Best Practices

Best Practices

Issue 05

Date 2025-04-18

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 Service Monitoring on E-Commerce Platforms

1.1 Overview

E-commerce services feature large data volume and large data access, which requires large memory, fast data exchange and processing, and extremely strict monitoring.

Elastic Cloud Servers (ECSs) is a core service in the e-commerce scenarios. Therefore, a comprehensive and three-dimensional ECS monitoring system plays an important role in service stability. **Server Monitoring** provides system-wide, active, and fine-grained ECS monitoring to ensure smooth service running.

People access the websites of e-commerce platforms and make transactions. During grand annual shopping festivals such as Double 12 and 618 shopping festivals , the websites are often hit by various problems like slow page loading and long network latency when people access from different networks.

For services used by an e-commerce platform, such as Relational Database Service (RDS), Elastic Load Balance (ELB), and Virtual Private Cloud (VPC), you can use the **Cloud Service Monitoring** function. On the **Cloud Service Monitoring** page, you can gain visibility into the running status of each cloud service and usage of each metric. After setting alarm rules for cloud service metrics, you can get a more accurate picture of the health of cloud services.

An e-commerce platform involves many cloud services, such as ECS, Content Delivery Network (CDN), Auto Scaling (AS), security services, RDS, ELB, and Object Storage Service (OBS). With the **Resource Groups** function, you can view resource usages, alarms, and health status from the service perspective and manage alarm rules. This greatly reduces O&M complexity and improves O&M efficiency.

1.2 Server Monitoring

ECSs are the cores of an e-commerce platform. Slight changes in ECS performance may cause dramatic fluctuation of e-commerce services or even breakdown, resulting in huge losses.

Server Monitoring provides **Basic Monitoring** and **OS Monitoring** of different monitoring granularities. **Basic Monitoring** monitors metrics reported by ECSs. **OS Monitoring** provides server monitoring that is system-wide, active, and fine-grained after the Agent is installed on an ECS.

Scenarios

In e-commerce scenarios such as promotions, flash sales, and red-hot sellers, the number of instantaneous visits multiplies to tens to hundreds of times than that in days without activities, which results in heavy server load and slow system response.

You can configure alarm rules for ECS metrics, for example, CPU usage. When the CPU usage reaches the threshold, an alarm notification is sent to remind you to handle the exception promptly.

Prerequisites

The Agent has been installed. For details, see **Agent Installation and Configuration**.

Procedure

1. Log in to the management console.
2. In the upper left corner, select a region and a project.
3. Choose **Service List** > **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 set the parameters.
   a. You do not need to set the monitored object because it is the current ECS.
   b. Set **Method** to **Create manually**, select a metric, and configure other parameters based on **parameter description**.

      NOTE

      Take **(Agent) CPU Usage** as an example. You are advised to set its threshold to 80% because some processing performance needs to be reserved to ensure that the server can run properly. When the (Agent) CPU usage exceeds the threshold for three consecutive times, an alarm is generated.

   c. Click **Create**.

After the alarm rule is created, once the service volume soars and the specified threshold is reached, Cloud Eye immediately informs you of the resource exception.

1.3 Cloud Service Monitoring

For the RDS, ELB, and VPC services used by an e-commerce platform, you can use the **Cloud Service Monitoring** function. On the **Cloud Service Monitoring** page, you can accurately master the status of each cloud service and usage of each metric by setting alarm rules.

Procedure

1. Log in to the management console.
2. In the upper left corner, select a region and a project.
3. Choose **Service List** > **Cloud Eye**.
4. In the navigation pane on the left, choose **Cloud Service Monitoring** > **Elastic Load Balance**.
5. Locate the target load balancer and click **Create Alarm Rule** in the **Operation** column.

   The **Create Alarm Rule** page is displayed.

   NOTE

   To create alarm rules for RDS and EIP and bandwidth metrics, choose **Relational Database Service** and **Elastic IP and Bandwidth**, respectively.

   For details about other parameters, see **Creating an Alarm Rule**.

   NOTE

   - To better monitor the ELB service, you need to enable the ELB health check first. For details, see **How Do I Troubleshoot an Unhealthy Backend Server?** You are advised to set the outbound rate threshold to 80%.
   - You are advised to set the CPU usage threshold of the RDS instance to 80% and set to trigger an alarm if the threshold is exceeded for three consecutive times. Set thresholds for other RDS metrics, such as Disk Utilization, IOPS, and Database Connections in Use as required.
   - You are advised to set the outbound bandwidth usage threshold of Elastic IP and Bandwidth to 80% and trigger an alarm if the threshold is exceeded for three consecutive times. Set thresholds for other Elastic IP and Bandwidth metrics as required.
6. Click **Create**.

   If the service volume soars and the specified RDS, Elastic IP and Bandwidth, or ELB threshold is reached, Cloud Eye immediately informs you of the resource exception.

1.4 Resource Groups

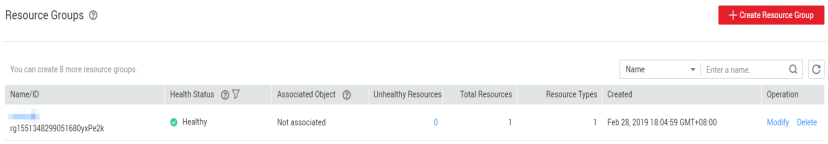
A complete e-commerce platform uses a number of cloud services, such as ECS, CDN, AS, security services, RDS, OBS, and VPC. You can create resource groups and divide resources into different groups. You can accurately view resource usages, alarms, and health status, and manage alarm rules from the service perspective on the **Resource Groups** page. This greatly reduces O&M complexity and improves O&M efficiency.

This section describes how to create a resource group.

Procedure

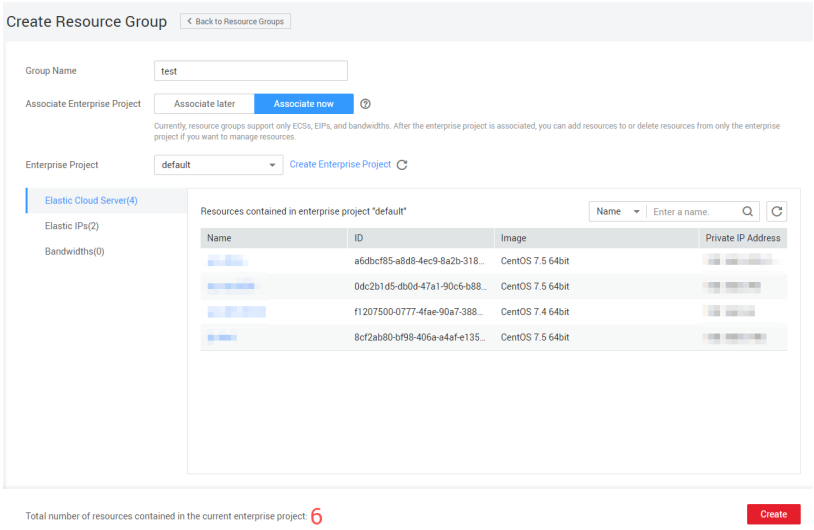
1. Log in to the management console.
2. In the upper left corner, select a region and a project.
3. Choose **Service List** > **Cloud Eye**.
4. In the navigation pane on the left, choose **Resource Groups**.
5. In the upper right corner, click **Create Resource Group**.

Figure 1-1 Create Resource Group



6. Specify a name for the group.
7. Select the target cloud service resources.

Figure 1-2 Selecting cloud service resources



8. Click **Create**.

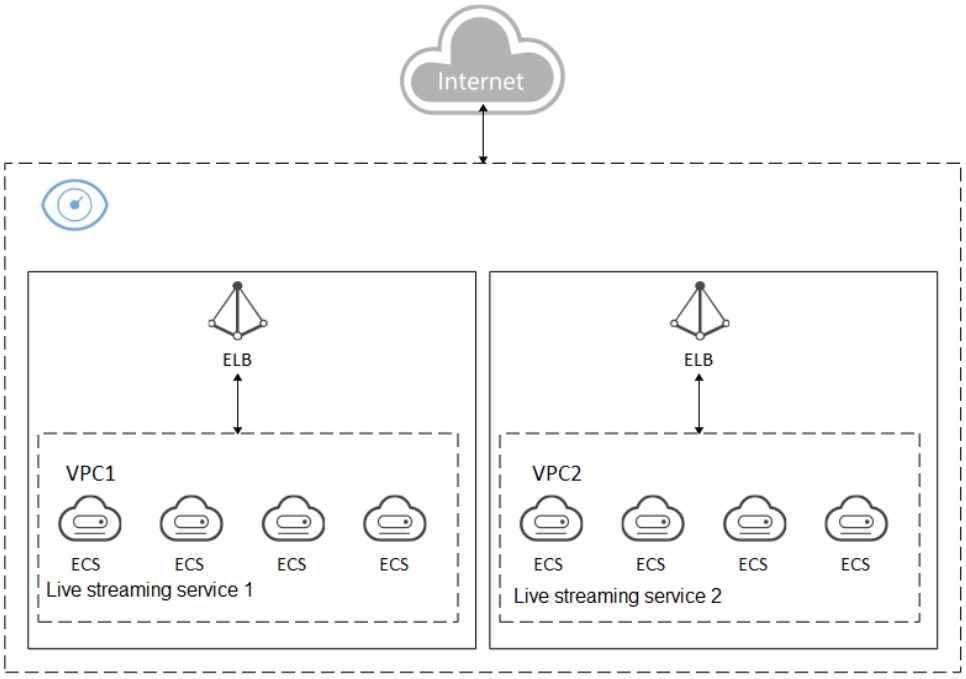
2 Live Streaming Monitoring

2.1 Overview

In the era of rapid Internet development, the demand for live video streaming is increasing. Services on Huawei Cloud, such as ECS, VPC, and ELB, provide stable resources to ensure convenient access, low latency, high concurrency, high definition, and smoothness of live streaming services. This solves the poor user experience caused by video freeze and blurring.

Figure 2-1 shows the typical architecture of live video streaming deployed on Huawei Cloud. Multiple ECSs, VPCs, and load balancers are used. ECSs are the basis of live video streaming, VPCs provide networks, and load balancers are used for traffic distribution. Subtle ECS performance changes and sudden increase of network access traffic will cause service instability. In this regard, real-time monitoring of cloud resources and timely notification of resource exceptions become increasingly important. Cloud Eye monitors ECS, VPC, and ELB resources, detects exceptions in a timely manner, and notifies users of the exceptions.

Figure 2-1 Service architecture of live streaming services



2.2 Server Monitoring

ECSs are the core of live video streaming. Slight changes in ECS performance may greatly affect other cloud services. To monitor more fine-grained metrics, you can install the Agents on ECSs. For details, see **Agent Installation and Configuration**.

This section describes how to create alarm rules for ECS CPU usage, memory usage, and disk usage. It also includes how to configure an AS policy. When the ECS CPU usage reaches 90% for five consecutive times within 5 minutes, AS automatically adds an ECS to ensure stable service running.

Create an alarm rule.

1. Log in to the management console.
2. In the upper left corner, select a region and a project.
3. Choose **Service List** > **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, set parameters as prompted.

   When configuring **Notification Object**, select a topic from the drop-down list. For details about how to create a topic, see **Creating a Topic**.

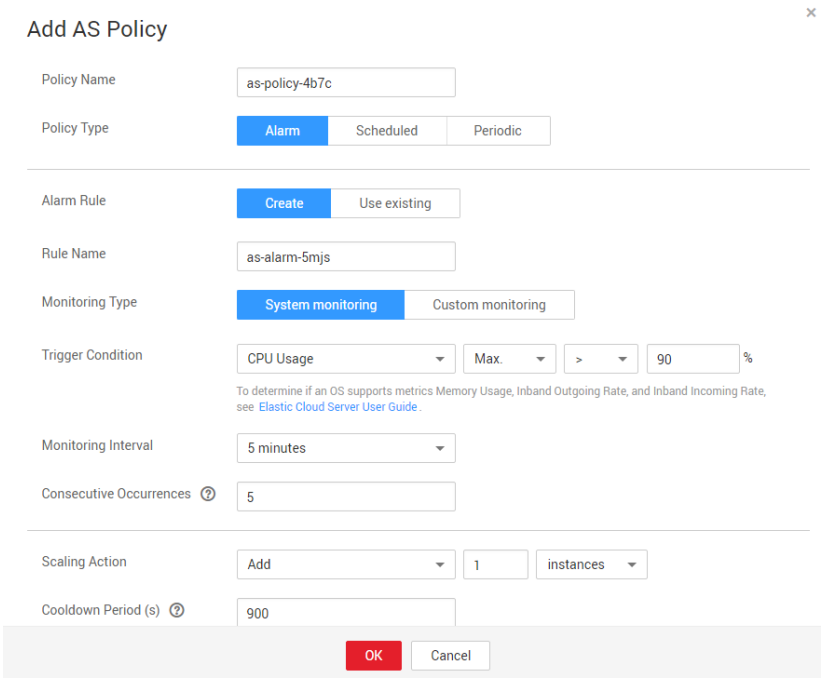
NOTE

- CPU Usage, Memory Usage, and Disk Usage are metrics for ECS basic monitoring. (Agent) CPU Usage, (Agent) Memory Usage, and (Agent) Disk Usage are metrics for fine-grained OS monitoring.
- You are advised to set **Threshold** of (Agent) CPU Usage, (Agent) Memory Usage, and (Agent) Disk Usage to **Avg. ≥ 80%**, and set **Alarm Severity** to **Major**. Create alarm rules for the three Agent metrics in which **Threshold** is set to **Avg. ≥ 90%** and **Alarm Severity** is set to **Critical**.

Configure an AS policy.

1. Choose **Computing** > **Auto Scaling**.
2. Click **Create AS Group**. For details, see **Creating an AS Group**.
3. In the AS group list, locate the created AS group and click **View AS Policy** in the **Operation** column.
4. On the **AS Policies** tab page, click **Add**. In the displayed **Add AS Policy** dialog box, set parameters based on **Figure 2-2**.

Figure 2-2 Add AS Policy



After the alarm rule and AS policy are created, if the service volume soars and the specified threshold is reached, AS automatically adds an ECS and Cloud Eye immediately informs you of the resource exception.

2.3 ELB Monitoring

In live video streaming, sudden increase of network access traffic may cause service instability. Therefore, most live video streaming platforms use ELB to automatically distribute traffic to multiple ECSs.

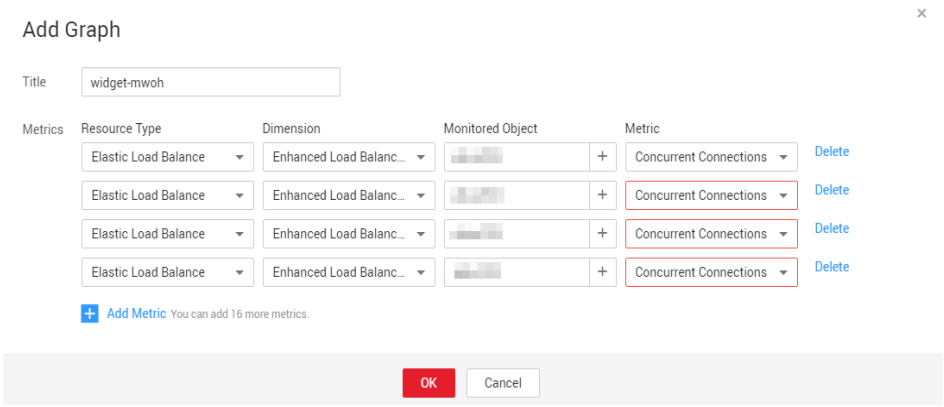
Stable and reliable load balancing is critical to the proper running of live video streaming. Cloud Eye can monitor unhealthy backend servers and concurrent connections of load balancers to ensure proper running of your services.

Procedure

1. Log in to the management console.
2. In the upper left corner, select a region and a project.
3. Choose **Service List** > **Cloud Eye**.
4. In the navigation pane on the left, choose **Dashboard** > **Monitoring Panels**.
5. Switch to the monitoring panel for which you want to add a graph. Click **Add Graph** in the upper right corner.

   In the **Add Graph** dialog box, add the concurrent connections of all enhanced elastic load balancers involved in live video streaming to the same graph.

   Figure 2-3 Add Graph

   NOTE

   The running trends of all concurrent connections in the same live video streaming must be consistent. If the trend of one or more concurrent connections is inconsistent with other trends, an exception occurs. In this case, locate the cause and rectify the fault immediately.

6. In the navigation pane, choose **Alarm Management** > **Alarm Rules** and click **Create Alarm Rule** in the **Operation** column.
7. On the **Create Alarm Rule** page, follow the prompts to set the parameters.

   When configuring **Notification Object**, select a topic from the drop-down list. For details about how to create a topic, see **Creating a Topic**.

   NOTE

   For live video streaming, you can set an alarm rule for the number of unhealthy servers. If the raw data is greater than 1 for one time, an alarm is triggered.

8. Click **Create**.

   When ELB is abnormal, Cloud Eye interworks with SMN to notify you of the resource exception in real time.

2.4 Network Monitoring

In live video streaming, random packet loss occurs when the outbound bandwidth reaches the upper limit. Therefore, attention must be paid to this metric of Elastic IP and Bandwidth.

This section describes how to set alarm rules for the outbound bandwidth usage of Elastic IP and Bandwidth.

Procedure

1. Log in to the management console.
2. In the upper left corner, select a region and a project.
3. Choose **Service List** > **Cloud Eye**.
4. In the navigation pane on the left, choose **Cloud Service Monitoring** > **Elastic IP and Bandwidth**, locate the target bandwidth or EIP, and click **Create Alarm Rule** in the **Operation** column.

   NOTE

   You are advised to configure alarm rules for the EIPs and bandwidths involved in the service. Set the threshold of **Outbound Bandwidth Usage** to **Raw data ≥ 90%** of the purchased bandwidth.
5. Set alarm rule parameters as prompted.
6. Click **Create**.

   When the bandwidth is abnormal, Cloud Eye interworks with SMN to notify you of the resource exception in real time.

3 Crowdsourcing Platforms

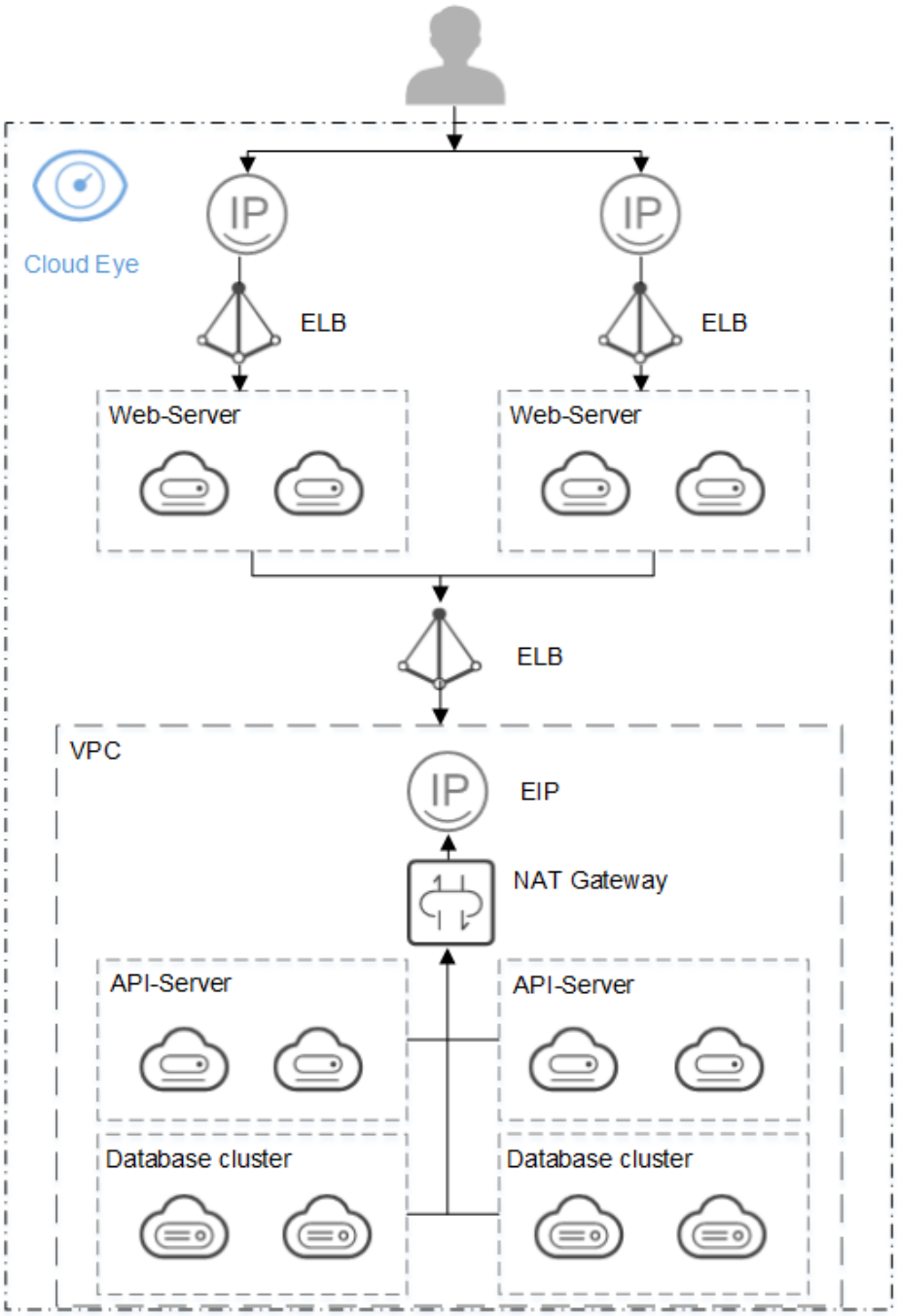
3.1 Overview

Crowdsourcing platforms, as knowledge worker sharing platforms, use the Internet to allocate jobs and connect employers with service providers. Many service providers provide customized solutions for enterprises, public institutions, and individuals to transform ideas, wisdom, and skills into business value and social value.

Figure 3-1 shows the typical architecture of the crowdsourcing platform deployed on Huawei Cloud. The core databases use the BMS clusters to deploy the database clusters. Web-Servers and API-Servers are deployed on ECSs. Web-Servers provide website search, category, store, and transaction services, and API-Servers are basic interfaces for connecting services with databases. The running statuses of BMSs and ECSs are critical to the entire service. CPU, memory, and disk usages affect the overall service status. Therefore, you need to use the server monitoring and event monitoring functions to monitor the running statuses of ECSs and BMSs at any time. For details, see **3.2 Server Monitoring** and **3.4 Event Monitoring**.

Services like VPC, NAT Gateway, and ELB provide basic network support. The network status affects the connectivity between services. Therefore, you need to use the cloud service monitoring function to monitor the running status of each service system at any time. For details, see **3.3 Network Monitoring**.

Figure 3-1 Crowdsourcing platform architecture



3.2 Server Monitoring

On crowdsourcing platforms, ECSs provide computing resources, and databases are deployed on BMSs. Therefore, BMS disk read and write rates affect the database operation speed. ECS memory and CPU usages affect the service execution speed. To monitor more fine-grained metrics, you can **install and configure the Agent** on ECSs.

You can set the thresholds of CPU usage, memory usage, and disk usage to > 80%, respectively. The following procedure uses CPU usage as an example.

Procedure

1. Log in to the management console.
2. In the upper left corner, select a region and a project.
3. Choose **Service List** > **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, set parameters as prompted.

   When configuring **Notification Object**, select a topic from the drop-down list. For details about how to create a topic, see **Creating a Topic**.

   After the alarm rule is created, when the service volume surges and the metric data reaches the threshold, Cloud Eye notifies you of the resource exception in real time through SMN emails or text messages.

3.3 Network Monitoring

During activities on a crowdsourcing platform, traffic to the website homepage, login page, and store details page increases instantaneously. Therefore, the outbound bandwidth needs to be monitored at any time.

In addition, if the number of connections increases sharply due to DDoS attacks or heavy traffic, service access becomes slow. The number of SNAT connections on days with activities is expected to be two to three times higher. Therefore, you need to monitor the number of SNAT connections at any time.

Procedure

1. Log in to the management console.
2. In the upper left corner, select a region and a project.
3. Choose **Service List** > **Cloud Eye**.
4. Choose **Cloud Service Monitoring**.
5. Locate the target bandwidth, elastic IP, and NAT gateway, and click **Create Alarm Rule** in the **Operation** column.

   NOTE

   - In this example, the number of SNAT connections is 10,000 in normal days, and that number is two to three times in peak hours. Therefore, you are advised to set the threshold of SNAT connections to 30,000.
   - You are advised to set the threshold of the outbound bandwidth usage to 80%.
6. Click **Create**.

   When the bandwidth is abnormal, Cloud Eye notifies you of the resource exception in real time through the SMN service.

3.4 Event Monitoring

During service running, you can delete, reboot, or stop ECSs and BMSs, and delete NICs or security group rules for the ECSs and BMSs at any time as required. You

can use the event monitoring function to monitor the running status of ECSs and BMSs at any time.

Procedure

1. Log in to the management console.
2. In the upper left corner, select a region and a project.
3. Choose **Service List** > **Cloud Eye**.
4. In the navigation pane on the left, choose **Event Monitoring**. Select an event and click **Create Alarm Rule** in the **Operation** column.

   NOTE

   This section uses **Delete ECS** as an example. You can also create alarm rules for other events, such as **Reboot ECS**, **Stop ECS**, and **Delete NIC** based on service requirements.

   When the ECSs or BMSs are abnormal, Cloud Eye notifies you of the resource exception in real time through the SMN service.

4 Best Practices of Event Monitoring

4.1 ECS Events

Elastic Cloud Server (ECS) is a cloud server that provides scalable, on-demand computing resources for secure, flexible, and efficient applications. ECSs are the core of various services. Slight changes in ECS performance, abnormal running, and automatic recovery, may greatly affect the applications that run on the ECS.

Therefore, elastic load balancers are required to distribute access traffic to multiple backend ECSs based on forwarding policies. Traffic distribution expands the external service capability of the application system. This eliminates single point of failures (SPOFs), thereby improving the application system availability. The event monitoring function of Cloud Eye can monitor ECS running exceptions and automatic recovery. You can subscribe to the ECS event notification when changes occur.

Table 4-1 Key ECS events

Event Name	Event Description	Handling Method
Restart triggered due to hardware fault	ECSs on a faulty host would be automatically migrated to another properly-running host. During the migration, the ECSs were restarted and Cloud Eye sent an event Restart triggered due to hardware fault. After the migration is complete, Cloud Eye sent an event Restart completed due to hardware failure.	This event indicates that a fault has occurred and the ECS cannot be used. In this case, you need to replace the ECS or direct traffic to other ECSs.
Restart completed due to hardware failure		This event indicates that the ECS is working properly and can be used again.

Procedure

1. Log in to the management console.
2. In the upper left corner, select a region and a project.
3. Choose **Service List** > **Cloud Eye**.
4. In the navigation pane on the left, choose **Event Monitoring**. In the upper right corner, click **Create Alarm Rule** and set parameters as prompted.

   NOTE

   In this example, **Event Name** of one alarm policy is set to **Restart triggered due to hardware fault** and of another policy is set to **Restart completed due to hardware failure**. For details about the parameters, see **Creating an Alarm Rule to Monitor an Event**.
5. Click **Create**.

   When abnormal ECS events occur, Cloud Eye notifies you in real time through the SMN service.

4.2 RDS Events

RDS is an online relational database service based on the cloud computing platform. RDS is reliable, scalable, and easy to manage, and immediately ready for use. When using relational databases, you need to pay attention to the database status. You can use event monitoring to track abnormal events to ensure stable service running.

Table 4-2 Key RDS events

Event Name	Event Description	Handling Method
DB instance creation failure	Generally, DB instances fail to be created because the number and quota of disks are small, and the underlying resources are exhausted.	Check the number and quota of disks. Release resources and create DB instances again.
Full backup failure	A single full backup failure does not affect the files that have been successfully backed up, but prolongs the incremental backup time during the point-in-time restore (PITR).	Create a manual backup again.

Event Name	Event Description	Handling Method
Primary/standby switchover failure	The standby DB instance does not take over services from the primary DB instance due to some network or server failures. The original primary DB instance continues to provide services within a short time.	Check whether the connection between the application and the database is re-established.
Replication status abnormal	The replication delay between the primary and standby DB instances is too long (usually occurs when a large amount of data is written to databases or a large transaction is performed). During off-peak hours, the replication delay between the primary and standby DB instances gradually decreases. Another possible cause is that the network between the primary and standby DB instances is interrupted. However, the network interruption does not interrupt data read and write of a single DB instance, and customers' applications are unaware of the interruption.	Submit a service ticket for processing.
DB instance faulty	A single or primary DB instance is faulty due to a disaster or a server failure. This event is critical and may cause database service unavailability.	Check whether an automated backup policy has been configured for the DB instance and submit a service ticket for processing.

Event Name	Event Description	Handling Method
Failure of changing single DB instance to primary/standby	During the standby DB instance creation or after the standby DB instance is created, the configuration synchronization between the primary DB instance and the standby DB instance is faulty. Generally, the fault is caused by insufficient resources of the data center where the standby DB instance is located. This event does not cause the data read and write interruption of the original single DB instance, and customers' applications are unaware of this event.	Submit a service ticket for processing.
Replication status recovered	The replication delay between the primary and standby DB instances is within the normal range, or the network connection between the two is restored.	No action is required.
DB instance recovered	RDS uses high availability tools to rebuild the standby DB instance for disaster recovery.	No action is required.

Procedure

1. Log in to the management console.
2. In the upper left corner, select a region and a project.
3. Choose **Service List** > **Cloud Eye**.
4. In the navigation pane on the left, choose **Event Monitoring**. In the upper right corner, click **Create Alarm Rule** and set parameters as prompted.

   NOTE

   In this example, **Event Name** is set to **Full backup failure**. Set the event name based on the site requirements. For details about other parameters, see **Creating an Alarm Rule to Monitor an Event**.

   Click **Create**.
5. When abnormal DB instance events occur, Cloud Eye notifies you in real time through the SMN service.

4.3 EIP Events

VPC enables you to build isolated, configurable, and manageable virtual networks for ECSs, improving the security of your resources on the cloud and simplifying network deployment.

You can bind an EIP assigned in a VPC to your ECS to access the Internet. Different EIPs can share a bandwidth, reducing your bandwidth costs.

With the event monitoring function, Cloud Eye monitors the EIP status. This prevents abnormal events and packet loss that affect your services. You can subscribe to the EIP event notification when changes occur.

Table 4-3 Key EIP events

Event Name	Event Description	Handling Method
EIP bandwidth overflow	If this event is reported, the bandwidth exceeds the purchased bandwidth, which may slow down the network or cause packet loss. **NOTE** EIP bandwidth overflow is available only in the following regions: CN North-Beijing1, CN North-Beijing4, CN North-Ulanqab1, CN East-Shanghai1, CN East-Shanghai2, CN Southwest-Guiyang1, and CN South-Guangzhou.	Check whether the EIP bandwidth keeps increasing and whether services are normal. Expand capacity if required.
EIP blocked	If the bandwidth exceeds 5 Gbit/s, the traffic is blocked. That is, the traffic is directly discarded. This indicates that the bandwidth exceeds the threshold or the system suffers from attacks (generally DDoS attacks). If the EIP unblocked event is reported, the blocking has been resolved.	Replace the EIP to prevent services from being affected. In addition, check the blocking cause and rectify the fault.
EIP unblocked		Use the unblocked EIP again to avoid resource waste.

Procedure

1. Log in to the management console.
2. In the upper left corner, select a region and a project.
3. Choose **Service List** > **Cloud Eye**.

4. In the navigation pane on the left, choose **Event Monitoring**. In the upper right corner, click **Create Alarm Rule** and set parameters as prompted.

   NOTE

   In this example, **Event Name** is set to **EIP bandwidth overflow**. For details about other parameters, see **Creating an Alarm Rule to Monitor an Event**.

5. Click **Create**.

   When abnormal EIP events occur, Cloud Eye notifies you in real time through the SMN service.

5 Resource Group Monitoring

Scenarios

Cloud Eye provides the resource group and alarm functions. How to effectively group and monitor resources and receive alarm notifications of the resources in different groups?

This section will give the answer.

Assume that there are four ECSs, namely ECS-01, ECS-02, ECS-03, and ECS-04. ECS-01 and ECS-02 are used by the development team. ECS-03 and ECS-04 are used by the test team. You need to obtain the running status of the two ECSs in the development team in a timely manner, including their CPU usage, idle CPU usage, average load, I/O usage, disk usage, memory usage, and percentage of total inode used.

Table 5-1 ECS list and group planning

ECS Name	Group	Whether to Install the Agent	Department
ECS-01	Development team resources	Yes	Development team
ECS-02	Development team resources	Yes	Development team
ECS-03	N/A	No	Test team
ECS-04	N/A	No	Test team

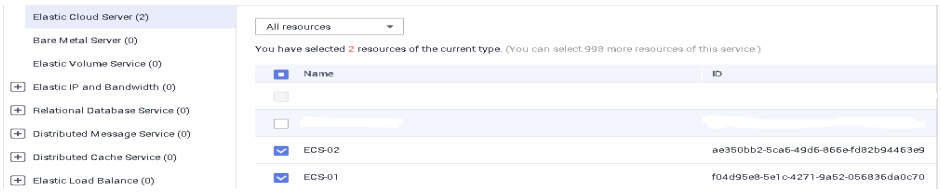
Prerequisites

The Agent has been installed on ECS-01 and ECS-02. For details, see **Agent Installation and Configuration**.

Step 1 Creating a Resource Group

1. Log in to the management console.
2. In the upper left corner, select a region and a project.
3. Choose **Service List** > **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 as prompted. In this example, enter **Development-group-resources**.
7. Select the target cloud service resources.

   Figure 5-1 Selecting cloud service resources

8. Click **Create**.

Step 2 Creating a Topic and Configuring the Notification Object

When resource exceptions occur, an alarm notification can be sent to the configured topic subscribers.

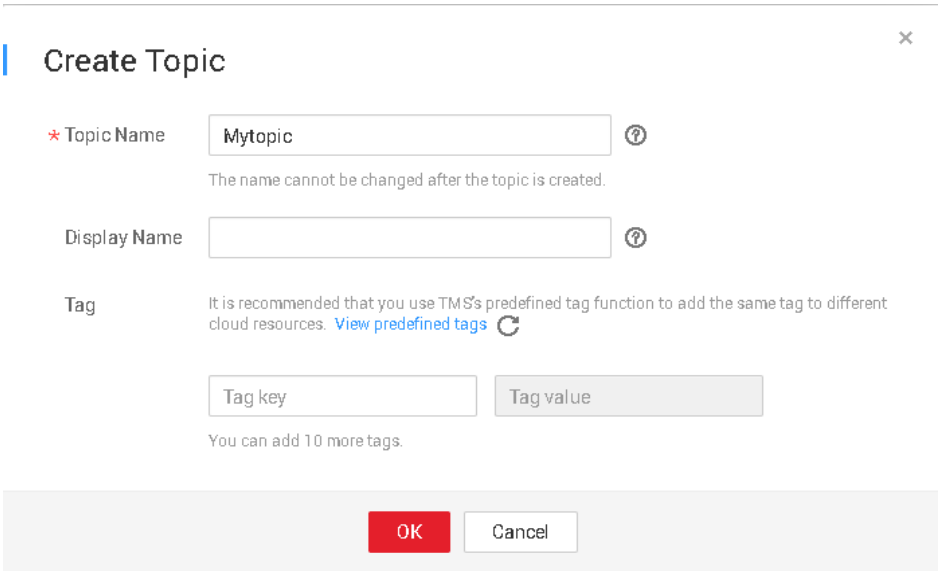
1. Log in to the management console.
2. In the upper left corner, select a region and a project.
3. Under **Application**, select **Simple Message Notification**.

   The SMN console is displayed.
4. In the navigation pane on the left, choose **Topic Management** > **Topics**.

   The **Topics** page is displayed.
5. In the upper right corner, click **Create Topic**.

   The **Create Topic** dialog box is displayed.

Figure 5-2 Create Topic



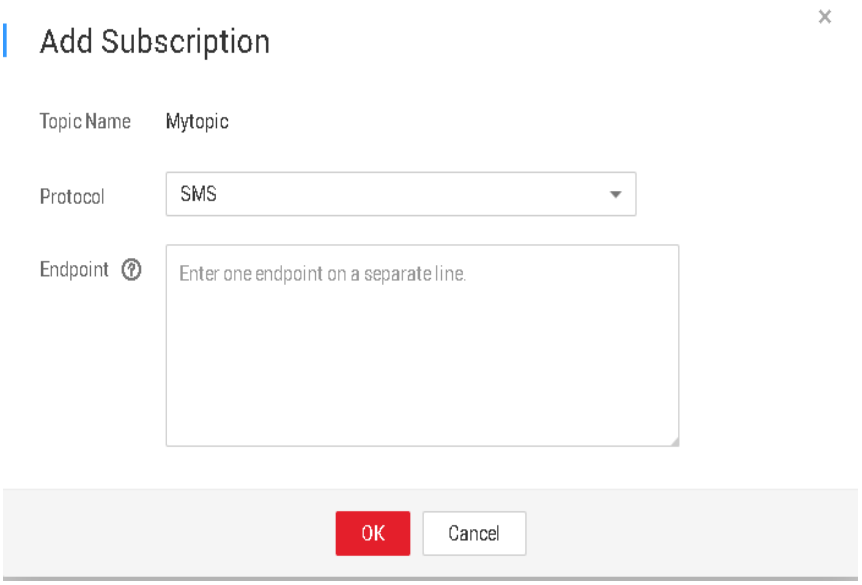
6. Enter a topic name and display name.
7. Click **OK.**

   The topic you created is displayed in the topic list.

   NOTE

   Click the topic name to view the topic details and the total number of topic subscriptions.
8. In the topic list, locate the new topic. In the **Operation** column, click **More** and select **Add Subscription**.

Figure 5-3 Add Subscription



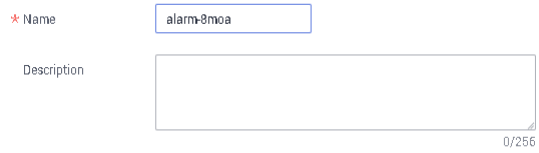
9. Specify the subscription protocol and endpoints.
10. Click **OK**.

    The subscriptions you added are displayed in the subscription list.

Step 3 Creating an Alarm Rule

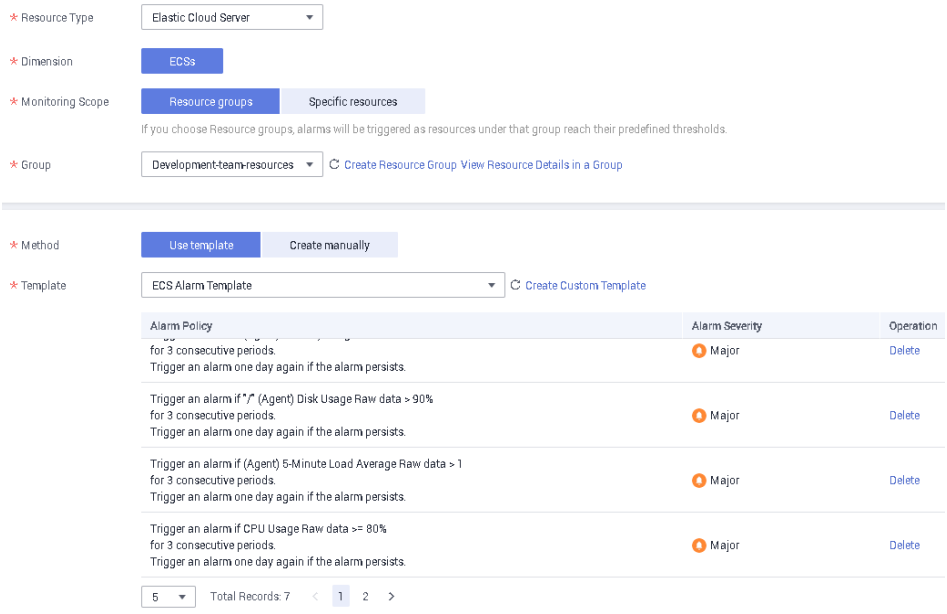
1. Log in to the management console.
2. In the upper left corner, select a region and a project.
3. Choose **Service List** > **Cloud Eye**.
4. In the navigation pane on the left, choose **Alarm Management** > **Alarm Rules**.
5. In the upper right corner, click **Create Alarm Rule**.
6. On the **Create Alarm Rule** page, follow the prompts to set the parameters.
   a. Set the alarm rule name.

      Figure 5-4 Setting an alarm rule name

   b. Set the monitored object and alarm triggering conditions.

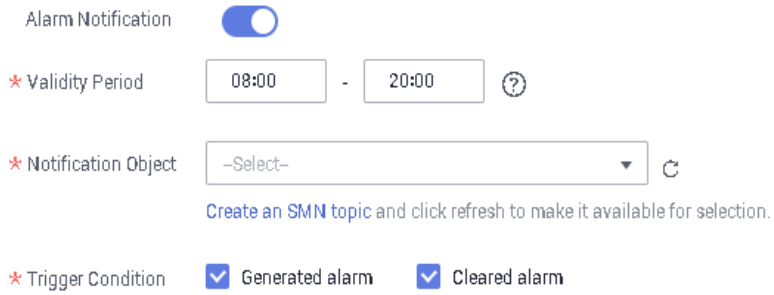
      Figure 5-5 Configuring an alarm rule

   > **NOTE**
   >
   > Set **Group** to **Development-group-resources** created in **Step 1 Creating a Resource Group**.

   c. Set **Alarm Notification** parameters.

Figure 5-6 Configuring alarm notifications



NOTE

- Note: When configuring **Notification Object**, select **Mytopic** created in **Step 2 Creating a Topic and Configuring the Notification Object**.

d. Click **Create**.

After the alarm rule is added, if the metric data reaches the threshold, Cloud Eye immediately informs you that the metric data of group **Development group resources** (ECS-01 and ECS-02) is abnormal through SMN.

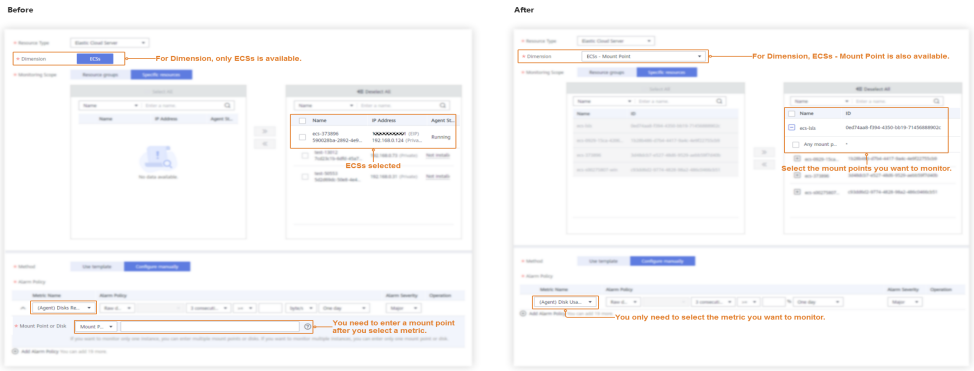
6 Configuring an Alarm Rule for the Disk Usage of All Mount Points on an ECS

Scenarios

Cloud Eye allows you to configure alarm rules for all mount points of an ECS. This section describes how to configure alarm rules for the disk usage of all mount points on an ECS.

- The mount point dimension is added to metric disk usage. When you configure a new alarm rule for the disk usage, you need to select the **ECS - Mount Point** dimension.
- If you have configured an alarm rule for **Any mount point** of an ECS, the alarm rule will automatically apply to new mount points of the ECS.
- If you have configured an alarm rule for the disk usage of the mount point, when you modify the alarm rule, the system prompts you to split the alarm rule into multiple rules in different dimensions. You are advised to select all mount points for the new alarm rules.

Figure 6-1 Alarm rule configuration before and after optimization



Prerequisites

The Agent has been installed on the ECS.

Procedure

1. Log in to the management console.
2. Choose **Service List** > **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, configure **Name** and **Enterprise Project** as prompted.
5. Set **Resource Type** to **Elastic Cloud Server** and **Dimension** to **ECSs - Mount Point**.
6. Set **Monitoring Scope** to **Specific resources**. In the resource list, select **Any mount point** of your target ECS. (You are advised to click **Select All** to select all mount points of all ECSs under the account.)
7. Select **(Agent) Disk Usage** for **Metric Name** and configure an alarm policy.
8. If you want to receive alarm notifications, enable **Alarm Notification** and select the notification object and method.

7 Suggestions on Cloud Eye Security Configuration

This section provides actionable guidance for enhancing the overall security of Cloud Eye. You can continuously evaluate the security of Cloud Eye and combine different security capabilities to enhance overall defense. By doing this, stored data can be protected from leakage and tampering both at rest and in transit.

Consider the security configurations from the following aspects:

- **Granting User Permissions Using Access Control Capabilities**
- **Protecting Privacy and Sensitive Information Through Data Masking**
- **Enabling CTS to Record All Cloud Eye Access Operations**

Granting User Permissions Using Access Control Capabilities

You need to grant necessary permissions to IAM users with different roles to prevent data leakage or misoperations caused by excessive permissions

To better isolate and manage permissions, you are advised to configure independent IAM administrators and grant them permissions to manage IAM policies. An IAM administrator can create different user groups based on your service requirements. User groups correspond to different data access scenarios. By adding users to user groups and binding IAM policies to user groups, the IAM administrator can grant different data access permissions to employees in different departments based on the principle of least privilege. For details, see **Login Protection** and **Login Authentication Policy**.

Protecting Privacy and Sensitive Information Through Data Masking

When a service request includes sensitive information, you are advised to use the data masking function. On the data masking page, create masking configurations for your components. The platform will then replace sensitive information in traces with a globally unique random character string (**Hash code** mode) or a fixed number of asterisks (*) (**Mask** mode). After the configuration is applied, you can go to the tracing page to view the trace details.

Enabling CTS to Record All Cloud Eye Access Operations

Cloud Trace Service (CTS) is a log audit service intended for Huawei Cloud security. It allows you to collect, store, and query cloud resource operation records. You can use these records to track resource changes, analyze security compliance, and locate faults.

After you enable CTS and configure a tracker, CTS records management traces of Cloud Eye for auditing. For details about Cloud Eye operations recorded by CTS, see **Key Cloud Eye Operations**.

