Cloud Eye

Service Overview

Issue 01

Date 2025-09-10

HUAWEI

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Trademarks and Permissions


and other Huawei trademarks are the property 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 Cloud 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 Cloud Computing Technologies Co., Ltd.

Address: Huawei Cloud Data Center Jiaoxinggong Road
Qianzhong Avenue
Gui'an New District
Gui Zhou 550029
People's Republic of China

Website: https://www.huaweicloud.com/intl/en-us/

Contents

1 What Is Cloud Eye?....1
2 Advantages....3
3 Application Scenarios....4
4 Basic Concepts....6
5 Notes and Constraints....8
6 Security....10
6.1 Shared Responsibilities....10
6.2 Identity and Access Management....11
6.2.1 Access Control for Cloud Eye....11
6.3 Auditing and Logging....12
6.4 Data Protection Technologies....13
7 Region and AZ....15
8 Permissions....17

1 What Is Cloud Eye?

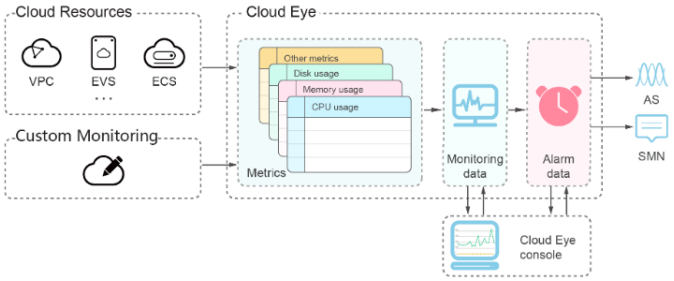
Cloud Eye is a multi-dimensional resource monitoring service. You can use Cloud Eye to monitor resources, set alarm rules, identify resource exceptions, and quickly respond to resource changes.

Architecture

Cloud Eye collects metrics from various cloud services. You can also use APIs to report custom metric data according to the specifications stipulated by Cloud Eye.

All metrics are stored in the Cloud Eye's metric database. When a cloud service reports monitoring data to Cloud Eye, its metrics will be displayed on a default graph where you can view resource details. You can also configure alarm rules with varying severity levels based on the importance of metrics. When a metric reaches its preset threshold, an alarm is triggered, and notifications will be sent to you over different protocols through Simple Message Notification (SMN). This allows you to quickly address any resource issues.

Figure 1-1 Cloud Eye architecture



Major Features

Cloud Eye provides the following functions:

- Automatic monitoring

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

- Server monitoring

After you install the Agent (Telescope) on an ECS or Bare Metal Server (BMS), you can collect 60-second granularity ECS and BMS monitoring data in real-time. Cloud Eye provides 40 metrics, such as CPU, memory, and disk metrics. For details, see **Overview**.

- Flexible alarm rule configuration

  You can create alarm rules for multiple resources at the same time. After you create an alarm rule, you can modify, enable, disable, or delete it at any time. For details, see **Overview**.

- Real-time notification

  You can enable **Alarm Notifications** when creating alarm rules. When a metric reaches the threshold specified in an alarm rule, Cloud Eye will notify you by SMS, email, HTTP or HTTPS message, FunctionGraph (function), FunctionGraph (workflow), WeCom, DingTalk, Lark, or WeLink. You can track the service status and establish programs accordingly to handle the alarms. For more information, see **Alarm Notifications**.

- Monitoring panel

  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. For details, see **Overview**.

- Resource group

  A resource group allows you to centrally manage resources, such as ECSs, EVS disks, EIPs, bandwidth, and databases, from the respective of your services. You can manage different types of resources, alarm rules, and alarm records by service. This improves O&M efficiency. For more information about resource groups, see **Overview**.

- Event monitoring

  You can query system events and custom events reported to Cloud Eye through APIs. You can create alarm rules for both system events and custom events. When specific events occur, Cloud Eye generates alarms for you. For details, see **Overview**.

- Data dump

  You can use the data dump function to query metrics on the DMS for Kafka console or on an open-source Kafka client. It helps you dump cloud service monitoring data to Kafka in real time.

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 monitoring panels and graphs to compare multiple metrics. The graphs automatically refresh to 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 will notify you by SMS message, email, FunctionGraph (function), FunctionGraph (workflow), WeCom, DingTalk, Lark, or WeLink, or by sending HTTP/HTTPS messages to a specified IP address. You can track the service status and establish programs accordingly to handle the alarms.

Batch Creation of Alarm Rules

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

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.

Server Monitoring

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

Performance Issues

When an alarm rule's conditions are met, Cloud Eye generates an alarm and invokes the Simple Message Notification (SMN) API to send a notification. After receiving the notification, you can take according actions to identify the root cause.

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

4 Basic Concepts

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

- **Metrics**
- **Rollup**
- **Dashboards**
- **Topics**
- **Alarm Rules**
- **Alarm Templates**
- **Projects**

Metrics

A metric refers to a quantized value of a resource dimension on the cloud platform, such as the ECS CPU usage and memory usage. A metric is a time-dependent variable that generates a certain amount of monitoring data over time. It helps you understand the changes over a specific period of time. For details about how to view cloud service monitoring data, see **Viewing a Cloud Service Dashboard**. For details about the metrics supported by Cloud Eye, see **Cloud Product Metrics**.

Rollup

Rollup is the process in which Cloud Eye calculates the average, maximum, minimum, sum, or variance value based on the 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. For details, see **What Is Rollup?**

Dashboards

Monitoring 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. For more information, see **Overview**.

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. For details, see **Creating a Topic**.

Alarm Rules

The status of an alarm rule changes based on the threshold you set. Cloud Eye notifies you by email, SMS message, HTTP/HTTPS request, FunctionGraph (function), FunctionGraph (workflow), WeCom, DingTalk, Lark, or WeLinkemail or HTTP/HTTPS request, so you can handle faults quickly and prevent service interruptions. For details, see **Creating an Alarm Rule**.

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. For more information, see **Creating a Custom Alarm or Event Template**.

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. For details, see **Projects**.

5 Notes and Constraints

Table 5-1 lists the default Cloud Eye resource quotas per user. For details about how to adjust the quotas, see **Quota Adjustment**.

Table 5-1 Resource quotas

Item	Default Limit
Alarm rules that can be created	1,000
Number of alarm templates that can be created	200
Number of alarm policies that can be configured for a single service in an alarm template	50
Dashboards that can be created	10
Graphs that can be added to a dashboard	50
Objects that can be selected for monitoring when creating an alarm rule	5,000
Alarm rules that can be created at a time	1,000 **NOTE** If you select 50 monitored objects and 20 metrics, the number of alarm rules that can be created is 1,000.
Topics that can be selected for receiving notifications	20

Item	Default Limit
Monitoring data records that can be exported at a time	400 **NOTE** If 400 monitored objects are to be exported, only records of one metric can be exported. If 80 monitored objects are to be exported, records of 5 metrics can be exported.

6 Security

6.1 Shared Responsibilities
6.2 Identity and Access Management
6.3 Auditing and Logging
6.4 Data Protection Technologies

6.1 Shared Responsibilities

Huawei Cloud guarantees that its commitment to cyber security will never be outweighed by the consideration of commercial interests. To cope with emerging cloud security challenges and pervasive cloud security threats and attacks, Huawei Cloud builds a comprehensive cloud service security assurance system for different regions and industries based on Huawei's unique software and hardware advantages, laws, regulations, industry standards, and security ecosystem.

Unlike traditional on-premises data centers, cloud computing separates operators from users. This approach not only enhances flexibility and control for users but also greatly reduces their operational workload. For this reason, cloud security cannot be fully ensured by one party. Cloud security requires joint efforts of Huawei Cloud and you, as shown in **Figure 6-1**.

- **Huawei Cloud**: Huawei Cloud is responsible for infrastructure security, including security and compliance, regardless of cloud service categories. The infrastructure consists of physical data centers, which house compute, storage, and network resources, virtualization platforms, and cloud services Huawei Cloud provides for you. In PaaS and SaaS scenarios, Huawei Cloud is responsible for security settings, vulnerability remediation, security controls, and detecting any intrusions into the network where your services or Huawei Cloud components are deployed.
- **Customer**: As our customer, your ownership of and control over your data assets will not be transferred under any cloud service category. Without your explicit authorization, Huawei Cloud will not use or monetize your data, but you are responsible for protecting your data and managing identities and access. This includes ensuring the legal compliance of your data on the cloud, using secure credentials (such as strong passwords and multi-factor authentication), and properly managing those credentials, as well as

monitoring and managing content security, looking out for abnormal account behavior, and responding to it, when discovered, in a timely manner.

Figure 6-1 Huawei Cloud shared security responsibility model

Cloud security responsibilities are determined by control, visibility, and availability. When you migrate services to the cloud, assets, such as devices, hardware, software, media, VMs, OSs, and data, are controlled by both you and Huawei Cloud. This means that your responsibilities depend on the cloud services you select. As shown in **Figure 6-1**, customers can select different cloud service types (such as IaaS, PaaS, and SaaS services) based on their service requirements. As control over components varies across different cloud service categories, the responsibilities are shared differently.

- In on-premises scenarios, customers have full control over assets such as hardware, software, and data, so tenants are responsible for the security of all components.
- In IaaS scenarios, customers have control over all components except the underlying infrastructure. So, customers are responsible for securing these components. This includes ensuring the legal compliance of the applications, maintaining development and design security, and managing vulnerability remediation, configuration security, and security controls for related components such as middleware, databases, and operating systems.
- In PaaS scenarios, customers are responsible for the applications they deploy, as well as the security settings and policies of the middleware, database, and network access under their control.
- In SaaS scenarios, customers have control over their content, accounts, and permissions. They need to protect their content, and properly configure and protect their accounts and permissions in compliance with laws and regulations.

6.2 Identity and Access Management

6.2.1 Access Control for Cloud Eye

Cloud Eye interconnects with **Identity and Access Management (IAM)** . If you need to assign different permissions to employees in your enterprise to access your Cloud Eye resources, IAM is a good choice for fine-grained permissions management. IAM provides identity authentication, permissions management,

and access control, helping you securely manage access to your Huawei Cloud resources.

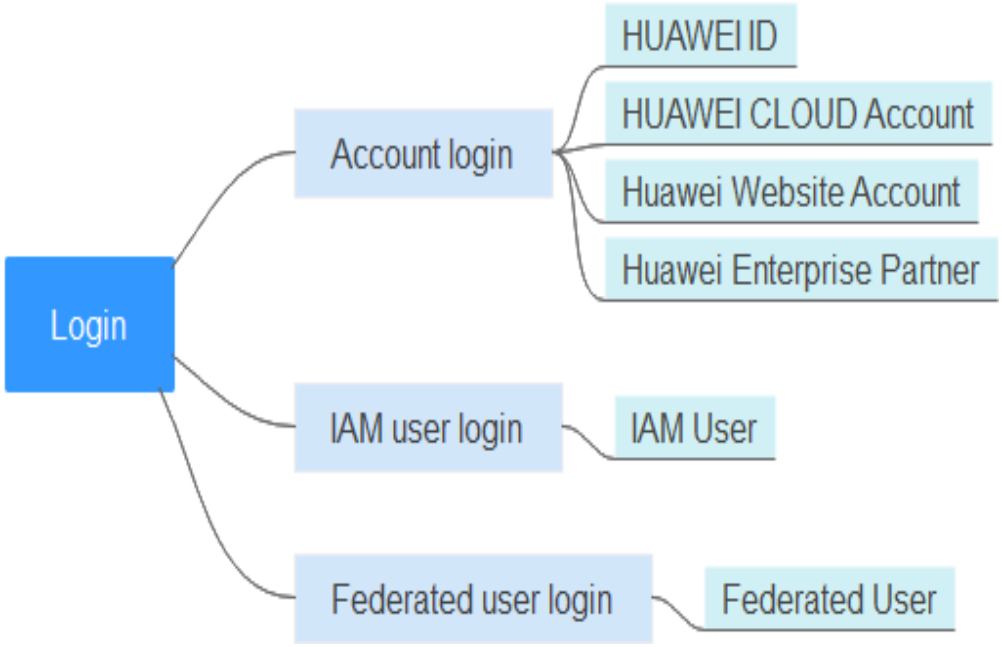
Authentication

You can log in to Huawei Cloud using the following methods (see **Figure 6-2**):

- **Account login**: Log in with the account that was created when you use Huawei Cloud. Your account has full access permissions for your cloud resources and makes payments for the use of these resources.
- **IAM user login**: IAM users are created by an administrator to use specific cloud services.

  Federated user login: Federated users are registered with an enterprise IdP that is created by the administrator in IAM.

Figure 6-2 Logging in to Huawei Cloud



Access control

You need to configure system-defined or custom policies provided by Cloud Eye for IAM users to allow them to create or access Cloud Eye resources. For details, see **Creating a User and Granting Permissions** You are advised to create custom policies for Cloud Eye based on the principle of least privilege (PoLP).

6.3 Auditing and Logging

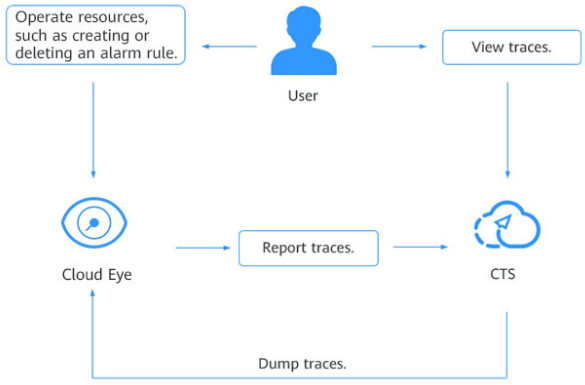
Audit

Cloud Trace Service (CTS) is a log audit service for Huawei Cloud security. It allows you to collect, store, and query cloud resource operation records. You can use these records for security analysis, audit compliance, resource tracking, and fault locating.

After you enable CTS and configure a tracker, CTS can record management and data traces of Cloud Eye for auditing.

- For details about how to enable and configure CTS, see **Enabling CTS**.
- For details about Cloud Eye operations recorded by CTS, see **Key Cloud Eye Operations**.

Figure 6-3 Cloud Trace Service



Logs

After you have enabled CTS, the system starts recording operations on Cloud Eye resources. You can view the operation records of the last seven days on the CTS console. For details about how to view or export operation records of the last seven days on the CTS console, see **Viewing Cloud Eye Logs**.

6.4 Data Protection Technologies

For data protections, you are advised to protect Huawei Cloud account credentials and use IAM to set up individual user accounts. In this way, each user is given only the permissions necessary to fulfill their job duties. We also recommend that you secure your data in the following ways:

- Use multi-factor authentication (MFA) for each account.
- Use Secure Sockets Layer (SSL) or Transport Layer Security (TLS) protocols to communicate with Huawei Cloud resources. TLS 1.2 or later is recommended.
- Use CTS to configure API and user activity logging.
- Use Data Encryption Workshop (DEW), along with all default security controls within Huawei Cloud services.

We strongly advise you against putting confidential or sensitive information (such as your customers' email addresses) into tags or free-form fields (such as a name field) when you work with Cloud Eye or other Huawei Cloud services using the console, APIs, Huawei Cloud command-line interface (CLI), or Huawei Cloud software development kit (SDK). Any data that you enter into tags or free-form fields form field used for names may be used for billing or diagnostic logs. If you provide the URL of an external server, we strongly recommend that you do not include credential information in the URL to validate your request to that server.

Data Transmission Encryption

Cloud Eye uses end-to-end encryption for data in transit.

7 Region and AZ

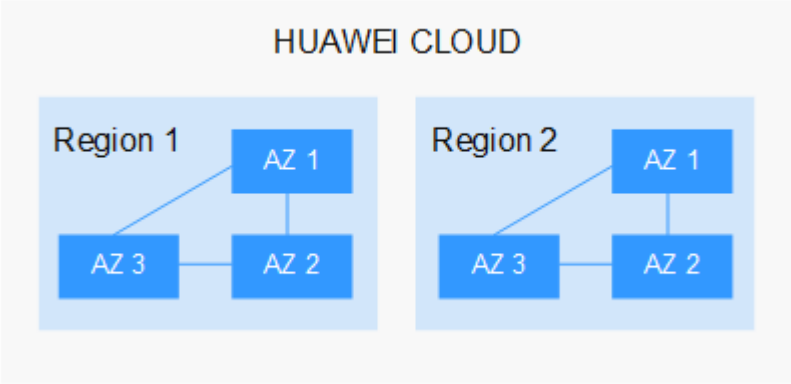
Concept

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

- Regions are divided based on geographical location and network latency. Public services, such as Elastic Cloud Server (ECS), Elastic Volume Service (EVS), Object Storage Service (OBS), Virtual Private Cloud (VPC), Elastic IP (EIP), and Image Management Service (IMS), are shared within the same region. Regions are classified into universal regions and dedicated regions. A universal region provides universal cloud services for common tenants. A dedicated region provides specific services for specific tenants.
- An AZ contains one or more physical data centers. Each AZ has independent cooling, fire extinguishing, moisture-proof, and electricity facilities. Within an AZ, computing, network, storage, and other resources are logically divided into multiple clusters. AZs within a region are interconnected using high-speed optical fibers, to support cross-AZ high-availability systems.

Figure 7-1 shows the relationship between regions and AZs.

Figure 7-1 Regions and AZs



Huawei Cloud provides services in many regions around the world. You can select a region and an AZ based on requirements. For more information, see **Huawei Cloud Global Regions**.

Selecting a Region

When selecting a region, consider the following factors:

- Location

  It is recommended that you select the closest region for lower network latency and quick access.

  - If your target users are in Asia Pacific (excluding the Chinese mainland), select the **CN-Hong Kong**, **AP-Bangkok**, or **AP-Singapore** region.
  - If your target users are in Africa, select the **AF-Johannesburg** region.
  - If your target users are in Latin America, select the **LA-Santiago** region.

    NOTE

    The **LA-Santiago** region is located in Chile.

- Resource price

  Resource prices may vary in different regions. For details, see **Product Pricing Details**.

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 information, see **Regions and Endpoints**.

8 Permissions

If you need to grant your enterprise personnel permission to access your Cloud Eye resources, use Identity and Access Management (IAM). IAM provides identity authentication, fine-grained permissions management, and access control. IAM helps you secure access to your Huawei Cloud resources.

With IAM, you can create IAM users and grant them permissions to access only specific resources. For example, if you want some software developers in your enterprise to be able to use Cloud Eye resources but do not want them to be able to delete other cloud resources or perform any other high-risk operations, you can create IAM users and grant them only the permissions to use Cloud Eye resources.

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

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

Cloud Eye Permissions

New IAM users do not have any permissions assigned by default. You need to first add them to one or more groups and then attach policies or roles to these groups. The users then inherit permissions from the groups and can perform specified operations on cloud services based on the permissions they have been assigned.

Cloud Eye is a project-level service deployed and accessed in specific physical regions. Cloud Eye permissions are assigned to users in specific regions (such as **CN-Hong Kong**) and only take effect in these regions. To make the permissions take effect in all regions, 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 coarse-grained authorization strategy that defines permissions by job responsibility. Only a limited number of service-level roles are available 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 fine-grained authorization strategy that defines permissions required to perform operations on specific cloud resources under certain conditions. This type of authorization is more flexible and is ideal for least privilege access. For example, you can grant Cloud Eye users only the permissions for managing a certain type of Cloud Eye resources.

  A majority of fine-grained policies contain permissions for specific APIs, and permissions are defined using API actions. For the API actions supported by Cloud Eye, see **Permissions Policies and Supported Actions**.

Table 8-1 lists all the system-defined permissions for Cloud Eye.

Table 8-1 System-defined permissions for Cloud Eye

Role/Policy Name	Description	Type	Dependencies
CES FullAccessPolicy	All permissions for Cloud Eye. Users granted these permissions can perform all operations on Cloud Eye.	System-defined policies	Cloud Eye monitoring involves querying resources of other cloud services. This policy contains the resource query permissions of some cloud services. If you encounter permission problems, configure required fine-grained permissions for the services involved. For details, see **Supported Cloud Services**. Alarm notification: depends on SMN FullAccess. Data dump: depends on OBS OperateAccess.
CES ReadOnlyAccessPolicy	Read-only permissions for viewing data on Cloud Eye	System-defined policies	Cloud Eye monitoring involves querying resources of other cloud services. This policy contains the resource query permissions of some cloud services. If you encounter permission problems, configure required fine-grained permissions of the involved services. For details, see **Supported Cloud Services**.

Role/Policy Name	Description	Type	Dependencies
CES AgentAccess	Permissions required for the Cloud Eye Agent to run **NOTE** To ensure that the Cloud Eye Agent can provide services, you need to configure an agency. For details, see **How Do I Configure an Agency?**	System-defined policies	None
CES Administrator	Administrator permissions for Cloud Eye	System-defined roles	Depends on the **Tenant Guest** policy. **Tenant Guest**: global policy, which must be assigned in the global project.
CES FullAccess	All permissions for Cloud Eye. Users granted these permissions can perform all operations on Cloud Eye. **NOTE** It is recommended that you use CES FullAccessPolicy because CES FullAccess does not meet the least privilege principle.	System-defined policies	Cloud Eye monitoring involves querying resources of other cloud services. This policy contains the resource query permissions of some cloud services. If you encounter permission problems, configure required fine-grained permissions of the involved services. For details, see **Supported Cloud Services**. Alarm notification: depends on SMN FullAccess. Data dump: depends on OBS OperateAccess.
CES ReadOnlyAccess	Read-only permissions for viewing data on Cloud Eye **NOTE** It is recommended that you use CES ReadOnlyAccessPolicy because CES ReadOnlyAccess does not meet the least privilege principle.	System-defined policies	Cloud Eye monitoring involves querying resources of other cloud services. This policy contains the resource query permissions of some cloud services. If you encounter permission problems, configure required fine-grained permissions of the involved services. For details, see **Supported Cloud Services**.

Table 8-2 lists common operations supported by the Cloud Eye system-defined permissions.

Table 8-2 Common operations supported by system-defined permissions

Feature	Operation	CES FullAccessPolicy	CES ReadOnlyAccessPolicy	CES Administrator (The Tenant Guest policy must be added at the same time.)	Tenant Guest
Monitoring Overview	Viewing the monitoring overview	Supported	Supported	Supported	Supported
	Viewing monitoring data in a large screen	Supported	Supported	Supported	Supported
Monitoring Panels	Creating a dashboard	Supported	Not supported	Supported	Not supported
	Viewing monitoring data in a large screen	Supported	Supported	Supported	Supported
	Querying a panel	Supported	Supported	Supported	Supported
	Deleting a monitoring panel	Supported	Not supported	Supported	Not supported
	Adding a graph	Supported	Not supported	Supported	Not supported
	Viewing a graph	Supported	Supported	Supported	Supported
	Modifying a graph	Supported	Not supported	Supported	Not supported
	Deleting a graph	Supported	Not supported	Supported	Not supported
	Adjusting the position of a graph	Supported	Not supported	Supported	Not supported

Feature	Operation	CES FullAccessPolicy	CES ReadOnlyAccessPolicy	CES Administrator (The Tenant Guest policy must be added at the same time.)	Tenant Guest
Resource Groups	Creating a resource group	Supported	Not supported	Supported	Not supported
	Viewing resource groups	Supported	Supported	Supported	Supported
	Viewing resource groups (Resource Overview)	Supported	Supported	Supported	Supported
	Viewing resource groups (Alarm Rules)	Supported	Supported	Supported	Supported
	Modifying a resource group	Supported	Not supported	Supported	Not supported
	Deleting a resource group	Supported	Not supported	Supported	Not supported
Alarm Rules	Creating an alarm rule	Supported	Not supported	Supported	Not supported
	Modifying an alarm rule	Supported	Not supported	Supported	Not supported
	Enabling an alarm rule	Supported	Not supported	Supported	Not supported
	Disabling an alarm rule	Supported	Not supported	Supported	Not supported

Feature	Operation	CES FullAccessPolicy	CES ReadOnlyAccessPolicy	CES Administrator (The Tenant Guest policy must be added at the same time.)	Tenant Guest
	Deleting an alarm rule	Supported	Not supported	Supported	Not supported
	Exporting alarm rules	Supported	Not supported	Supported	Not supported
	Viewing alarm rules	Supported	Supported	Supported	Supported
	Viewing details of an alarm rule	Supported	Supported	Supported	Supported
	Viewing a graph	Supported	Supported	Supported	Supported
Alarm Records	Viewing alarm records	Supported	Supported	Supported	Supported
Alarm Templates	Viewing a default alarm template	Supported	Supported	Supported	Supported
	Viewing a custom template	Supported	Supported	Supported	Supported
	Creating a custom template	Supported	Not supported	Supported	Not supported
	Modifying a custom alarm template	Supported	Not supported	Supported	Not supported
	Deleting a custom template	Supported	Not supported	Supported	Not supported
One-Click Monitoring	Enable one-click monitoring	Supported	Not supported	Supported	Not supported

Feature	Operation	CES FullAccessPolicy	CES ReadOnlyAccessPolicy	CES Administrator (The Tenant Guest policy must be added at the same time.)	Tenant Guest
	Viewing one-click monitoring	Supported	Supported	Supported	Supported
	Modifying one-click monitoring	Supported	Not supported	Supported	Not supported
	Disabling one-click monitoring	Supported	Not supported	Supported	Not supported
Server Monitoring	Viewing servers	Supported	Supported	Supported	Supported
	Viewing server monitoring metrics	Supported	Supported	Supported	Supported
	Installing the Agent	Supported (You must have the **ECS FullAccess** permissions.)	Not supported	Supported (You must have the **ECS FullAccess** permissions.)	Not supported
	Restoring the Agent configurations	√ (You must have the **Security Administrator** and **ECS FullAccess** permissions.)	Not supported	√ (You must have the **Security Administrator** and **ECS FullAccess** permissions.)	Not supported
	Uninstalling the Agent	Supported (You must have the **ECS FullAccess** permissions.)	Not supported	Supported (You must have the **ECS FullAccess** permissions.)	Not supported

Feature	Operation	CES FullAccessPolicy	CES ReadOnlyAccessPolicy	CES Administrator (The Tenant Guest policy must be added at the same time.)	Tenant Guest
	Configuring process monitoring	Supported	Not supported	Supported	Not supported
	Configuring monitoring for a process	Supported	Not supported	Supported	Not supported
Cloud Service Monitoring	Viewing the cloud service list	Supported (See **Supported Cloud Services**.)	Supported (See **Supported Cloud Services**.)	Supported	Supported
	Querying metrics of a cloud service	Supported	Supported	Supported	Supported
Custom Monitoring	Adding custom monitoring data	Supported	Not supported	Supported	Not supported
	Viewing the custom monitoring list	Supported	Supported	Supported	Supported
	Viewing custom monitoring data	Supported	Supported	Supported	Supported
Event Monitoring	Adding a custom event	Supported	Not supported	Supported	Not supported
	Viewing events	Supported	Supported	Supported	Supported
	Viewing details of an event	Supported	Supported	Supported	Supported

Feature	Operation	CES FullAccessPolicy	CES ReadOnlyAccessPolicy	CES Administrator (The Tenant Guest policy must be added at the same time.)	Tenant Guest
Data Dumping to DMS Kafka	Creating a dump task	Supported	Not supported	Supported	Not supported
	Querying data dump tasks	Supported	Supported	Supported	Supported
	Querying a data dump task	Supported	Supported	Supported	Supported
	Modifying a data dump task	Supported	Not supported	Supported	Not supported
	Starting a data dump task	Supported	Not supported	Supported	Not supported
	Stopping a data dump task	Supported	Not supported	Supported	Not supported
	Deleting a data dump task	Supported	Not supported	Supported	Not supported
Others	Configuring data dump	Supported (You must have the **OBS Bucket Viewer** permissions.)	Not supported	Supported (You must have the **Tenant Administrator** permission.)	Not supported
	Exporting monitoring data	Supported	Not supported	Supported	Not supported
	Sending an alarm notification	Supported	Not supported	Supported	Not supported

Roles or Policies Required for Operations on the Cloud Eye Console

To grant an IAM user the permissions to view or use resources of other cloud services on the Cloud Eye console, you must first grant the **CES Administrator**, **CES FullAccessPolicy**, or **CES ReadOnlyAccessPolicy** policy to the user group that the user belongs to and then grant the dependency roles or policies listed in **Table 8-3** to the user. These dependency policies will allow the IAM user to access resources of other cloud services.

Table 8-3 Roles or policies required for operations on the Cloud Eye console

Function	Dependent Services	Roles or Policies Required
Cloud service monitoring	• Cloud Phone Host (CPH) • ROMA Connect: – Business Flow Service (BFS) – Fast Data Integration (FDI) – API Connect (APIC) • Cloud Search Service (CSS) • Workspace • Message & SMS	IAM users with the **CES Administrator**, **CES FullAccessPolicy**, or **CES ReadOnlyAccessPolicy** permission can view information about cloud service monitoring.

Helpful Links

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

