Cloud Eye

Service Overview

Issue 01

Date 2023-12-29

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

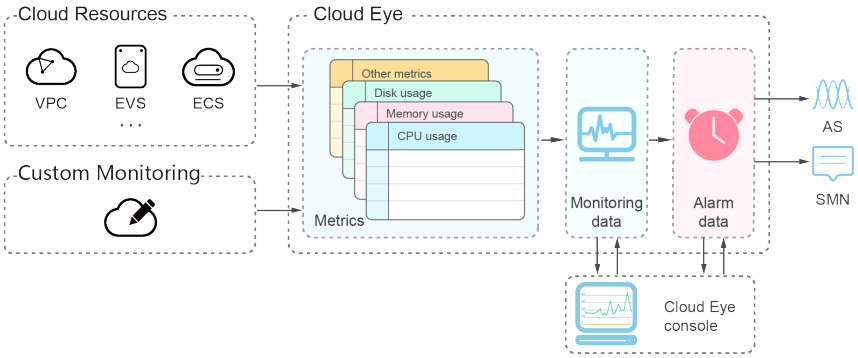
Website: https://www.huaweicloud.com/intl/en-us/

Contents

1 What Is Cloud Eye?

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

Figure 1-1 Cloud Eye architecture



Cloud Eye provides the following functions:

- Automatic monitoring

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

- Server monitoring

  After you install the Agent (Telescope) on an ECS and Bare Metal Server (BMS), you can collect 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 **Introduction to Server Monitoring**.

- Flexible alarm rule configuration

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

- Real-time notification

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

alarm rules, Cloud Eye notifies you by emails, or by sending messages to server addresses, allowing you to monitor the cloud resource status and changes in real time.

- Monitoring panel

  The panel enables you to view cross-service and cross-dimension monitoring data. It displays key metrics, providing an overview of the service status and monitoring details that you can use for troubleshooting.

- Resource group

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

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 the metric reaches the threshold specified in an alarm rule, Cloud Eye notifies you by emails, or by sending HTTP/HTTPS messages to an IP address of your choice, allowing you to keep track of the statuses of cloud services and enabling you to build smart alarm handling programs.

Batch Creation of Alarm Rules

Alarm templates allow you to create alarm rules in batches for multiple cloud services.

3 Application Scenarios

Cloud Service Monitoring

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

Server Monitoring

By monitoring the ECS or BMS metrics, such as CPU usage, memory usage, and disk usage, you can ensure that the ECS or BMS runs normally and 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 SMN API to send notifications, allowing you to identify root causes of performance issues.

Capacity Expansion

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

Custom Monitoring

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

Event Monitoring

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.

4 Basic Concepts

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

- **Metrics**
- **Rollup**
- **Monitoring Panels**
- **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.

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.

Monitoring Panels

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

Topics

A topic is used to publish messages and subscribe to notifications. Topics provide you with one-to-many publish subscription and message notification functions.

You can send messages to different types of endpoints with just one message request. Cloud Eye uses SMN to notify you of cloud service resource changes, enabling you to track the cloud service status in a timely manner.

Alarm Rules

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

Alarm Templates

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

Projects

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

5 Constraints

Table 5-1 lists Cloud Eye resource limits for a user. For details about how to adjust quotas, see Quota Adjustment.

Table 5-1 Resources and their default quotas

Resource	Default Quota
Alarm rules that can be created	1,000
Custom alarm templates that can be created	200
Alarm rules that can be added to an alarm template	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	5
Monitoring data records that can be exported at a time	400 **NOTE** If 400 monitored objects are to be exported, only records of one metric can be exported. If 80 monitored objects are to be exported, records of 5 metrics can be exported.

6 Security

6.1 Shared Responsibilities

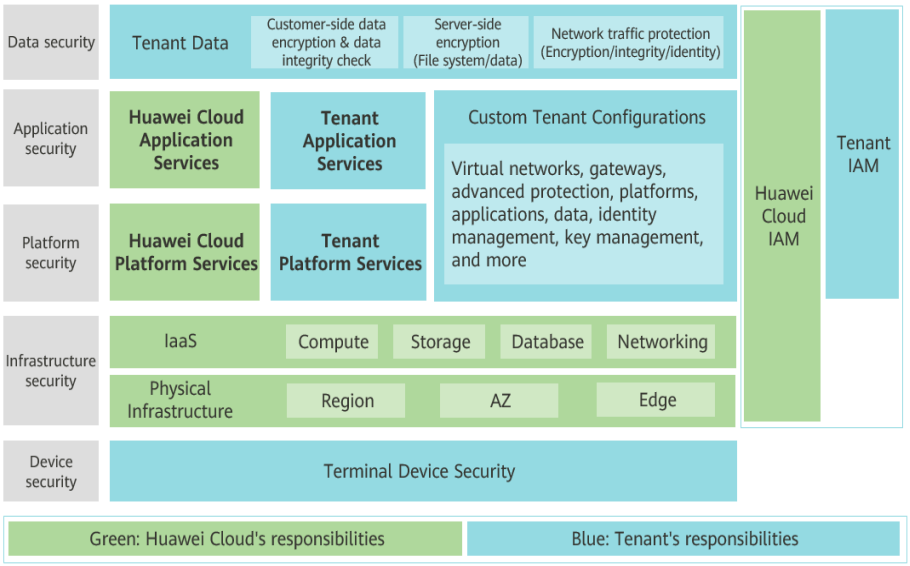
Huawei guarantees that its commitment to cyber security will never be outweighed by the consideration of commercial interests. To cope with emerging cloud security challenges and pervasive cloud security threats and attacks, Huawei Cloud builds a comprehensive cloud service security assurance system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

Figure 6-1 illustrates the responsibilities shared by Huawei Cloud and users.

- **Huawei Cloud**: Ensure the security of cloud services and provide secure clouds. Huawei Cloud's security responsibilities include ensuring the security of our IaaS, PaaS, and SaaS services, as well as the physical environments of the Huawei Cloud data centers where our IaaS, PaaS, and SaaS services operate. Huawei Cloud is responsible for not only the security functions and performance of our infrastructure, cloud services, and technologies, but also for the overall cloud O&M security and, in the broader sense, the security compliance of our infrastructure and services.
- **Tenant**: Use the cloud securely. Tenants of Huawei Cloud are responsible for the secure and effective management of the tenant-customized configurations of cloud services including IaaS, PaaS, and SaaS. This includes but is not limited to virtual networks, the OS of virtual machine hosts and guests, virtual firewalls, API Gateway, advanced security services, all types of cloud services, tenant data, identity accounts, and key management.

Huawei Cloud Security White Paper elaborates on the ideas and measures for building Huawei Cloud security, including cloud security strategies, the shared responsibility model, compliance and privacy, security organizations and personnel, infrastructure security, tenant service and security, engineering security, O&M security, and ecosystem security.

Figure 6-1 Huawei Cloud shared security responsibility model



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.

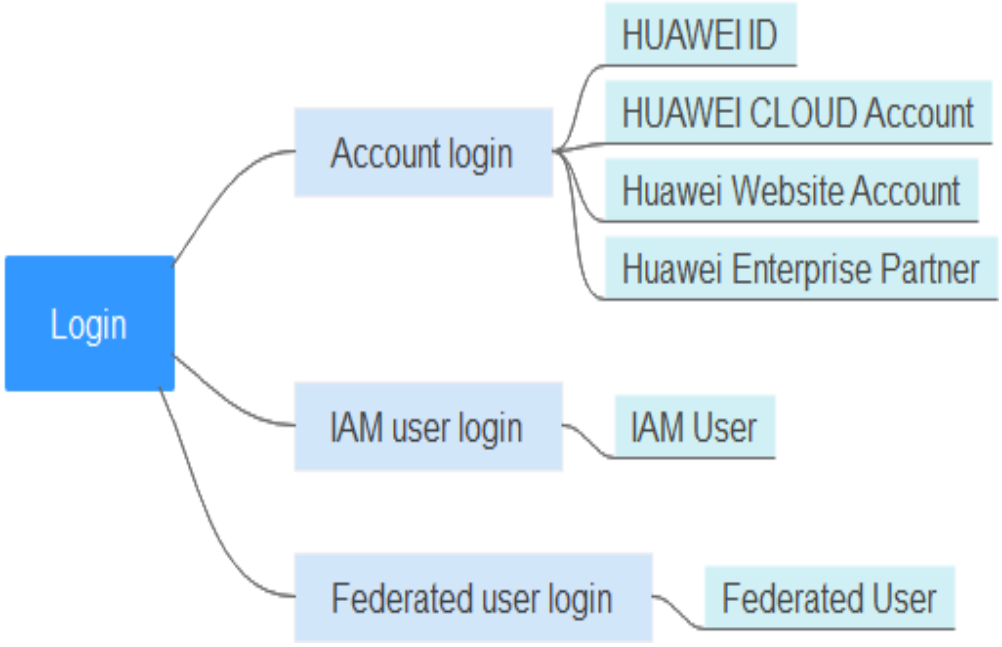
Authentication

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

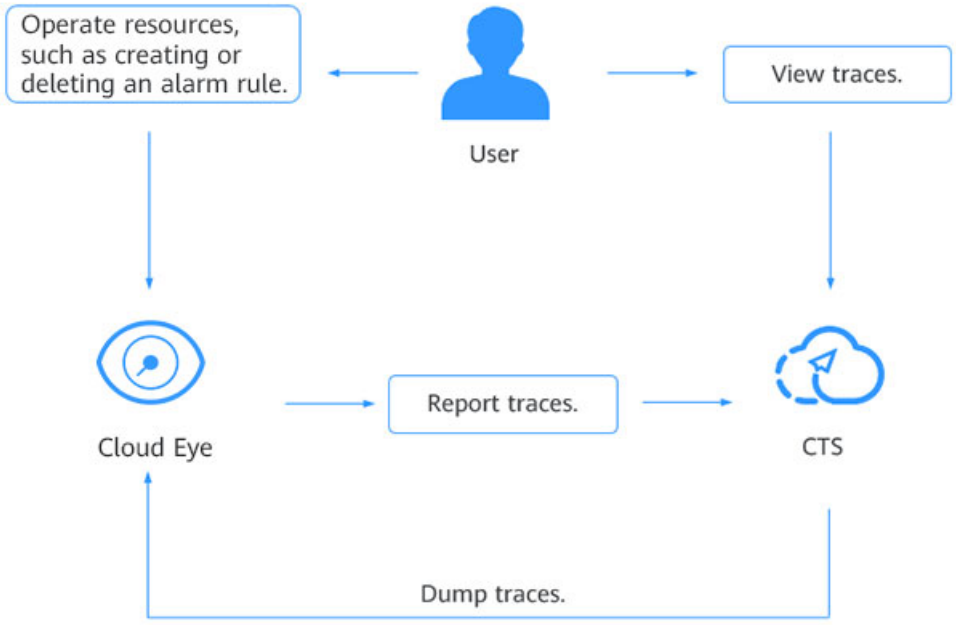
Audit

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 CTS



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 protection purposes, 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 recommend that you never put confidential or sensitive information, such as your customers' email addresses, into tags or free-form fields such as a Name field. This includes when you work with Cloud Eye or other Huawei Cloud services using the console, API, 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

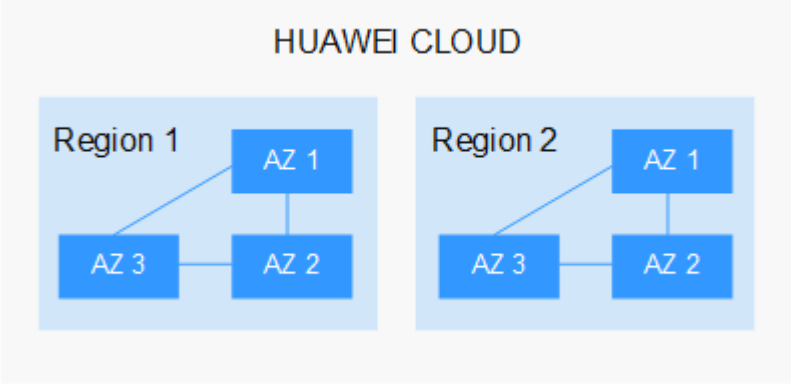
Concept

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. Select a region and 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 details, see **Regions and Endpoints**.

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 Huawei CloudHuawei Cloud resources.

With IAM, you can use your Huawei Cloud 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 of other cloud services 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 Huawei Cloud account does not require individual IAM users for permissions management, skip this section.

IAM can be used free of charge. You pay only for the resources in your account. For more information about IAM, see **What Is IAM**.

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. 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 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.

  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 the system-defined permissions supported by Cloud Eye.

Table 8-1 System-defined permissions

System-Defined Role/ Policy Name	Description	Type	Dependency
CES FullAccess	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 of the involved services. For details, see **Supported Cloud Services**.
CES ReadOnlyAccess	Read-only permissions for Cloud Eye. Users granted these permissions can only view Cloud Eye data.	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**.

System-Defined Role/ Policy Name	Description	Type	Dependency
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**: a global policy, which must be assigned in the Global project

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 FullAccess	CES ReadOnlyAccess	CES Administrator (The Tenant Guest policy must be added at the same time.)	Tenant Guest
Monitoring Overview	Viewing monitoring overview	√	√	√	√
	Viewing full screen monitoring	√	√	√	√
Monitoring Panels	Creating a monitoring panel	√	×	√	×
	Viewing full screen monitoring	√	√	√	√

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

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

Feature	Operation	CES FullAccess	CES ReadOnlyAccess	CES Administrator (The Tenant Guest policy must be added at the same time.)	Tenant Guest
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.)	×
	Restoring the Agent configurations	√ (You must have the **Security Administrator** and **ECS FullAccess** permissions.)	×	√ (You must have the **Security Administrator** and **ECS FullAccess** permissions.)	×

Feature	Operation	CES FullAccess	CES ReadOnlyAccess	CES Administrator (The Tenant Guest policy must be added at the same time.)	Tenant Guest
	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	√ (See **Supported Cloud Services**.)	√ (See **Supported Cloud Services**.)	√	√
	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	√	√	√	√

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

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 FullAccess**, or **CES ReadOnlyAccess** policy to the user group to which the user belongs 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

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 FullAccess**, or **CES ReadOnlyAccess** 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** permission, 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*.

