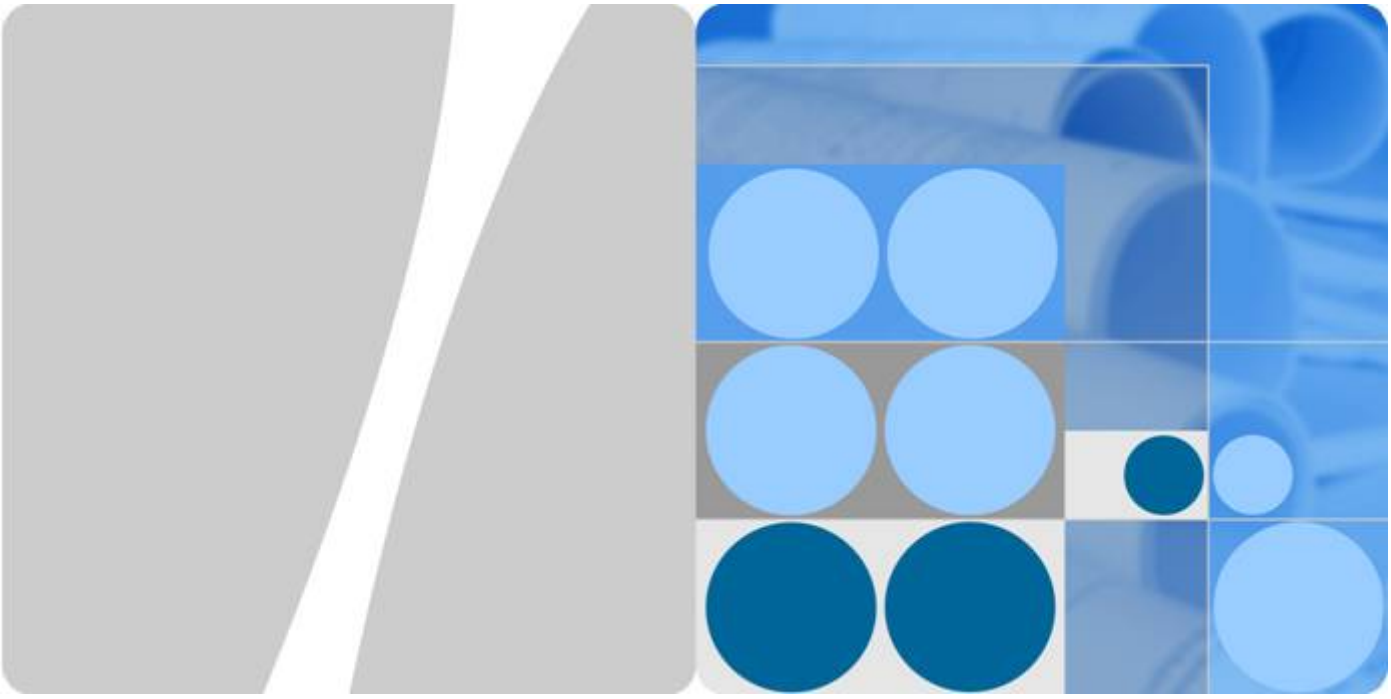


Cloud Eye

FAQs

Issue 01

Date 2022-09-30

HUAWEI TECHNOLOGIES CO., LTD.

HUAWEI

Trademarks and Permissions


and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.
All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

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

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

Huawei Technologies Co., Ltd.

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

Website: https://www.huawei.com

Email: support@huawei.com

Contents

1 General Consulting

1.1 What Is Rollup?

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

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

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

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

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

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

Choose whichever rollup method best meets your service requirements.

1.2 How Long Is Metric Data Retained?

Metric data includes raw data and rolled-up data.

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

Table 1-1 Retention periods for rolled-up data

Rollup Period	Retention Period
5 minutes	10 days
20 minutes	20 days
1 hour	155 days

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

1.3 How Many Rollup Methods Does Cloud Eye Support?

Cloud Eye supports the following rollup methods:

- Average

  If **Avg.** is selected for **Statistic**, Cloud Eye calculates the average value of metrics collected within a rollup period.
- Maximum

  If **Max.** is selected for **Statistic**, Cloud Eye calculates the maximum value of metrics collected within a rollup period.
- Minimum

  If **Min.** is selected for **Statistic**, Cloud Eye calculates the minimum value of metrics collected within a rollup period.
- Sum

  If **Sum** is selected for **Statistic**, Cloud Eye calculates the sum of metrics collected within a rollup period.
- Variance

  If **Variance** is selected for **Statistic**, Cloud Eye calculates the variance value of metrics collected within a rollup period.

  NOTE

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

1.4 How Can I Export Collected Data?

1. On the Cloud Eye console, choose **Cloud Service Monitoring** or **Server Monitoring**.
2. Click **Export Data**.

3. Configure the time range, period, resource type, dimension, monitored object, and metric.
4. Click **Export**.

NOTE

You can export data for multiple metrics at a time to a CSV file.

- The first row in the exported monitoring report displays the username, region, service, instance name, instance ID, metric name, metric data, time, and timestamp. You can view historical monitoring data.
- To convert the time using a Unix timestamp to the time of the target time zone, perform the following steps:
  a. Use Excel to open a .csv file.
  b. Use the following formula to convert the time:

     Target time = [Unix timestamp/1000 + (Target time zone) x 3600]/86400 + 70 x 365 + 19
  c. Set cell format to **Date**.

2 Server Monitoring

2.1 How Does the Cloud Eye Agent Obtain a Temporary AK/SK by Authorization?

To enable you to use the server monitoring function more securely and efficiently, Cloud Eye provides the latest Agent permission-granting method. That is, before installing Agents, you only need to click **Configure** on the **Server Monitoring** page of the Cloud Eye console, or select **cesgency** for **Agency** in **Advanced Options** when buying an ECS, the system automatically performs temporary AK/SK authorization for the Agents installed on all ECSs or BMSs in the region. And in the future, newly created ECSs or BMSs in this region will automatically get this authorization. This section describes the authorization as follows:

1. Authorization object

   On the Cloud Eye console, if you choose **Server Monitoring** > **Elastic Cloud Server** (or **Bare Metal Server**), selecting an ECS (or BMS), and click **One-Click Restore**, the system automatically creates an agency named **cesagency** on IAM. This agency is automatically granted to Cloud Eye internal account **op_svc_ces**.

   NOTE

   If the system displays a message indicating that you not have the required permission, obtain the permission by referring to **5.3 What Can I Do If the System Displays a Message Indicating Insufficient Permissions When I Click Configure on the Server Monitoring Page?**

2. Authorization scope

   Add the **CES Administrator** permission to internal account **op_svc_ces** in the region.

3. Authorization reason

   The Cloud Eye Agent runs on ECSs or BMSs and reports the collected monitoring data to Cloud Eye. After being authorized, the Agent automatically obtains a temporary AK/SK. As a result, you can use the Cloud Eye console or APIs to query the ECS or BMS monitoring data.

a. Security: The AK/SK used by the Agent is only the temporary AK/SK that has the **CES Administrator** permissions. That is, the temporary AK/SK has only the permissions to operate Cloud Eye resources.

b. Convenient: You only need to configure the Cloud Eye Agent once in each region instead of manually configuring each Agent.

4. If **cesagency** cannot be found on the IAM **Agencies** page after authorization, you can manually create it on the IAM console. For details, see **Creating an Agency (by a Delegating Party)**.

   NOTE

   - The name of the agency to be created must be **cesagency**.
   - If **Agency Type** is set to **Common account**, **Delegated Account** must be **op_svc_ces**.

2.2 How Can I Quickly Restore the Agent Configuration?

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

Most regions support one-click configuration restoration of the Agent. You can choose **Server Monitoring** > **Elastic Cloud Server** and click **Configure** on top of the page. After the configuration is complete, the Agent configurations of all servers in these regions are restored by default, and the **Configure** button is no longer displayed. If the system displays a message indicating that you not have the required permission, obtain the permission by referring to **5.3 What Can I Do If the System Displays a Message Indicating Insufficient Permissions When I Click Configure on the Server Monitoring Page?** After the Agent permission is granted for a region, you do not need to perform the following steps.

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

2.3 How Can I Ensure that a Newly Purchased ECS Comes with the OS Monitoring Function?

Scenarios

This topic describes how to ensure that the newly purchased ECS comes with the OS monitoring function.

NOTE

A private image can only be used in the region where it is created. If it is used in other regions, no monitoring data will be generated for the ECSs created by using this private image.

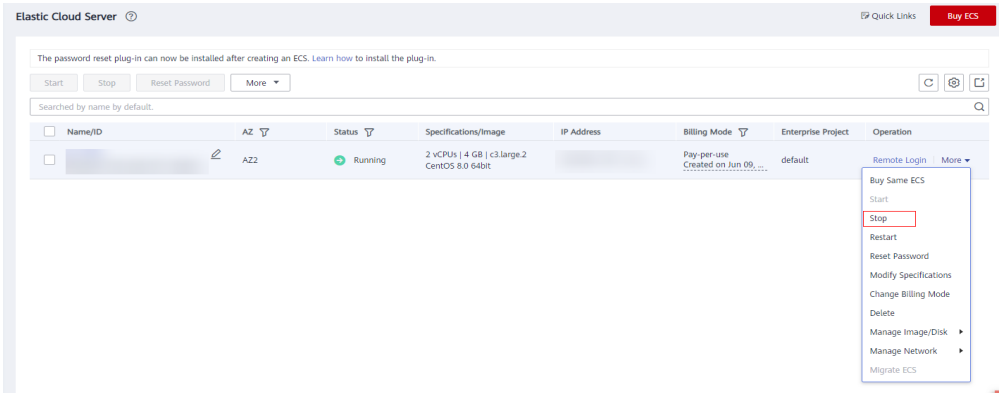
Prerequisites

An ECS with the Agent installed is available.

Procedure

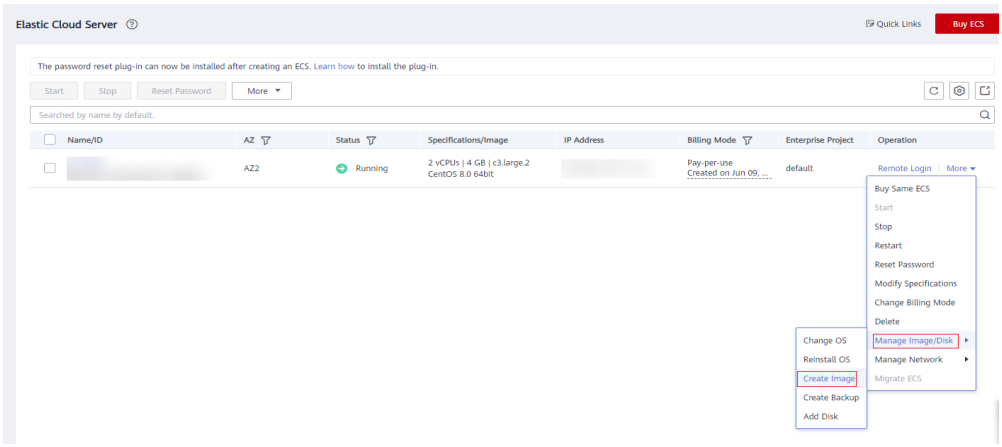
1. Log in to the ECS console. In the ECS list, locate the row containing the ECS with the Agent installed, choose **More** > **Stop** in the **Operation** column, and click **OK**.

   Figure 2-1 Stop



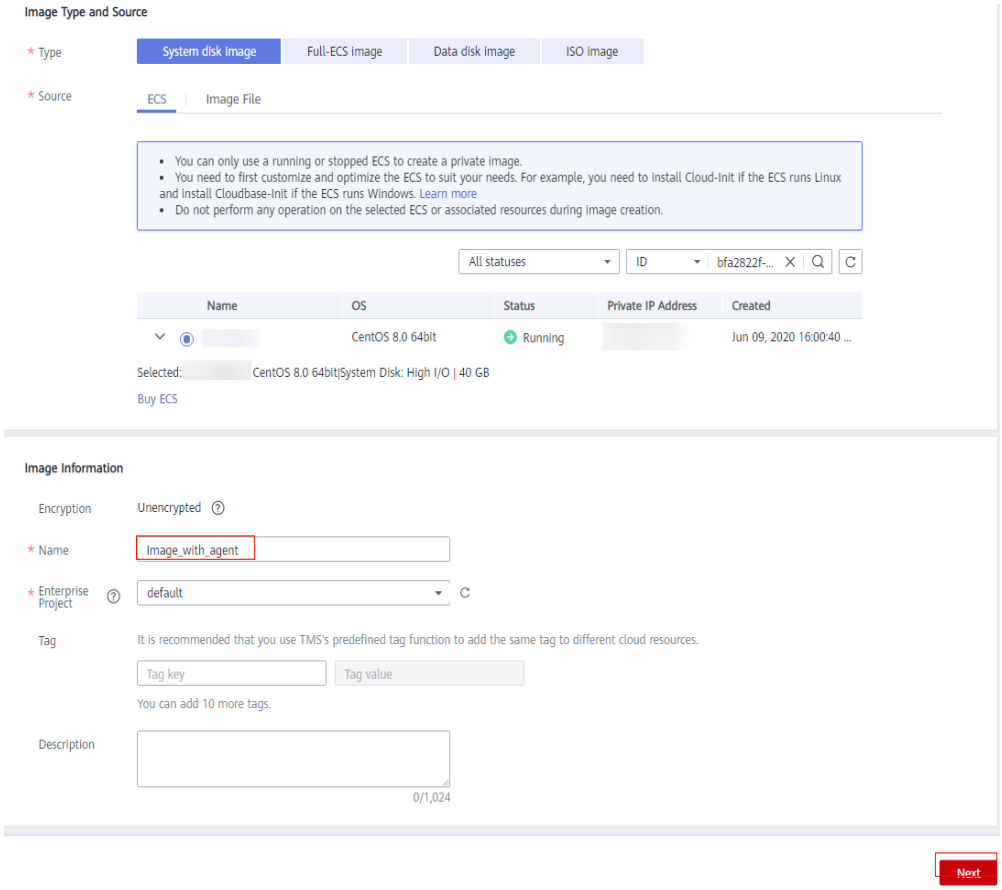
2. Choose **More** > **Manage Image/Disk** > **Create Image**.

   Figure 2-2 Create Image



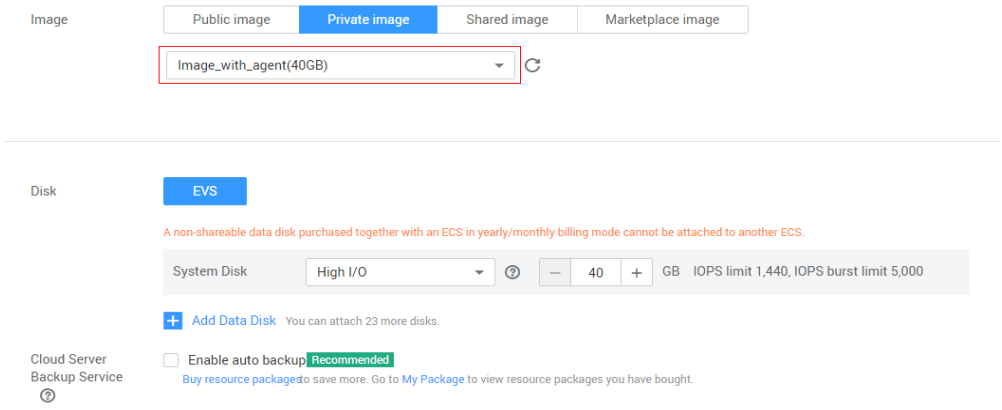
3. Set the private image name to **Image_with_agent** and click **Next**.

Figure 2-3 Image_with_agent



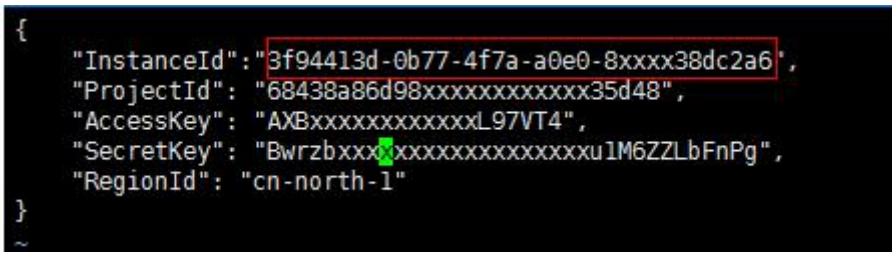
4. Purchase a new ECS and select the newly created private image **Image_with_agent**.

Figure 2-4 Image_with_agent(40GB)



5. Log in to the newly purchased ECS. Change **InstanceId** in Agent configuration file **/usr/local/telescope/bin/conf.json** to the ECS name.

Figure 2-5 Modifying the Agent configuration file



2.4 Why Is a BMS with the Agent Installed Displayed in the ECS List on the Server Monitoring Page?

Symptoms

The Agent was installed on a BMS, but the BMS is listed on the **Server Monitoring** > **Elastic Cloud Server** page on the Cloud Eye console.

Possible Causes

The Agent determines whether a server is an ECS or BMS based on the services provided by IP address 169.254.169.254. If the route for this address is changed, the Agent will consider the server to be an ECS by default.

Solution

Manually modify the Agent configuration file by adding BMS identifier **BmsFlag** and setting it to **true**.

- Linux OS: See **(Optional) Manually Configuring the Agent for Linux**.
- Windows OS: See **(Optional) Manually Configuring the Agent for Windows**.

2.5 What OSs Does the Agent Support?

The following table lists OSs compatible with the Agent. OSs not included in the table are being tested.

NOTICE

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

Table 2-1, **Table 2-2**, and **Table 2-3** list the ECS versions supported by the earlier version and new version of the Agent.

Table 2-1 ECS versions supported by the early version of the Agent

OS (64 bit)	Version
CentOS	6.3, 6.5, 6.8, 6.9, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6
OpenSUSE	13.2, 42.2
Debian	7.5.0, 8.2.0, 8.8.0, 9.0.0
Ubuntu	14.04 server, 16.04 server
EulerOS	2.2, 2.3
SUSE	Enterprise11 SP4, Enterprise12 SP1, Enterprise12 SP2
Fedora	24, 25
Oracle Linux	6.9, 7.4
CoreOS	10.10.5 **NOTE** Cloud-Init cannot be installed automatically. Install it manually in the **/** directory. To query the Agent status, run **systemctl telescoped status**.
Other	Gentoo Linux 13.0, Gentoo Linux 17.0 **NOTE** To query the Agent status, run **rc-service telescoped status**.
Windows	Windows Server 2016 Standard 64-bit Windows Server 2016 Datacenter 64-bit Windows Server 2012 R2 Standard 64-bit Windows Server 2012 R2 Datacenter 64-bit Windows Server 2008 R2 Standard 64-bit Windows Server 2008 R2 Datacenter 64-bit Windows Server 2008 R2 Enterprise 64-bit Windows Server 2008 R2 Web 64-bit
Arm general-computing	CentOS 7.4 64bit with ARM (40 GB) CentOS 7.5 64bit with ARM (40 GB) CentOS 7.6 64bit with ARM (40 GB) EulerOS 2.8 64bit with ARM (40 GB) Fedora 29 64bit with ARM (40 GB) Ubuntu 18.04 64bit with ARM (40 GB)

Table 2-2 ECS versions supported by the new version of the Agent

OS (64 bit)	Version
CentOS	6.5, 6.8, 6.9, 6.10, 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 7.8, 7.9, 8.0, 8.1, 8.2

OS (64 bit)	Version
OpenSUSE	15.0
Debian	8.2, 8.8, 9.0, 10.0
Ubuntu	16.04, 18.04, 20.04
EulerOS	2.2, 2.3, 2.5
Fedora	30
openEuler	20.3
Windows	2012, 2016, 2019

Table 2-3 System version (BMS)

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

NOTE

The GPU plug-in supports only Ubuntu 14.04 server, EulerOS 2.2, and CentOS 7.3.

2.6 What Statuses Does the Agent Have?

The Agent has the following statuses:

- **Not installed or started**: The Agent is not installed on an ECS or BMS or has been manually stopped.
- **Running**: The Agent is running and can report monitoring data.
- **Faulty**: The Agent failed to send heartbeat messages to Cloud Eye for 3 minutes running. In this case,
  - The domain name of the Agent cannot be resolved. Check whether the DNS server address is correct by referring to **Modifying the DNS Server Address and Adding Security Group Rules (Linux)**. If yes, check whether the Agent is correctly configured by referring to **(Optional) Manually Configuring the Agent (Linux)**.
  - The account is in arrears.
  - If the Agent process is faulty, restart it by following the instructions provided in **Managing the Agent**. If the restart fails, related files have been deleted by mistake. In this case, reinstall the Agent.
- **Configuration error**: No agency has been configured for the ECS or BMS, permissions of the current agency are abnormal, the current agency is invalid, security group rules of the default NIC are incorrectly configured, or the DNS is incorrectly configured.

- **Stopped**: The Agent has been manually stopped. For details about how to start the Agent, see **Managing the Agent**.

2.7 What Should I Do If the Monitoring Period Is Interrupted or the Agent Status Keeps Changes?

Symptoms

The Agent is overloaded if you see either of the following symptoms:

- On the **Server Monitoring** page of the Cloud Eye console, the Agent status frequently toggles between **Running** and **Faulty**.
- The time period in the monitoring panel is discontinuous.

Possible Causes

To prevent other services from being affected, Cloud Eye uses a circuit-breaker to automatically stop the Agent process if it is consuming too many CPU or memory resources on the server. After the Agent process is stopped, no monitoring data is reported.

Circuit-breaker Principles

By default, once per minute, the system checks whether the CPU usage of the Agent process is exceeding 30% or if the memory usage is exceeding 700 MB (the tier-2 threshold) every minute. If the tier-2 threshold is exceeded, the Agent process exits. If the tier-2 threshold is not exceeded, Cloud Eye checks whether the CPU usage is exceeding 10% or if the memory usage is exceeding 200 MB (the tier-1 threshold). If the tier-1 threshold is exceeded for three consecutive times, the Agent process exits, and the exit is logged.

After the Agent exits, the daemon process automatically starts the Agent process and checks the exit record. If there are three consecutive exit records, the Agent will hibernate for 20 minutes, during which monitoring data will not be collected.

When too many disks are attached to a server, the CPU or memory usage of the Agent process will become high. You can configure the tier-1 and tier-2 thresholds based on **Procedure** to trigger circuit-breaker according to the actual resource usages.

Procedure

1. Use the **root** account to log in to the ECS or BMS for which the Agent does not report data.
2. Go to the Agent installation path **bin**:

   cd /usr/local/telescope/bin

   NOTE

   For the Agent of the new version, run the **cd /usr/local/uniagent/extension/install/telescope/bin** command.

   In a Windows OS, the directory is **telescope_windows_amd64\bin**.

3. Modify configuration file **conf.json**.

   a. Open **conf.json**:

   vi conf.json

   b. Add the parameters listed in **Table 2-4** to the **conf.json** file.

   Table 2-4 Parameters

Parameter	Description
cpu_first_pct_threshold	Specifies the tier-1 threshold for the CPU usage. If the CPU usage of the Agent process is about 20%, set this parameter to **35**. Unit: percent (%)
memory_first_threshold	Specifies the tier-1 threshold for the memory usage. If the Agent used up about 100 MB of memory, set this parameter to **314572800** (300 MB). Unit: bytes
cpu_second_pct_threshold	Specifies the tier-2 threshold for the CPU usage. If the CPU usage of the Agent process is about 20%, set this parameter to **55**. Unit: percent (%)
memory_second_threshold	Specifies the tier-2 threshold for the memory usage. If the Agent process used up about 100 MB memory, set this parameter to **734003200** (700 MB). Unit: bytes
To query the CPU usage and memory usage of the Agent process, use the following method: • Linux **top -p** *telescope PID* • Windows View the details about the Agent process in **Task Manager**.	

   c. Save the **conf.json** file and exit:

   :wq

4. Run the following command to restart the Agent if the early version of the Agent is used:

   /usr/local/telescope/telescoped restart

   NOTE

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

   If the new version of the Agent is used, run the following command to check the PID of telescope:

ps -ef |grep telescope

After the process is forcibly stopped, wait for 3 to 5 minutes for the Agent to automatically restart. **Figure 2-6** shows an operation example.

kill -9 *PID*

Figure 2-6 Restarting the Agent

```
[root@arm1-2 ~]# ps -ef |grep telescope
root     11671     1  0 10:23 ?        00:00:00 ./telescope
root     20245 19980  0 10:33 pts/1    00:00:00 grep --color=auto telescope
[root@arm1-2 ~]#
[root@arm1-2 ~]#
[root@arm1-2 ~]# kill -9 11671
```

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

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

Procedure

1. Log in an ECS or BMS as user **root**.
2. Open the **sysctl.conf** file:

   vim /etc/sysctl.conf
3. (Permanent change) Add new ports to the **sysctl.conf** file:

   net.ipv4.ip_local_port_range=49152 65536
4. Make the modification take effect:

   sysctl -p /etc/sysctl.conf

   NOTE

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

   /usr/local/telescope/telescoped restart

   NOTE

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

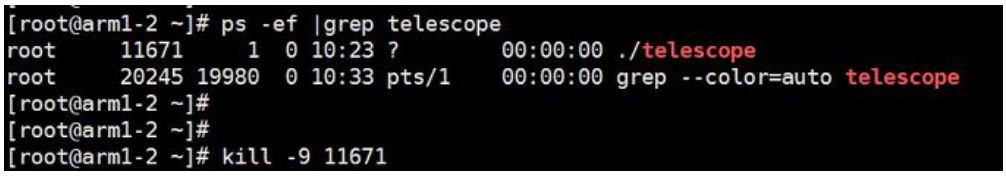
   If the new version of the Agent is used, run the following command to check the PID of telescope:

   ps -ef |grep telescope

   After the process is forcibly stopped, wait for 3 to 5 minutes for the Agent to automatically restart. **Figure 2-7** shows an operation example.

kill -9 *PID*

Figure 2-7 Restarting the Agent



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

The OS monitoring Agent sends a heartbeat message to Cloud Eye every minute. If Cloud Eye does not receive any heartbeat messages for 3 minutes, **Agent Status** is displayed as **Faulty**.

It may because:

- The domain name of the Agent cannot be resolved. Check whether the DNS server address is correct by referring to **Modifying the DNS Server Address and Adding Security Group Rules (Linux)**. If yes, check whether the Agent is correctly configured by referring to **(Optional) Manually Configuring the Agent (Linux)**.
- The account is in arrears.
- If the Agent process is faulty, restart it by following the instructions provided in **Managing the Agent**. If the restart fails, related files have been deleted by mistake. In this case, reinstall the Agent.
- The server time is inconsistent with the local standard time.
- The log path varies according to the Agent version.

  The log paths are as follows:

  – Linux:

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

    Earlier version: **/usr/local/telescope/log/ces.log**

  – Windows:

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

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

3 Alarm Notifications or False Alarms

3.1 What Is an Alarm Notification? How Many Types of Alarm Notifications Are There? How Can I Configure an Alarm Notification?

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

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

Cloud Eye can:

- Send you email notifications, or send HTTP/HTTPS messages to servers.
- Work with Auto Scaling to trigger the system to automatically add or remove servers.

3.2 What Alarm Status Does Cloud Eye Support?

There are three Cloud Eye alarm statuses: **Alarm**, **OK**, and **Insufficient data**. If an alarm rule is disabled, its status is considered as invalid, and **Disabled** is displayed.

- **Alarm**: The monitoring data meets the preset alarm policy.
- **OK**: The monitoring data is reported but does not meet the preset alarm policy.
- **Insufficient data**: No monitoring data has been reported for three consecutive hours, and this is generally because the instance has been deleted or is abnormal.

3.3 What Alarm Severities Does Cloud Eye Support?

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

- **Critical**: An emergency fault has occurred and services are affected.

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

3.4 When Will an "Insufficient data" Alarm Be Triggered?

When monitoring data of a metric is not reported to Cloud Eye for three consecutive hours, the alarm rule status changes to **Insufficient data**.

In special cases, if monitoring data of a metric is reported at an interval longer than three hours and no monitoring data is reported for three consecutive intervals, the alarm rule status also changes to **Insufficient data**.

3.5 How Do I Monitor and View the Disk Usage?

To monitor the disk usage, install the server monitoring Agent and create an alarm rule for the disk usage. In the alarm rule, set the metric to **(Agent) Disk Usage (Recommended)** and select a mount point. Enable and configure **Alarm Notification**. For details, see **Creating an Alarm Rule to Monitor a Server**.

After you install the Agent, you can view the data disk usage on the Cloud Eye console. On the **OS Monitoring** page, click the **Disk** tab and select a mount point on the right of the **Auto Refresh** button.

3.6 How Can I Change the Phone Number and Email Address for Receiving Alarm Notifications?

Alarm notifications can be sent to the account contact or SMN topic subscribers configured in alarm rules.

You can change phone numbers and email addresses of the account contact or SMN topic subscribers.

Account Contact

If you set **Notification Object** to **Account contact**, alarm notifications will be sent to the mobile number and email address registered for your account.

You can update them on the **My Account** page by performing the following steps:

1. Log in to the management console.
2. Hover your mouse over the username in the upper right corner and select **Basic Information**.

   The **My Account** page is displayed.
3. Click **Edit** next to the phone number or email address.

4. Change the mobile number or email address as prompted.

SMN Topic Subscribers

If you set **Notification Object** to an SMN topic, perform the following steps to change the mobile numbers:

1. Log in to the management console.
2. In the service list, select **Simple Message Notification**.
3. In the navigation pane on the left, choose **Topic Management** >**Topics**.
4. Click the name of the target topic.
5. Add subscription endpoints to or delete subscription endpoints from the topic.

3.7 How Can a User Account Receive Alarm Notifications?

To enable a user account to receive alarm notifications, subscribe the account email address or phone number to an SMN topic and select the topic when you create alarm rules. For details, see **Creating a Topic** and **Adding Subscriptions**.

3.8 Why Did I Receive a Bandwidth Overflow Notification While There Being No Bandwidth Overflow Record in the Monitoring Data?

You may have configured Cloud Eye to trigger alarm notifications immediately when the bandwidth overflow occurs. However, if the average value for the last 5 minutes falls under the preset threshold, no alarm will be recorded in the system.

4 Monitored Data Exceptions

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

Possible causes are as follows:

- The service is not interconnected with Cloud Eye. To check whether a service has been interconnected with Cloud Eye, see **Services Interconnected with Cloud Eye**.
- The service has been interconnected with Cloud Eye. However, the collection and monitoring frequency for each service varies. The data may have just not been collected yet.
- The ECS or BMS has been stopped for more than 1 hour.
- The EVS disk has not been attached to an ECS or BMS.
- No backend server is bound to the elastic load balancer or all of the backend servers are shut down.
- It has been less than 10 minutes since the resource was purchased.

4.2 Why I Cannot See the Monitoring Data on the Cloud Eye Console After Purchasing Cloud Service Resources?

We are working to interconnect Cloud Eye with more cloud services. Before the interconnection is completed, you cannot view the resource monitoring data of the cloud services that have not been interconnected with Cloud Eye. Therefore, if you want to check the resource monitoring data of the cloud services you purchased, you need to first check whether the cloud services have been interconnected with Cloud Eye.

If the services have been interconnected with Cloud Eye, wait for a period of time, because the frequencies of each service to collect and report data to Cloud Eye are different. You can view the resource monitoring graph after Cloud Eye collects the first piece of monitoring data.

4.3 Why Doesn't the Cloud Eye Console Display the OS Monitoring Data or Why Isn't the Data Displayed Immediately After the Agent Is Installed and Configured on an ECS?

After you install the Agent successfully, choose **Server Monitoring**, and wait for 2 minutes. It takes about 2 minutes before monitoring data is displayed on the Cloud Eye console.

If **Agent Status** is **Running**, and you have waited for 5 minutes, but there is still no OS monitoring data displayed, check whether the ECS or BMS time and the console client time are consistent.

When the Agent reports data, it takes the ECS or BMS local time. When the console delivers requests, it takes the browser time of the user client. If the two times are inconsistent, no OS monitoring data will be displayed on the Cloud Eye console.

4.4 Why Is Basic Monitoring Data Inconsistent with Data Monitored by the OS?

Symptoms

CPU Usage under **Basic Monitoring** is close to 100%, which is very different from the CPU usage monitored by the OS (50%).

Possible Causes

- If you set **idle** to **poll** in the guest operating system (guest OS), and the guest OS is idle and enters the **polling** state, it consumes compute resources and does not proactively release CPU resources. As a result, the CPU usage is abnormal.
- In a HANA ECS, **idle** is set to **mwait** in the guest OS. When the guest OS is idle and enters the **mwait** state, the guest OS consumes less resources than that when **idle** is set to **poll**. However, the guest OS does not proactively release CPU resources, either. As a result, the CPU usage is abnormal.

Solution

Install and configure the Agent to view OS monitoring data.

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

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

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

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

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

4.6 Why Is the Metric Collection Point Lost During Certain Periods of Time?

There may be no monitoring data for that period, which can be perfectly normal. The Agent collects metrics based on the server OS time, and sometimes time synchronization leads to server time changes, which can result in the appearance of periods of time when no data was collected.

4.7 Why Are the Four Metrics Memory Usage, Disk Usage, Inband Incoming Rate, and Inband Outgoing Rate Not Displayed for an ECS?

Linux ECSs do not support the four metrics. Your ECS may run a Linux OS.

To learn more about basic metrics supported by different OSs, see **Basic ECS Metrics**.

To monitor memory and disk usages, see **Installing the Agent (Linux)**.

4.8 What Are the Impacts on ECS Metrics If UVP VMTools Is Not Installed on ECSs?

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

To learn more about ECS metrics supported by Cloud Eye, see **Basic ECS Metrics**.

5 User Permissions

5.1 What Should I Do If the IAM Account Permissions Are Abnormal?

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

NOTE

Cloud Eye provides a list of system policies, operations, and policy permissions. For details, see **Permissions Management**.

5.2 What Can I Do If the System Displays a Message Indicating Insufficient Permissions When I Access Cloud Eye?

Generally, this is because that the IAM user account does not have sufficient permissions. Check your permissions configured on IAM.

1. Use the Huawei Cloud account to log in to the Huawei Cloud management console.
2. On the management console, in the upper right corner, hover your mouse over the username, and choose **Identity and Access Management** from the drop-down list.
3. In the navigation pane on the left, choose **User Groups**.
4. Expand details about the user group the user belongs to.
5. Add the required permissions as described in **Creating a User Group and Assigning Permissions**.

   NOTE

   Cloud Eye provides a list of system policies, operations, and policy permissions. For details, see **Permissions Management**.

5.3 What Can I Do If the System Displays a Message Indicating Insufficient Permissions When I Click Configure on the Server Monitoring Page?

Symptoms

When you click **Configure** on the **Server Monitoring** page as an IAM user account, a message is displayed, indicating that you do not have the required permissions. In this case, the administrator needs to grant the agency query permissions for the user account.

Procedure

Step 1 Add a custom policy for querying the agencies.

1. Use the Huawei Cloud account to log in to the Huawei Cloud management console.
2. Ensure that the Huawei Cloud account has been granted the Agent permissions for the region. On the Cloud Eye console, choose **Server Monitoring** > **Elastic Cloud Server**. Check whether **Configure** is displayed above the ECS list.
   - If it is not, the Agent permission has been granted for the region.
   - If it is, click **Configure** to enable the Agent permissions for the region.
3. On the management console, hover your mouse over the username in the upper right corner, and choose **Identity and Access Management** from the drop-down list.
4. In the navigation pane on the left, choose **Permissions**. In the upper right corner of the displayed page, click **Create Custom Policy**.
5. Enter the following information to create a policy:
   - **Policy Name**: Specify a custom policy name.
   - **Scope**: Select **Global services**.
   - **Policy View**: Select **JSON**.
   - **Policy Content**: Copy the following code and paste it to the text box.

```
{
   "Version": "1.1",
   "Statement": [
      {
         "Action": [
            "iam:roles:listRoles",
            "iam:permissions:listRolesForAgencyOnProject",
            "iam:agencies:listAgencies",
            "iam:agencies:getAgency",
            "iam:agencies:createAgency",
            "iam:permissions:grantRoleToAgency",
            "iam:permissions:grantRoleToAgencyOnProject",
            "iam:permissions:revokeRoleFromAgencyOnProject",
            "iam:permissions:grantRoleToAgencyOnDomain",
            "iam:permissions:revokeRoleFromAgencyOnProject",
            "iam:permissions:revokeRoleFromAgency",
            "iam:permissions:revokeRoleFromAgencyOnDomain"
         ],
```

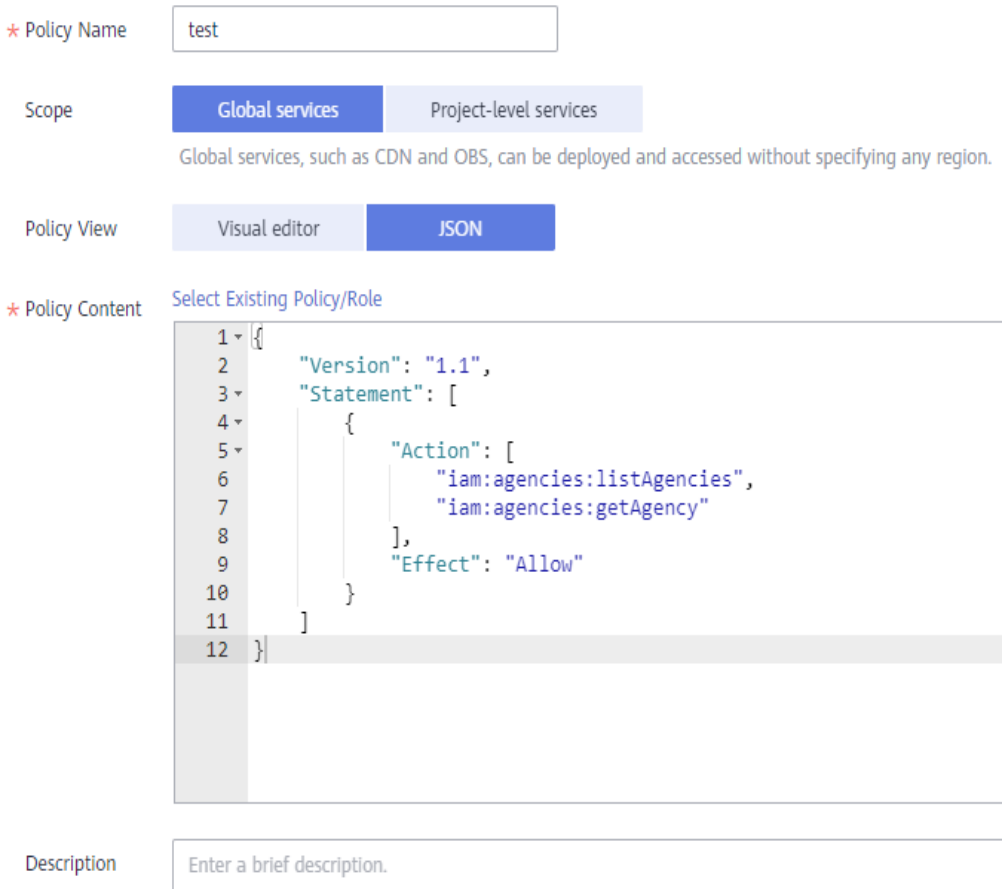


```
        "Effect": "Allow"
    }
  ]
}
```

- (Optional) **Description**: Provide supplementary information about the policy.

6. Confirm the policy content and click **OK** to save the policy.

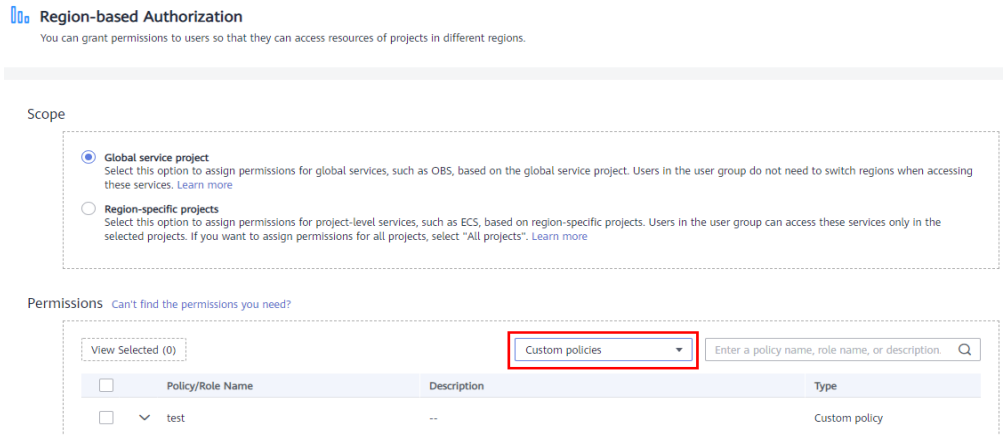
Figure 5-1 Create Custom Policy



Step 2 Assign permissions to the user account.

1. On the IAM console, in the navigation pane on the left, choose **User Groups**, locate the row containing the user group the user account belongs to, and choose **More** > **Manage Permissions** in the **Operation** column.
2. Click **Assign Permissions**. On the page displayed, search for the created custom policy, select it, and click **OK**.

Figure 5-2 Assign Permissions



----End

