Cloud Eye

Service Overview

Issue	01
Date	2022-09-30

HUAWEI TECHNOLOGIES CO., LTD.

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

Contents

1 What Is Cloud Eye?....1

2 Advantages.... 3

3 Application Scenarios.... 4

4 Basic Concepts....6

5 Constraints.... 8

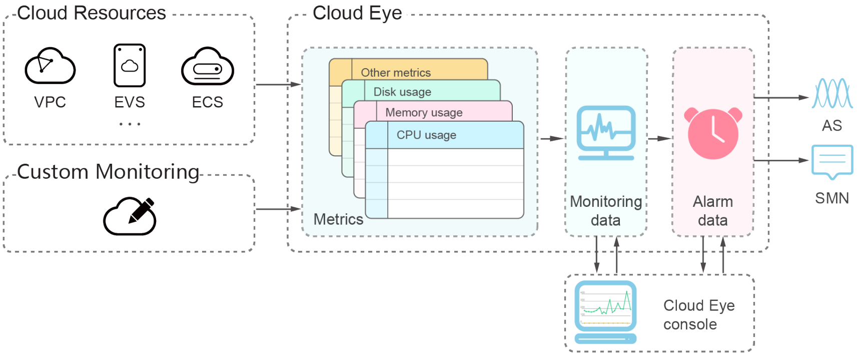
6 Region and AZ....10

7 Permissions Management.... 11

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 lastic 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 run normally and prevent service interruptions caused by overuse of resources.

Performance Issues

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

Capacity Expansion

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

Custom Monitoring

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

Log Monitoring

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

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 User resource limits

Item	Maximum Number Allowed
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
Monitoring panels that can be created	20
Graphs that can be added to a monitoring panel	24
Instances that can be selected for single alarm rule creation	50
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

Item	Maximum Number Allowed
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 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. to support high-availability systems.

Selecting a Region

If your target users are in Europe, select the **EU-Dublin** region.

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.

7 Permissions Management

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

You can grant users permissions by using roles and policies.

- Roles: A type of coarse-grained authorization mechanism that defines permissions related to user responsibilities. This mechanism provides only a limited number of service-level roles for authorization. When using roles to grant permissions, you also need to assign other roles on which the permissions depend to take effect. However, roles are not an ideal choice for fine-grained authorization and secure access control.

- Policies: A type of fine-grained authorization mechanism that defines permissions required to perform operations on specific cloud resources under certain conditions. This mechanism allows for more flexible policy-based authorization, meeting requirements for secure access control. For example, you can grant ECS users only the permissions for managing a certain type of ECSs. Most policies define permissions based on APIs. For the API actions supported by Cloud Eye, see **Permissions Policies and Supported Actions**.

Table 7-1 lists the system-defined policies supported by Cloud Eye. Dependencies are policies on which a system policy depends to take effect. For example, some Cloud Eye policies are dependent on the policies of other services. When assigning Cloud Eye permissions to users, you also need to assign dependent policies for the Cloud Eye permissions to take effect.

Table 7-1 System policies

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

Table 7-2 lists common operations supported by the Cloud Eye system policy.

Table 7-2 Common operations supported by the Cloud Eye system policy

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

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

Feature	Operation	CES Administrator (The Tenant Guest policy must be added at the same time.)	Tenant Guest	CES FullAccess	CES ReadOnlyAccess
	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 Administrator (The Tenant Guest policy must be added at the same time.)	Tenant Guest	CES FullAccess	CES ReadOnlyAccess
	Uninstalling the Agent	√ (You must have the **ECS FullAccess** permission.)	×	√ (You must have the **ECS FullAccess** permission.)	×
	Configuring process monitoring	√	×	√	×
	Configuring monitoring for a process	√	×	√	×
Cloud Service Monitoring	Viewing the cloud service list	√	√	√ (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	√	√	√	√
	Viewing details of an event	√	√	√	√

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

Helpful Links

- What Is IAM
- Creating a User and Authorizing the User to Use Cloud Eye
- Cloud Eye Custom Policies

- **Permissions Policies and Supported Actions** in *Cloud Eye API Reference*.