object in the WMI to obtain disk I/O data. - The path of the mount point prefix cannot exceed 64 characters. It must start with a letter, and contain only digits, letters, hyphens (-), periods (.), and swung dashes (~). - When the CPU usage is high, monitoring data obtaining timeout may occur and result in the failure of obtaining monitoring data. 	≥ 0 Request/s	ECS	1 minute

Metric	Metric	Metric Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
disk_readTime	(Agent) Average Read Request Time	<p>Average amount of time that read requests have waited on the disks</p> <p>Unit: ms/count</p> <ul style="list-style-type: none"> Linux: The average read request time is calculated by calculating the data changes in the seventh column of the corresponding device in file /proc/diskstats in a collection period. The path of the mount point prefix cannot exceed 64 characters. It must start with a letter, and contain only digits, letters, hyphens (-), periods (.), and swung dashes (~). Windows is not supported. 	≥ 0 ms/count	ECS	1 minute
disk_writeTime	(Agent) Average Write Request Time	<p>Average amount of time that write requests have waited on the disks</p> <p>Unit: ms/count</p> <ul style="list-style-type: none"> Linux: The average write request time is calculated by calculating the data changes in the eleventh column of the corresponding device in file /proc/diskstats in a collection period. The path of the mount point prefix cannot exceed 64 characters. It must start with a letter, and contain only digits, letters, hyphens (-), periods (.), and swung dashes (~). Windows is not supported. 	≥ 0 ms/count	ECS	1 minute

Metric	Metric	Metric Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
disk_io Utils	(Agent) Disk I/O Usage	<p>Percentage of the time that the disk has had I/O requests queued to the total disk operation time</p> <p>Unit: Percent</p> <ul style="list-style-type: none"> Linux: The disk I/O usage is calculated by calculating the data changes in the thirteenth column of the corresponding device in file /proc/diskstats in a collection period. <p>The path of the mount point prefix cannot exceed 64 characters. It must start with a letter, and contain only digits, letters, hyphens (-), periods (.), and swung dashes (~).</p> Windows is not supported. 	0-100%	ECS	1 minute
disk_queue_length	(Agent) Disk Queue Length	<p>Average number of read or write requests queued up for completion for the monitored disk in the monitoring period</p> <p>Unit: Count</p> <ul style="list-style-type: none"> Linux: The average disk queue length is calculated by calculating the data changes in the fourteenth column of the corresponding device in file /proc/diskstats in a collection period. <p>The path of the mount point prefix cannot exceed 64 characters. It must start with a letter, and contain only digits, letters, hyphens (-), periods (.), and swung dashes (~).</p> Windows is not supported. 	≥ 0 Counts	ECS	1 minute

Metric	Metric	Metric Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
disk_write_bytes_per_operation	(Agent) Average Disk Write Size	<p>Average number of bytes in an I/O write for the monitored disk in the monitoring period</p> <p>Unit: ms/op</p> <ul style="list-style-type: none"> Linux: <p>The average disk write size is calculated by calculating the data changes in the tenth column of the corresponding device to divide that of the eighth column in file /proc/diskstats in a collection period.</p> <p>The path of the mount point prefix cannot exceed 64 characters. It must start with a letter, and contain only digits, letters, hyphens (-), periods (.), and swung dashes (~).</p> Windows is not supported. 	≥ 0 ms/op	ECS	1 minute
disk_read_bytes_per_operation	(Agent) Average Disk Read Size	<p>Average number of bytes in an I/O read for the monitored disk in the monitoring period</p> <p>Unit: KB/op</p> <ul style="list-style-type: none"> Linux: <p>The average disk read size is calculated by using the data changes in the sixth column of the corresponding device to divide that of the fourth column in file /proc/diskstats in a collection period.</p> <p>The path of the mount point prefix cannot exceed 64 characters. It must start with a letter, and contain only digits, letters, hyphens (-), periods (.), and swung dashes (~).</p> Windows is not supported. 	≥ 0 KB/op	ECS	1 minute

Metric	Metric	Metric Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
disk_io_svctm	(Agent) Disk I/O Service Time	<p>Average time in an I/O read or write for the monitored disk in the monitoring period</p> <p>Unit: ms/op</p> <ul style="list-style-type: none"> Linux: The average disk I/O service time is calculated by using the data changes in the thirteenth column of the corresponding device to divide the sum of data changes in the fourth and eighth columns in file /proc/diskstats in a collection period. The path of the mount point prefix cannot exceed 64 characters. It must start with a letter, and contain only digits, letters, hyphens (-), periods (.), and swung dashes (~). Windows is not supported. 	≥ 0 ms/op	ECSs	1 minute

Table 12-8 File system metrics

Metric	Metric	Metric Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
disk_fs_rwstate	(Agent) File System Read/Write Status	<p>Read and write status of the mounted file system of the monitored object Possible statuses are 0 (read and write) and 1 (read only).</p> <p>Linux: Check file system information in the fourth column in file /proc/mounts.</p>	0,1	ECSs	1 minute

Metric	Metric	Metric Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
disk_inodesTotal	(Agent) Disk inode Total	Total number of index nodes on the disk Linux: Run the df -i command to check the value in the Inodes column. The path of the mount point prefix cannot exceed 64 characters. It must start with a letter, and contain only digits, letters, hyphens (-), periods (.), and swung dashes (~).	≥ 0	ECSs	1 minute
disk_inodesUsed	(Agent) Total inode Used	Number of used index nodes on the disk Linux: Run the df -i command to check the value in the IUsed column. The path of the mount point prefix cannot exceed 64 characters. It must start with a letter, and contain only digits, letters, hyphens (-), periods (.), and swung dashes (~).	≥ 0	ECSs	1 minute
disk_inodesUsedPercent	(Agent) Percentage of Total inode Used	Number of used index nodes on the disk Unit: Percent Linux: Run the df -i command to check the value in the IUse % column. The path of the mount point prefix cannot exceed 64 characters. It must start with a letter, and contain only digits, letters, hyphens (-), periods (.), and swung dashes (~).	0-100%	ECSs	1 minute

 NOTE

The Windows OS does not support the file system metrics.

Table 12-9 NIC metrics

Metric	Metric	Metric Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
net_bitRecv	(Agent) Outbound Bandwidth	Number of bits received by this NIC per second Unit: bit/s <ul style="list-style-type: none"> Linux: Check metric value changes in file /proc/net/dev in a collection period. Windows: Use the MibIfRow object in the WMI to obtain network metric data. 	≥ 0 bits/s	ECSSs	1 minute
net_bitSent	(Agent) Inbound Bandwidth	Number of bits sent by this NIC per second Unit: bit/s <ul style="list-style-type: none"> Linux: Check metric value changes in file /proc/net/dev in a collection period. Windows: Use the MibIfRow object in the WMI to obtain network metric data. 	≥ 0 bits/s	ECSSs	1 minute
net_packetRecv	(Agent) NIC Packet Receive Rate	Number of packets received by this NIC per second Unit: Count/s <ul style="list-style-type: none"> Linux: Check metric value changes in file /proc/net/dev in a collection period. Windows: Use the MibIfRow object in the WMI to obtain network metric data. 	≥ 0 counts/s	ECSSs	1 minute
net_packetSent	(Agent) NIC Packet Send Rate	Number of packets sent by this NIC per second Unit: Count/s <ul style="list-style-type: none"> Linux: Check metric value changes in file /proc/net/dev in a collection period. Windows: Use the MibIfRow object in the WMI to obtain network metric data. 	≥ 0 counts/s	ECSSs	1 minute
net_tcp_total	(Agent) TCP TOTAL	Total number of TCP connections of the target NIC	≥0	ECSSs	1 minute

Metric	Metric	Metric Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
net_tcp_established	(Agent) Number of ESTABLISHED TCP connections	Number of ESTABLISHED TCP connections of the target NIC	≥0	ECSs	1 minute
net_errin	(Agent) Receive Error Rate	Percentage of receive errors detected by this NIC per second Unit: Percent <ul style="list-style-type: none"> Linux: Check metric value changes in file /proc/net/dev in a collection period. Windows is not supported. 	0-100%	ECSs	1 minute
net_errout	(Agent) Transmit Error Rate	Percentage of transmit errors detected by this NIC per second Unit: Percent <ul style="list-style-type: none"> Linux: Check metric value changes in file /proc/net/dev in a collection period. Windows is not supported. 	0-100%	ECSs	1 minute
net_dropin	(Agent) Received Packet Drop Rate	Percentage of packets received by this NIC which were dropped per second Unit: Percent <ul style="list-style-type: none"> Linux: Check metric value changes in file /proc/net/dev in a collection period. Windows is not supported. 	0-100%	ECSs	1 minute
net_dropout	(Agent) Transmitted Packet Drop Rate	Percentage of packets transmitted by this NIC which were dropped per second Unit: Percent <ul style="list-style-type: none"> Linux: Check metric value changes in file /proc/net/dev in a collection period. Windows is not supported. 	0-100%	ECSs	1 minute

12.1.3 AS Metrics

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

Table 12-10 AS metrics

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

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

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

12.2 Storage

12.2.1 EVS Metrics

Table 12-11 EVS metrics

Metric ID	Metric Name	Description	Value Range	Monitored Object	Monitoring Period
disk_device_read_bytes_rate	Disk Read Bandwidth	Number of bytes read from the monitored disk per second Unit: Bytes/s	≥ 0 bytes/s	EVS disk	5 minutes in average

Metric ID	Metric Name	Description	Value Range	Monitored Object	Monitoring Period
disk_device_write_bytes_rate	Disk Write Bandwidth	Number of bytes written to the monitored disk per second Unit: Bytes/s	≥ 0 bytes/s	EVS disk	5 minutes in average
disk_device_read_requests_rate	Disk Read IOPS	Number of read requests sent to the monitored disk per second Unit: Requests/s	≥ 0 Requests/s	EVS disk	5 minutes in average
disk_device_write_requests_rate	Disk Write IOPS	Number of write requests sent to the monitored disk per second Unit: Requests/s	≥ 0 Requests/s	EVS disk	5 minutes in average

12.3 Network

12.3.1 EIP and Bandwidth Metrics

Table 12-12 EIP and bandwidth metrics

ID	Name	Description	Value Range	Monitored Object	Monitoring Interval (Raw Data)
upstream_bandwidth	Outbound Bandwidth	Network rate of outbound traffic Unit: bit/s	≥ 0 bit/s	Bandwidth or EIP	1 minute
downstream_bandwidth	Inbound Bandwidth	Network rate of inbound traffic Unit: bit/s	≥ 0 bit/s	Bandwidth or EIP	1 minute
upstream	Outbound Traffic	Network traffic going out of the cloud platform in a minute Unit: byte	≥ 0 bytes	Bandwidth or EIP	1 minute

ID	Name	Description	Value Range	Monitored Object	Monitoring Interval (Raw Data)
down_stream	Inbound Traffic	Network traffic going into the cloud platform in a minute Unit: byte	≥ 0 bytes	Bandwidth or EIP	1 minute

12.3.2 ELB Metrics

Table 12-13 Metrics supported by ELB

Metric ID	Name	Description	Value	Monitored Object	Monitoring Period (Raw Data)
m1_cps	Concurrent Connections	Load balancing at Layer 4: total number of TCP and UDP connections from the monitored object to backend servers Load balancing at Layer 7: total number of TCP connections from the clients to the monitored object Unit: N/A	≥ 0	<ul style="list-style-type: none"> Load balancer Listener 	1 minute
m2_act_conn	Active Connections	Number of TCP and UDP connections in the ESTABLISHED state between the monitored object and backend servers You can run the following command to view the connections (both Windows and Linux servers): <code>netstat -an</code> Unit: N/A	≥ 0		

Metric ID	Name	Description	Value	Monitored Object	Monitoring Period (Raw Data)
m3_inact_conn	Inactive Connections	Number of TCP connections between the monitored object and backend servers except those in the ESTABLISHED state You can run the following command to view the connections (both Windows and Linux servers): netstat -an Unit: N/A	≥ 0		
m4_ncps	New Connections	Number of connections established between clients and the monitored object per second Unit: Count/s	≥ 0/ second		
m5_in_pps	Incoming Packets	Number of packets received by the monitored object per second Unit: Packet/s	≥ 0/ second		
m6_out_pps	Outgoing Packets	Number of packets sent from the monitored object per second Unit: Packet/s	≥ 0/ second		
m7_in_Bps	Inbound Rate	Traffic used for accessing the monitored object from the Internet per second Unit: byte/s	≥ 0 bytes/s		

Metric ID	Name	Description	Value	Monitored Object	Monitoring Period (Raw Data)
m8_out_Bps	Outbound Rate	Traffic used by the monitored object to access the Internet per second Unit: byte/s	≥ 0 bytes/s		
m9_abnormal_servers	Unhealthy Servers	Number of unhealthy backend servers associated with the monitored object Unit: N/A	≥ 0	<ul style="list-style-type: none"> Load balancer 	1 minute
ma_normal_servers	Healthy Servers	Number of healthy backend servers associated with the monitored object Unit: N/A	≥ 0		
mb_l7_qps	Layer-7 Query Rate	Number of requests the monitored object receives per second Unit: Query/s	≥ 0 query/s	<ul style="list-style-type: none"> Load balancer Listener 	1 minute
md_l7_http_3xx	Layer-7 3xx Status Codes	Number of 3xx status codes returned by the monitored object Unit: Count/s	≥ 0 /second	<ul style="list-style-type: none"> Load balancer Listener 	1 minute
mc_l7_http_2xx	Layer-7 2xx Status Codes	Number of 2xx status codes returned by the monitored object Unit: Count/s	≥ 0 /second	<ul style="list-style-type: none"> Load balancer Listener 	1 minute
me_l7_http_4xx	Layer-7 4xx Status Codes	Number of 4xx status codes returned by the monitored object Unit: Count/s	≥ 0 /second		
mf_l7_http_5xx	Layer-7 5xx Status Codes	Number of 5xx status codes returned by the monitored object Unit: Count/s	≥ 0 /second		

Metric ID	Name	Description	Value	Monitored Object	Monitoring Period (Raw Data)
m10_l7_http_other_status	Layer-7 Other Status Codes	Number of status codes returned by the monitored object except 2xx, 3xx, 4xx, and 5xx status codes Unit: Count/s	≥ 0/second		
m11_l7_http_404	Layer-7 404 Not Found	Number of 404 Not Found status codes returned by the monitored object Unit: Count/s	≥ 0/second		
m12_l7_http_499	Layer-7 499 Client Closed Request	Number of 499 Client Closed Request status codes returned by the monitored object Unit: Count/s	≥ 0/second		
m13_l7_http_502	Layer-7 502 Bad Gateway	Number of 502 Bad Gateway status codes returned by the monitored object Unit: Count/s	≥ 0/second		
m14_l7_rt	Average Layer-7 Response Time	Average response time of the monitored object The response time starts when the monitored object receives requests from the clients and ends when it returns all responses to the clients. Unit: ms NOTE The average response time it takes to establish a WebSocket connection may be very high. This metric cannot be used as a reference.	≥ 0 ms		

12.3.3 NAT Gateway Metrics

Table 12-14 NAT Gateway metrics

Metric ID	Name	Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
snat_connection	SNAT Connections	Number of SNAT connections of the NAT gateway Unit: count	≥ 0	NAT gateway	1 minute
Server IP address set	Monitoring Details of Top 10	IP addresses of the top 10 servers that occupy the most SNAT connections Unit: count	≥ 0	NAT gateway	1 minute

Table 12-15 Private NAT gateway metrics

Metric ID	Name	Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
snat_connection	SNAT Connections	Number of SNAT connections of the NAT gateway Unit: count	≥ 0	Private NAT gateway	1 minute
inbound_bandwidth	Inbound Bandwidth	Inbound bandwidth of servers using the SNAT function Unit: bit/s	≥ 0 bit/s	Private NAT gateway	1 minute

Metric ID	Name	Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
outbound_bandwidth	Outbound Bandwidth	Outbound bandwidth of servers using the SNAT function Unit: bit/s	≥ 0 bit/s	Private NAT gateway	1 minute
inbound_pps	Inbound PPS	Inbound PPS of servers using the SNAT function Unit: count	≥ 0	Private NAT gateway	1 minute
outbound_pps	Outbound PPS	Outbound PPS of servers using the SNAT function Unit: count	≥ 0	Private NAT gateway	1 minute
inbound_traffic	Inbound Traffic	Inbound traffic of servers using the SNAT function Unit: byte	≥ 0 bytes	Private NAT gateway	1 minute
outbound_traffic	Outbound Traffic	Outbound traffic of servers using the SNAT function Unit: byte	≥ 0 bytes	Private NAT gateway	1 minute

13 FAQs

13.1 General Consulting

13.1.1 What Is Rollup?

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

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

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

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

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

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

Choose whichever rollup method best meets your service requirements.

13.1.2 How Long Is Metric Data Retained?

Metric data includes raw data and rolled-up data.

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

Table 13-1 Retention periods for rolled-up data

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

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

13.1.3 How Many Rollup Methods Does Cloud Eye Support?

Cloud Eye supports the following rollup methods:

- **Average**
If **Avg.** is selected for **Statistic**, Cloud Eye calculates the average value of metrics collected within a rollup period.
- **Maximum**
If **Max.** is selected for **Statistic**, Cloud Eye calculates the maximum value of metrics collected within a rollup period.
- **Minimum**
If **Min.** is selected for **Statistic**, Cloud Eye calculates the minimum value of metrics collected within a rollup period.
- **Sum**
If **Sum** is selected for **Statistic**, Cloud Eye calculates the sum of metrics collected within a rollup period.
- **Variance**
If **Variance** is selected for **Statistic**, Cloud Eye calculates the variance value of metrics collected within a rollup period.

NOTE

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

13.1.4 How Can I Export Collected Data?

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

- The first row in the exported CSV file displays the username, region, service, instance name, instance ID, metric name, metric data, time, and timestamp. You can view historical monitoring data.
- To convert the time using a Unix timestamp to the time of the target time zone, perform the following steps:
 - a. Use Excel to open a .csv file.
 - b. Use the following formula to convert the time:
$$\text{Target time} = [\text{Unix timestamp}/1000 + (\text{Target time zone}) \times 3600]/86400 + 70 \times 365 + 19$$
 - c. Set cell format to **Date**.

13.2 Server Monitoring

13.2.1 How Can I Quickly Restore the Agent Configuration?

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

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

13.2.2 What OSs Does the Agent Support?

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

NOTICE

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

[Table 13-2](#) and [Table 13-3](#) lists the supported OSs.

Table 13-2 OS versions supported for ECS

OS (64 bit)	Version
CentOS	6.3, 6.5, 6.8, 6.9, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6
OpenSUSE	13.2, 42.2
Debian	7.5.0, 8.2.0, 8.8.0, 9.0.0
Ubuntu	14.04 server, 16.04 server
EulerOS	2.2, 2.3

OS (64 bit)	Version
SUSE	Enterprise11 SP4, Enterprise12 SP1, Enterprise12 SP2
Fedora	24, 25
Oracle Linux	6.9, 7.4
CoreOS	10.10.5 NOTE Cloud-Init cannot be installed automatically. Install it manually in the / directory. To query the Agent status, run systemctl telescoped status .
Other	Gentoo Linux 13.0, Gentoo Linux 17.0 NOTE To query the Agent status, run rc-service telescoped status .
Windows	Windows Server 2016 Standard 64-bit Windows Server 2016 Datacenter 64-bit Windows Server 2012 R2 Standard 64-bit Windows Server 2012 R2 Datacenter 64-bit Windows Server 2008 R2 Standard 64-bit Windows Server 2008 R2 Datacenter 64-bit Windows Server 2008 R2 Enterprise 64-bit Windows Server 2008 R2 Web 64-bit
Arm general-computing	CentOS 7.4 64bit with ARM (40 GB) CentOS 7.5 64bit with ARM (40 GB) CentOS 7.6 64bit with ARM (40 GB) EulerOS 2.8 64bit with ARM (40 GB) Fedora 29 64bit with ARM (40 GB) Ubuntu 18.04 64bit with ARM (40 GB)

Table 13-3 OS versions for BMS


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

 **NOTE**

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

13.2.3 How Do I Query the Current Agent Version?

You can log in to the management console to query the Agent version of the current server. The procedure is as follows:

1. Log in to the management console.
2. Click  in the upper left to select a region and project.
3. Click **Service List** in the upper left corner, and select **Cloud Eye**.
The **Cloud Eye** console is displayed.
4. In the navigation pane on the left, choose **Server Monitoring**.
The **Server Monitoring** page is displayed.
5. Locate the row containing the target ECS. In the **Operation** column, click **More**, and choose **Modify Upgrade Method**.

NOTE

You can modify the Agent upgrade method only for ECSs whose **Agent Status** is **Running**.

6. In the displayed **Modify Upgrade Method** dialog box, check the value of **Current Version**.

For example, if **Current Version** is 1.1.4, the version of the Agent installed on the current ECS is 1.1.4.

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

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

Procedure

1. Log in an ECS as user **root**.
2. Open the **sysctl.conf** file:
vim /etc/sysctl.conf
3. (Permanent change) Add new ports to the **sysctl.conf** file:
net.ipv4.ip_local_port_range=49152 65536
4. Make the modification take effect:
sysctl -p /etc/sysctl.conf

NOTE

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

 NOTE

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

13.2.5 How Can I Create an Agency?

Scenarios

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

Procedure


1. Log in to the management console.
2. Click  in the upper left to select a region and project.
3. Click **Service List** in the upper left corner, and select **Identity and Access Management**.
4. In the navigation pane on the left, choose **Agencies**. In the upper right corner, click **Create Agency**.
5. Configure the parameters by referring to [Table 13-4](#).

Table 13-4 Creating an agency

Parameter	Description
Agency Name	Specifies the name of the agency. Example: CESAgentAutoConfigAgency
Agency Type	Select Cloud service .
Cloud Service	Select Elastic Cloud Server (ECS) from the drop-down list.
Validity Period	Select Unlimited .
Description	(Optional) Provides supplementary information about the agency.

6. In the **Permissions** area, click **Modify** in the row where the current region is located.
7. In the **Available Policies** area on the left, enter **CES**. In the search result, select **CES** and **CES Administrator**.
8. Click **OK**.

Agency Configuration

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

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

 **NOTE**

If you purchase a BMS, choose **Computing > Bare Metal Server**.

3. Click the name of the target ECS on which the Agent is installed.
4. For **Agency**, select the agency created in [5](#) and click the green tick to make the agency take effect.

13.2.6 What Can't I Create Another Agency?

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

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

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

You can delete the agency you created and then restore the Agent configuration, or manually configure the agency based on [How Can I Create an Agency?](#)

13.2.8 What Can I Do If Agency CESAgentAutoConfigAgency Is Invalid?

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

13.2.9 Will the Agent Affect the Server Performance?

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

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

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

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

It may be because:

- Your account is in arrears.

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

The log paths are as follows:

- Linux:

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

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

- Windows:

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

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

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

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

13.3 Alarm Notifications or False Alarms

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

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

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

Cloud Eye can:

- Send emails to you.
- Work with Auto Scaling to trigger the system to automatically add or remove servers.

13.3.2 What Alarm Status Does Cloud Eye Support?

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

- **Alarm**: The metric value reached the alarm threshold, and an alarm has been triggered but not cleared for the resource.
- **Resolved**: The metric value went back to the normal range, and the resource alarm was cleared.
- **Insufficient data**: No monitoring data has been reported for three consecutive hours, and this is generally because the instance has been deleted or is abnormal.

- **Triggered:** An event configured in the alarm policy triggered an alarm.
- **Expired:** The monitored resources or alarm policies in the alarm rule were adjusted, so the original alarm record status expired.

13.3.3 What Alarm Severities Does Cloud Eye Support?

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

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

13.4 Monitored Data Exceptions

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

Possible causes are as follows:

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

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

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

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

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

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

13.4.3 What Are the Impacts on ECS Metrics If Not Installed on ECSs?

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

13.5 User Permissions

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

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

A Change History

Released On	Description
2024-04-15	This issue is the first official release.