

**Cloud Eye**

# FAQs

**Issue**                    05  
**Date**                      2023-09-15



**Copyright © Huawei Cloud Computing Technologies Co., Ltd. 2024. All rights reserved.**

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Cloud Computing Technologies Co., Ltd.

## **Trademarks and Permissions**



HUAWEI 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

<b>1 General Consulting</b>	<b>1</b>
1.1 What Is Rollup?	1
1.2 How Long Is Metric Data Retained?	2
1.3 How Many Rollup Methods Does Cloud Eye Support?	2
1.4 How Can I Export Collected Data?	3
1.5 What Should I Do If I See Garbled Chinese Characters in an Exported CSV File?	3
1.6 Why Can't a User of an Enterprise Project View the One-Click Monitoring Function?	4
1.7 Why Can't a User of an Enterprise Project Select All Resources When Configuring Alarm Rules?	4
<b>2 Server Monitoring</b>	<b>5</b>
2.1 Agent Installation	5
2.1.1 How Do I Configure DNS and Security Groups?	5
2.1.2 How Do I Configure an Agency?	8
2.1.3 How Does the Cloud Eye Agent Obtain a Temporary AK/SK by Authorization?	9
2.1.4 What OSs Does the Agent Support?	10
2.1.5 Resource Usage and Circuit Breaker Pattern of Agent	14
2.1.6 What Should I Do If the Monitoring Is Periodically Interrupted or the Agent Status Keeps Changing?	14
2.1.7 What Should I Do If a Service Port Is Used by the Agent?	16
2.1.8 Troubleshooting Agent One-Click Restoration Failures	17
2.1.9 No Monitoring Data Is Displayed After One-Click Restoration Performed for the Agent	19
2.1.10 Does the Server Monitoring Agent Affect Server Performance?	23
2.1.11 Troubleshooting the Problem of Reported Metrics Being Discarded	23
2.2 Metrics	24
2.2.1 Metrics Supported by the Agent	25
2.2.2 Environment Constraints for GPU Monitoring	65
2.2.3 BMS Hardware Metrics	66
2.3 Agent Statuses	69
2.3.1 How Can I Quickly Restore Agent Configurations?	69
2.3.2 What Should I Do If the Agent Status Is Faulty?	69
2.3.3 What Should I Do If the Agent Status Is Stopped?	70
2.3.4 What Should I Do If the Agent Status Is Running But There Is No Monitoring Data?	70
2.3.5 What Can I Do If No Monitoring Data Is Displayed After One-Click Agent Restoration? (Old Agent)	71

2.3.6 How Can I Enable the OS Monitoring for a New ECS?.....	75
2.3.7 Agent Status Description and Troubleshooting Methods.....	77
2.3.8 How Do I Obtain Debug Logs of the Agent?.....	78
<b>3 Alarm Notifications or False Alarms.....</b>	<b>80</b>
3.1 What Is an Alarm Notification? How Many Types of Alarm Notifications Are There? How Can I Configure an Alarm Notification?.....	80
3.2 What Alarm Status Does Cloud Eye Support?.....	81
3.3 What Alarm Severities Does Cloud Eye Support?.....	81
3.4 When Will an "Insufficient data" Alarm Be Triggered?.....	81
3.5 How Do I Monitor and View the Disk Usage?.....	81
3.6 How Can I Change the Phone Number and Email Address for Receiving Alarm Notifications?.....	82
3.7 How Can a User Account Receive Alarm Notifications?.....	83
3.8 Why Did I Receive a Bandwidth Overflow Notification While There Being No Bandwidth Overflow Record in the Monitoring Data?.....	83
<b>4 Monitored Data Exceptions.....</b>	<b>84</b>
4.1 Why Is the Monitoring Data Not Displayed on the Cloud Eye Console?.....	84
4.2 Why I Cannot See the Monitoring Data on the Cloud Eye Console After Purchasing Cloud Service Resources?.....	85
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?.....	85
4.4 Why Is Basic Monitoring Data Inconsistent with Data Monitored by the OS?.....	85
4.5 Why Are the Network Traffic Metric Values in Cloud Eye Different from Those Detected in ECS?.....	86
4.6 Why Is the Metric Collection Point Lost During Certain Periods of Time?.....	86
4.7 Why Are the Four Metrics Memory Usage, Disk Usage, Inband Incoming Rate, and Inband Outgoing Rate Not Displayed for an ECS?.....	86
4.8 What Are the Impacts on ECS Metrics If UVP VMTools Is Not Installed on ECSs?.....	87
4.9 Why Are the Inbound Bandwidth and Outbound Bandwidth Negative?.....	87
<b>5 Metric Descriptions.....</b>	<b>88</b>
5.1 What Are Outband Incoming Rate and Outband Outgoing Rate?.....	88
<b>6 User Permissions.....</b>	<b>90</b>
6.1 What Should I Do If the IAM Account Permissions Are Abnormal?.....	90
6.2 What Can I Do If the System Displays a Message Indicating Insufficient Permissions When I Access Cloud Eye?.....	91
6.3 What Can I Do If the System Displays a Message Indicating Insufficient Permissions When I Click Configure on the Server Monitoring Page?.....	91

# 1 General Consulting

---

[1.1 What Is Rollup?](#)

[1.2 How Long Is Metric Data Retained?](#)

[1.3 How Many Rollup Methods Does Cloud Eye Support?](#)

[1.4 How Can I Export Collected Data?](#)

[1.5 What Should I Do If I See Garbled Chinese Characters in an Exported CSV File?](#)

[1.6 Why Can't a User of an Enterprise Project View the One-Click Monitoring Function?](#)

[1.7 Why Can't a User of an Enterprise Project Select All Resources When Configuring Alarm Rules?](#)

## 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

### NOTE

For metric data in the AP-Bangkok region, the maximum retention period is one year, and the rollup period is 24 hours.

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:  
$$\text{Target time} = [\text{Unix timestamp}/1000 + (\text{Target time zone}) \times 3600]/86400 + 70 \times 365 + 19$$
  - c. Set cell format to **Date**.  
To convert a Unix timestamp of 1475918112000 to Shanghai time (UTC +8), using the formula from step b:  
$$\text{Target time} = [1475918112000/1000 + (+8) \times 3600]/86400 + 70 \times 365 + 19$$
  
Set the cell format to date and select a presentation format such as 2016/3/14 13:30.  
Then, the target time obtained will be presented as 2016/10/8 17:15.

## 1.5 What Should I Do If I See Garbled Chinese Characters in an Exported CSV File?

You can export the Cloud Eye monitoring data to a CSV file, but when you open this file with Excel, there may be garbled Chinese characters. This happens when

the exported CSV file is encoded in UTF-8, but the Excel is opened in ANSI format. To solve this problem, use either of the following solutions:

- Use a text editor such as Notepad or use WPS to open the CSV file you exported.
- Open the CSV file with Excel, but in the following manner:
  - a. Create an EXCEL file.
  - b. Choose **Data > From Text**.
  - c. Select the exported CSV file and click **Import**.  
The **Text Import Wizard** dialog box is displayed.
  - d. Select **Delimited** and click **Next**.
  - e. Deselect **Tab**, select **Comma**, and click **Next**.
  - f. Click **Finish**.
  - g. In the **Import Data** dialog box, click **OK**.

## 1.6 Why Can't a User of an Enterprise Project View the One-Click Monitoring Function?

The one-click monitoring function of Cloud Eye can be accessed and used only by the enterprise project account or the users with the Tenant Administrator permission.

For details about how to assign the Tenant Administrator permission to a user, see [Creating a User Group and Assigning Permissions](#).

## 1.7 Why Can't a User of an Enterprise Project Select All Resources When Configuring Alarm Rules?

When configuring alarm rules, only Huawei Cloud accounts or IAM users with the **Tenant Administrator** permissions can select all resources.

For details about how to assign the **Tenant Administrator** permissions to an IAM user, see .



# 2 Server Monitoring

---

[2.1 Agent Installation](#)

[2.2 Metrics](#)

[2.3 Agent Statuses](#)

## 2.1 Agent Installation

### 2.1.1 How Do I Configure DNS and Security Groups?

This topic describes how to add DNS server addresses and security groups to a Linux ECS to ensure successful Agent downloading and monitoring data collection. Here, ECSs are used as an example. The operations for other types of hosts are similar.

You can modify DNS configurations of an ECS in either of the following ways: command lines and management console. You can choose one as needed.

 **NOTE**

DNS and security group configurations are intended for the primary NIC.

#### DNS

- **Modifying a DNS Server Address (Command Lines)**

The following describes how to add a DNS server address to the **resolv.conf** file using command lines.

To use the management console, see [Modifying a DNS Server Address \(Management Console\)](#).

- a. Log in to an ECS as user **root**.
- b. Run the `vi /etc/resolv.conf` command to open the file `resolv.conf`.
- c. Add **nameserver 100.125.1.250** and **nameserver 100.125.21.250** to the file. Enter **:wq**, and press **Enter** to save the settings and exit.

**Figure 2-1** Adding a DNS server address (Linux)

```
# Generated by NetworkManager
search openstacklocal
nameserver 100.125.1.250
nameserver 100.125.21.250
options single-request-reopen
```

**NOTE**

The **nameserver** value varies depending on the region. For details, see [What Are Huawei Cloud Private DNS Server Addresses?](#)

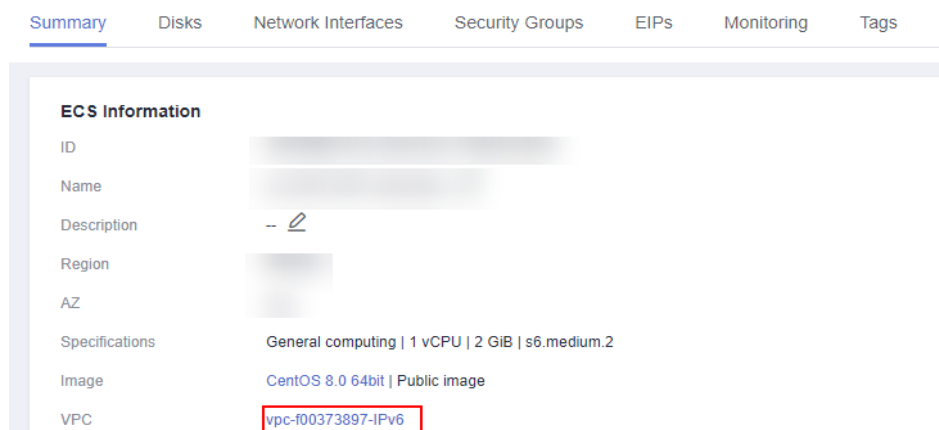
- **Modifying a DNS Server Address (Management Console)**


The following describes how to modify a DNS server address of an ECS on the management console. Here, ECSs are used as an example. The operations for BMSs are similar.

- Log in to the management console.
- In the upper left corner, select a region and project.
- Under **Service List**, choose **Computing > Elastic Cloud Server**.  
On the ECS console, click the name of the target ECS to view its details.
- In the **ECS Information** area of the **Summary** tab, click the VPC name as is shown in [Figure 2-2](#).

The **Virtual Private Cloud** page is displayed.

**Figure 2-2** VPC in ECS basic information

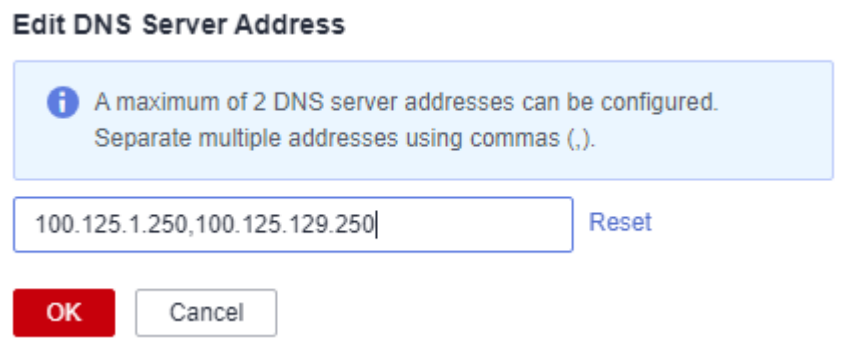


- Click the name of a target VPC.
- In the **Networking Components** area, click the number next to **Subnets**.  
The **Subnets** page is displayed.
- In the subnet list, click the name of a target subnet.
- In the **Gateway and DNS Information** area, click  after the **DNS Server Address**.

**NOTE**

Set the DNS server address to the value of **nameserver** in [3](#).

**Figure 2-3** Modifying a DNS server address



- i. Click **OK**.

 **NOTE**

The new DNS server address takes effect after the ECS or BMS is restarted.

## Security Groups

- **Modifying the ECS Security Group Rules (Management Console)**

The following describes how to modify security group rules for an ECS on the management console. ECSs are used as an example. The operations for BMSs are similar.

1. On the ECS details page, select the **Security Groups** tab.  
The security group list is displayed.
2. Click a security group name.
3. Click **Modify Security Group Rule**.

The security group details page is displayed.

 **NOTE**

Procedure for BMS:

1. Click the security group ID on the upper left corner of the list.
2. Click **Manage Rule** in the **Operation** column of the security group.
4. In the **Outbound Rules** tab, click **Add Rule**.
5. Add rules based on [Table 2-1](#).

**Table 2-1** Security group rules

Protocol	Port	Type	Destination IP Address	Description
TCP	80	IPv4	100.125.0.0/16	Used to download the Agent installation package from an OBS bucket to an ECS or BMS and obtain the ECS or BMS metadata and authentication information.

Protocol	Port	Type	Destination IP Address	Description
TCP and UDP	53	IPv4	100.125.0.0/16	Used by DNS to resolve domain names, for example, the OBS domain name for downloading the Agent installation package, and the Cloud Eye endpoint for sending monitoring data to Cloud Eye.
TCP	443	IPv4	100.125.0.0/16	Used to collect monitoring data to Cloud Eye.

## 2.1.2 How Do I Configure an Agency?

To enable you to monitor servers 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 **cesagency** 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:

- 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 do not have the required permissions, obtain the permissions by referring to [6.3 What Can I Do If the System Displays a Message Indicating Insufficient Permissions When I Click Configure on the Server Monitoring Page?](#)

- Authorization scope

Add the **CES AgentAccess** permissions to internal account **op\_svc\_ces** in the region.

- 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 query the ECS or BMS monitoring data on the Cloud Eye console or by calling the Cloud Eye APIs.

- a. Security: The AK/SK used by the Agent is only the temporary AK/SK that has the **CES AgentAccess** permissions. That is, the temporary AK/SK can only be used 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.

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

To enable you to monitor servers 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 **cesagency** 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 do not have the required permissions, obtain the permissions by referring to [6.3 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 query the ECS or BMS monitoring data on the Cloud Eye console or by calling the Cloud Eye APIs.

- 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 can only be used 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**.

## 2.1.4 What OSs Does the Agent Support?

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

### NOTICE

The following systems are created based using the public images provided by Image Management Service (IMS) from Huawei Cloud or public images. If an unverified external system is used, dependency problems may occur or other unstable factors may be introduced.

Operating System	Version	Agent Installation (ECS)	One-Click Agent Installation (ECS)	Agent Installation (BMS)
Windows	Windows 2012	√	×	√
	Windows 2016	√	×	√
	Windows 2019	√	×	√
CentOS	CentOS 6.9 64bit(40GB)	√	×	×
	CentOS 6.10 64bit	√	×	×
	CentOS 7.2 64bit	√	√	√
	CentOS 7.3 64bit	√	√	√
	CentOS 7.4 64bit	√	√	√
	CentOS 7.5 64bit	√	√	×
	CentOS 7.6 64bit	√	√	√
	CentOS 7.6 64bit(ARM)	×	×	√
	CentOS 7.7 64bit	√	√	×
	CentOS 7.8 64bit	√	√	×
	CentOS 7.9 64bit	√	√	√
	CentOS 8.0 64bit	√	√	×
	CentOS 8.1 64bit	√	√	×
	CentOS 8.2 64bit	√	√	×
	CentOS Stream 8/x86	√	×	×

Operating System	Version	Agent Installation (ECS)	One-Click Agent Installation (ECS)	Agent Installation (BMS)
	CentOS Stream 8/ARM	√	×	×
	CentOS Stream 9/x86	√	×	×
Alma Linux	AlmaLinux 8.7	√	×	×
	AlmaLinux 9.1	√	×	×
	AlmaLinux 9.0 64bit	√	√	×
Debian	Debian 9.0.0 64bit	√	×	×
	Debian 8.8.0 64bit	√	×	×
	Debian 8.2.0 64bit	√	×	×
	Debian 10.0.0 64bit	√	×	×
	Debian 10.2.0 64bit(ARM)	√	×	×
	Debian10.5	√	×	×
	Debian10.6	√	×	×
	Debian11.10	√	√	×
	debian 11.4	√	×	×
	debian 11.5	√	×	×
EulerOS	EulerOS 2.8 64bit	×	×	√
	EulerOS 2.5 64bit	√	√	×
	EulerOS 2.3 64bit	×	×	√
	EulerOS 2.2 64bit	√	×	×
	EulerOS 2.8 64bit(ARM)	√	×	√
	EulerOS 2.9 64bit	√	×	√
	EulerOS 2.9 64bit(ARM)	√	×	×
	EulerOS 2.10	√	×	√
Fedora	Fedora 30 64bit	√	×	×
	Fedora 31	√	×	×

Operating System	Version	Agent Installation (ECS)	One-Click Agent Installation (ECS)	Agent Installation (BMS)
	Fedora 36	√	×	×
Huawei Cloud EulerOS	Huawei Cloud EulerOS 1.0 64bit	√	×	×
	Huawei Cloud EulerOS 1.1 64bit	√	√	×
	Huawei Cloud EulerOS 2.0 64bit	√	√	√
	Huawei Cloud EulerOS 2.0 ARM 64bit(40GB)	√	√	√
KylinOS	Kylin Linux Advanced Server for Kunpeng V1	√	×	×
	Kylin-Server-10-SP2-20210524-x86.iso	√	×	×
	Kylin-Server-10-SP2-20210524-arm.iso	√	×	×
openEuler	openEuler 20.03 64bit	√	×	×
	openEuler 20.03 LTS SP3 64bit	√	×	×
	openEuler 22.03 LTS(ARM)	×	×	√
	openEuler 22.03 LTS 64bit	√	×	×
OpenSUSE	OpenSUSE 15.0 64bit	√	×	×
Redhat	Redhat Linux Enterprise 6.9 64bit	×	×	√
	Redhat Linux Enterprise 7.4 64bit	×	×	√
Rocky Linux	Rocky Linux 8.4 64bit	√	×	×



Operating System	Version	Agent Installation (ECS)	One-Click Agent Installation (ECS)	Agent Installation (BMS)
	Rocky Linux 8.5 64bit	√	×	×
	Rocky Linux 8.6 64 bit	√	×	×
	Rocky Linux 9.0 64bit	√	√	×
	Rocky Linux 9.1	√	×	×
	Rocky Linux 8.7-X86	√	×	×
	Rocky Linux 8.7-ARM	√	×	×
Ubuntu	Ubuntu 22.04 server 64bit	√	√	×
	Ubuntu 20.04 server 64bit	√	√	√
	Ubuntu 18.04 server 64bit	√	√	√
	Ubuntu 18.04 server 64bit(ARM)	×	×	√
	Ubuntu 16.04 server 64bit	√	√	√
	Ubuntu 14.04 server 64bit	×	×	√
	Ubuntu 18.04.6 server 64bit	√	×	×
UnionTechOS	UnionTech OS Server 20 Euler (1000) 64bit(ARM)	√	×	×
	UnionTech OS-Server-20-1050e-amd64-UFU.iso	√	×	×

## 2.1.5 Resource Usage and Circuit Breaker Pattern of Agent

### Resource Usage

The Agent uses very few system resources. The Agent will use 10% of a CPU core at most. Its memory usage will not exceed 200 MB. Generally, the CPU usage for a single core is less than 5% and the memory usage is less than 100 MB.

### Circuit Breaker Pattern

When the CPU usage of a single core is greater than 10%, or the memory usage exceeds 200 MB for three consecutive times, the Agent will implement the circuit breaker pattern, and host metrics collection will be stopped. The Agent will restart it later.

## 2.1.6 What Should I Do If the Monitoring Is Periodically Interrupted or the Agent Status Keeps Changing?

### Symptom

Monitoring interruptions and unstable Agent status may be caused by Agent overload. 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 changes between **Running** and **Faulty**.
- The period in the metric dashboard is discontinuous.

### Constraints

The restoration method in this section only supports new Agent version. If your Agent is of an earlier version, you are advised to upgrade it to the new version.

Run the following command to check the current Agent version:

```
if [[ -f /usr/local/uniagent/extension/install/telescope/bin/telescope ]]; then /usr/local/uniagent/extension/install/telescope/bin/telescope -v; elif [[ -f /usr/local/telescope/bin/telescope ]]; then echo "old agent"; else echo 0; fi
```

- If **old agent** is displayed, the Agent version is old.
- If a version ID is returned, the Agent version is new.
- If **0** is returned, the Agent has not been installed.

### Possible Causes

The circuit pattrer is implemented by the Agent when the CPU and memory usage is too high to prevent other services from being affected. The circuit breaker pattern will be implemented automatically when the Agent is overloaded, and no monitoring data will not be reported.

### Circuit Breaker Principles

By default, the Agent detection mechanism is as follows:

The Agent resource usage will be checked every one minute. If the resource usage exceeds the tier-2 thresholds (30% of CPU usage and 700 MB memory usage), the Agent exists. If the tier-1 thresholds (10% CPU usage and 200 MB memory usage) for three consecutive times, the Agent also exists and a record will be generated.

After the Agent exits, the daemon process automatically starts the Agent process and checks the exit records. 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 the circuit-breaker pattern 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. **Optional:** Go to the Agent installation path:  
 For Windows, the path is **C:\Program Files\uniagent\extension\install\telescope**.  
 For Linux, the path is **/usr/local/uniagent/extension/install/telescope/bin**.
3. Modify configuration file **conf.json**.
  - a. Run the following command to open **conf.json**:  
**vi conf.json**
  - b. Add the following parameters to the **conf.json** file. For details about the parameters, see [Table 2-2](#).

**Table 2-2** Parameters

Parameter	Description
cpu_first_pct_threshold	Tier-1 threshold of CPU usage. The default value is 10 (%).
memory_first_threshold	Tier-1 threshold of memory usage. The default value is 209715200 (200 MB). The unit is byte.
cpu_second_pct_threshold	Tier-2 threshold of CPU usage. The default value is 30 (%).
memory_second_threshold	Tier-2 threshold of memory usage. The default value is 734003200 (700 MB). The unit is byte.
<p><sup>a</sup> To query the CPU usage and memory usage of the Agent, use the following method:</p> <ul style="list-style-type: none"> <li>• Linux: <b>top -p telescope PID</b></li> <li>• Windows: View the details about the Agent process in <b>Task Manager</b>.</li> </ul>	

```
{
  "cpu_first_pct_threshold": xx,
  "memory_first_threshold": xxx,
  "cpu_second_pct_threshold": xx,
  "memory_second_threshold": xxx
}
```

- c. Run the following command to save and exit the **conf.json** file:  
**:wq**
4. Restart the Agent:
  - Windows:
    - In the directory where the Agent installation package is stored, double-click the **shutdown.bat** script to stop the Agent, and then execute the **start.bat** script to start the Agent.
  - Linux:
    - 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 2-4](#) shows an operation example.
    - **kill -9 PID**

**Figure 2-4** 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
```

## 2.1.7 What Should I Do If a 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.

### Constraints

The restoration method in this section only supports new Agent version. If your Agent is of an earlier version, you are advised to upgrade it to the new version.

Run the following command to check the current Agent version:

```
if [[ -f /usr/local/uniagent/extension/install/telescope/bin/telescope ]]; then /usr/local/uniagent/extension/install/telescope/bin/telescope -v; elif [[ -f /usr/local/telescope/bin/telescope ]]; then echo "old agent"; else echo 0; fi
```

- If **old agent** is displayed, the early version of the Agent is used.
- If a version is returned, the new version of the Agent is used.
- If **0** is returned, the Agent is not installed.

## Procedure

1. Log in to the primary node as a root user.
2. Run the following command to 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. Run the following command to make the change take effect:  
**sysctl -p /etc/sysctl.conf**

### NOTE

- The modification is permanent and still takes effect after the host is restarted.
  - To make a temporary modification (the password becomes invalid after the host is restarted), run the **# echo 49152 65536 > /proc/sys/net/ipv4/ip\_local\_port\_range** command.
5. Restart the Agent:
    - Windows:
      - In the directory where the Agent installation package is stored, double-click the **shutdown.bat** script to stop the Agent, and then execute the **start.bat** script to start the Agent.
    - Linux:
      - 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 2-5](#) shows an operation example.
      - **kill -9 PID**

Figure 2-5 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
```

## 2.1.8 Troubleshooting Agent One-Click Restoration Failures

### Symptom

After you click **Restore Agent Configurations**, the Agent status is still **Configuration error**.

### Constraints

The restoration method in this section only supports new Agent version. If your Agent is of an earlier version, you are advised to upgrade it to the new version.

Run the following command to check the current Agent version:

```
if [[ -f /usr/local/uniagent/extension/install/telescope/bin/telescope ]]; then /usr/local/uniagent/extension/install/telescope/bin/telescope -v; elif [[ -f /usr/local/telescope/bin/telescope ]]; then echo "old agent"; else echo 0; fi
```

- If **old agent** is displayed, the early version of the Agent is used.
- If a version is returned, the new version of the Agent is used.
- If **0** is returned, the Agent is not installed.

## Possible Causes

Troubleshooting methods:

1. Check DNS configurations
2. Check the IAM agency configurations.
3. Check user permissions

## Procedure

### Step 1 Check DNS configurations.

1. Log in to the management console.
2. Under **Compute**, select **Elastic Cloud Server**.
3. Click the name of the ECS.  
The ECS details page is displayed.
4. Click the VPC name.  
The VPC console is displayed.
5. In the VPC list, click the VPC name.
6. On the **Subnets** tab, check whether the DNS server addresses are correct.  
For details about how to configure the DNS servers for different regions, see [Modifying the DNS Server Address and Adding Security Group Rules \(Windows\)](#) or [Modifying the DNS Server Address and Adding Security Group Rules \(Linux\)](#).

Figure 2-6 DNS server address

Name	Status	AZ	CIDR Block	Gateway	DNS Server Address	DHCP	Network ACL	Operation
ops-subnet02	Available	AZ1	192.168.0.0/24	192.168.0.1	100.128.1.250, 100.128.21.250	Enabled	--	Modify Details

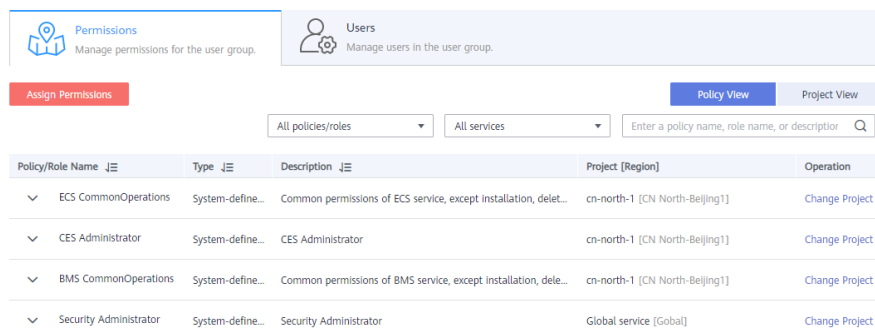
### Step 2 Check IAM agency quota

1. Log in to the management console.
2. In the service list, select **Identity and Access Management**.
3. On the IAM console, choose **Agencies**.
4. Check the agency quota.  
Check whether there is the agency: **CESAgentAutoConfigAgency**.  
If there is no such an agency and the quota has been used up, delete unnecessary agencies and then perform one-click Agent restoration.

**Step 3** Check user permissions.

1. Log in to the management console.
2. In the service list, select **Identity and Access Management**.
3. In the navigation pane on the left, click **User Groups**.
4. Locate your user group and click **Assign Permissions** in the **Operation** column.
5. To install the Agent, you must have the following permissions:
  - Global: Security Administrator
  - Region: ECS CommonOperationsr, or BMS CommonOperations and CES Administrator, or CES FullAccess

**Figure 2-7** Permissions required for installing the Agent



-----End

## 2.1.9 No Monitoring Data Is Displayed After One-Click Restoration Performed for the Agent

### Symptom

The Agent is running normally after being restored, but no monitoring data is generated.

### Constraints

The restoration method in this section only supports new Agent version. If your Agent is of an earlier version, you are advised to upgrade it to the new version.

Run the following command to check the current Agent version:

```
if [[ -f /usr/local/uniagent/extension/install/telescope/bin/telescope ]]; then /usr/local/uniagent/extension/install/telescope/bin/telescope -v; elif [[ -f /usr/local/telescope/bin/telescope ]]; then echo "old agent"; else echo 0; fi
```

- If **old agent** is displayed, the early version of the Agent is used.
- If a version is returned, the new version of the Agent is used.
- If **0** is returned, the Agent is not installed.

## Possible Causes

If no OS monitoring data is available for an ECS or BMS with the Agent installed, the possible causes are as follows:

- There is a problem with the Agent process.
- There is a problem with agency configurations.
- The network is not well connected.

## Procedure (Linux)

1. Log in to the ECS or BMS as the user **root**.
2. Run the following command to check whether the **telescope** process is running:

```
ps -ef |grep telescope
```

If following information is displayed, the telescope process is normal.

**Figure 2-8** Viewing the telescope process

```
[root@centos7 ~]#  
[root@centos7 ~]# ps -ef |grep telescope  
root      3245      1  0 Aug17 ?        00:00:54 ./telescope  
root      22879    1560  0 09:10 pts/0    00:00:00 grep --color=auto telescope  
[root@centos7 ~]#  
[root@centos7 ~]#
```

- If the telescope process is normal, go to [4](#).
  - If the telescope process is abnormal, go to [3](#).
3. Run the following command to start the Agent:  
**service uniagent restart**
  4. Run the following command to check whether the required agency has been created:  
**curl -ivk https://agent.ces.myhuaweicloud.com/v1.0/agencies/cesagency/securitykey**
    - If data is returned, the agency is normal and AK/SK can be obtained. No further action is required.
    - If the request fails or the following information is displayed, go to [5](#).

**Figure 2-9** Failing to obtain the AK/SK

```
<html>  
<head>  
<title>401 Unauthorized</title>  
</head>  
<body>  
<h1>401 Unauthorized</h1>  
agency_name is empty in metadata<br /><br />  
</body>
```

5. On the IAM console, in the left navigation pane, choose **Agencies**, and search for **cesagency**. Expand the **cesagency** details, check whether the current



region is included in **Project [Region]**. If no, in the **Operation** column, click **More**, and choose **Manage Permissions**. Click **Assign Permissions**, search for **CES Administrator**, click the drop-down list box, and select the current region.

Figure 2-10 Searching for cesagency

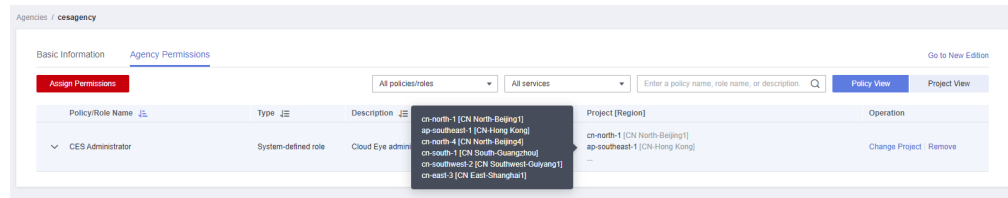
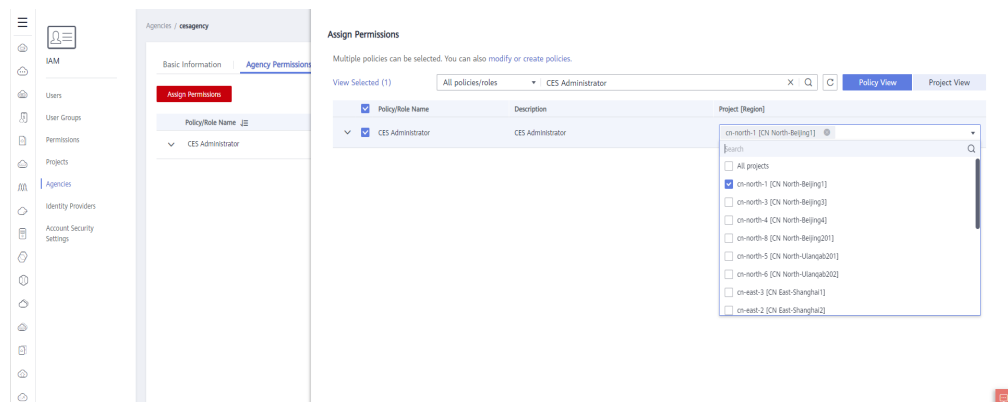


Figure 2-11 Assign permissions



- If the problem is resolved, no further action is required.
  - Otherwise, go to 6.
6. Run the following command to check whether the DNS service is normal:
- ping agent.ces.myhuaweicloud.com**
- If the network is normal, no further action is required.
  - Otherwise, modify the **DNS server address** or the Cloud Eye endpoint.

**NOTE**

For details about Cloud Eye endpoints for each region, see [Regions and Endpoints](#).

**Procedure (Windows)**

1. Log in to the ECS or BMS as an administrator.
2. Open the **Task Manager** and check whether the telescope process is running. If there are [Figure 2-12](#) and [Figure 2-13](#), the telescope process is running.

Figure 2-12 Agent process (Windows)

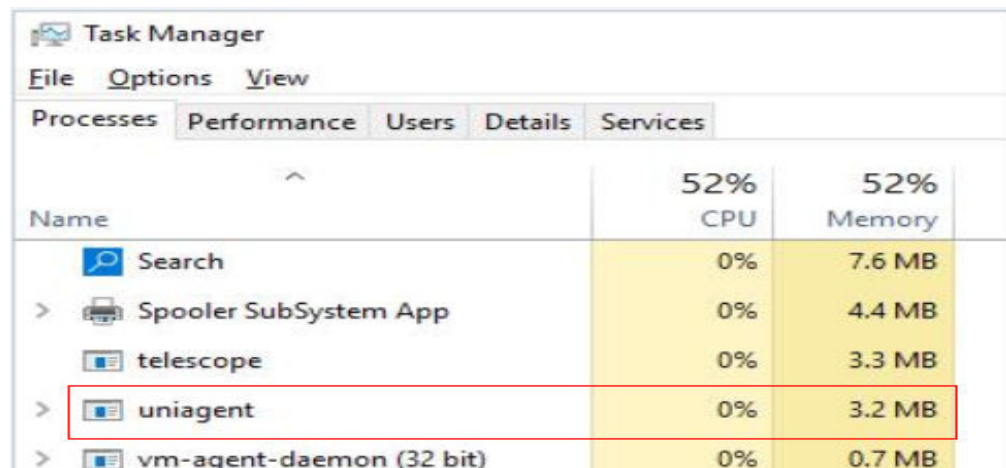
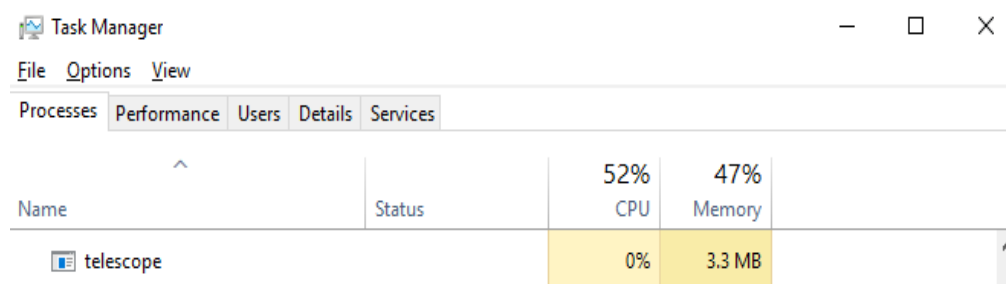


Figure 2-13 Telescope process (Windows)

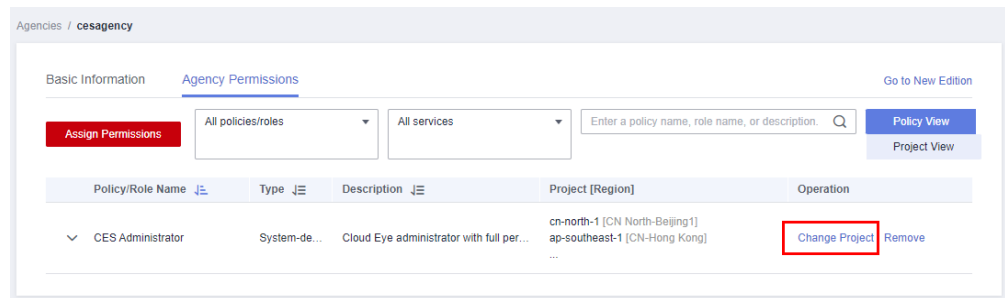


- If the process is normal, go to 4.
  - If the process is abnormal, go to 3.
3. Double-click **start.bat** in **C:\Program Files\uniagent\script** to start the Agent.
  4. On the IAM console, in the left navigation pane, choose **Agencies**, and search for **cesagency**. Expand the **cesagency** details, check whether the current region is in **Project [Region]**. If no, in the **Operation** column, click **More**, and choose **Manage Permissions**. Click **Assign Permissions**, search for **CES Administrator**, click the drop-down list box, and select the current region.

Figure 2-14 Searching for the cesagency agency



Figure 2-15 Assign permissions



- If the problem is resolved, no further action is required.
  - Otherwise, go to 6.
5. Run the following command to check whether the DNS service is normal:
- ping agent.ces.myhuaweicloud.com**
- If the network is normal, no further action is required.
  - Otherwise, modify the **DNS server address** or the Cloud Eye endpoint.

**NOTE**

For details about Cloud Eye endpoints for each region, see [Regions and Endpoints](#).

## 2.1.10 Does the Server Monitoring Agent Affect Server Performance?

The Agent uses a small portion of system resources and basically it will not affect server performance.

- Agent resource usage for an ECS is as follows:  
No more than 10% of a CPU core and no more than 200 M memory  
Generally, CPU usage (one core) is less than 5%, and the memory usage is less than 100 MB.
- Agent resource usage for a BMS is as follows:  
No more than 10% of a CPU core and no more than 200 M memory  
Generally, CPU usage (one core) is less than 5%, and the memory usage is less than 100 MB.

## 2.1.11 Troubleshooting the Problem of Reported Metrics Being Discarded

### Symptom

The plug-in status is normal, but the monitoring data for some metric is not continuous.

### Analysis

Possible causes are as follows:

- When there is a large gap between the Linux time and the actual time, the metrics collected by the Agent are considered invalid when being reported to the server. As a result, the reported metrics are discarded.

### Procedure (Linux)

Log in to the host as a root user, ensure that the ntp service is normal, and the run the following command:

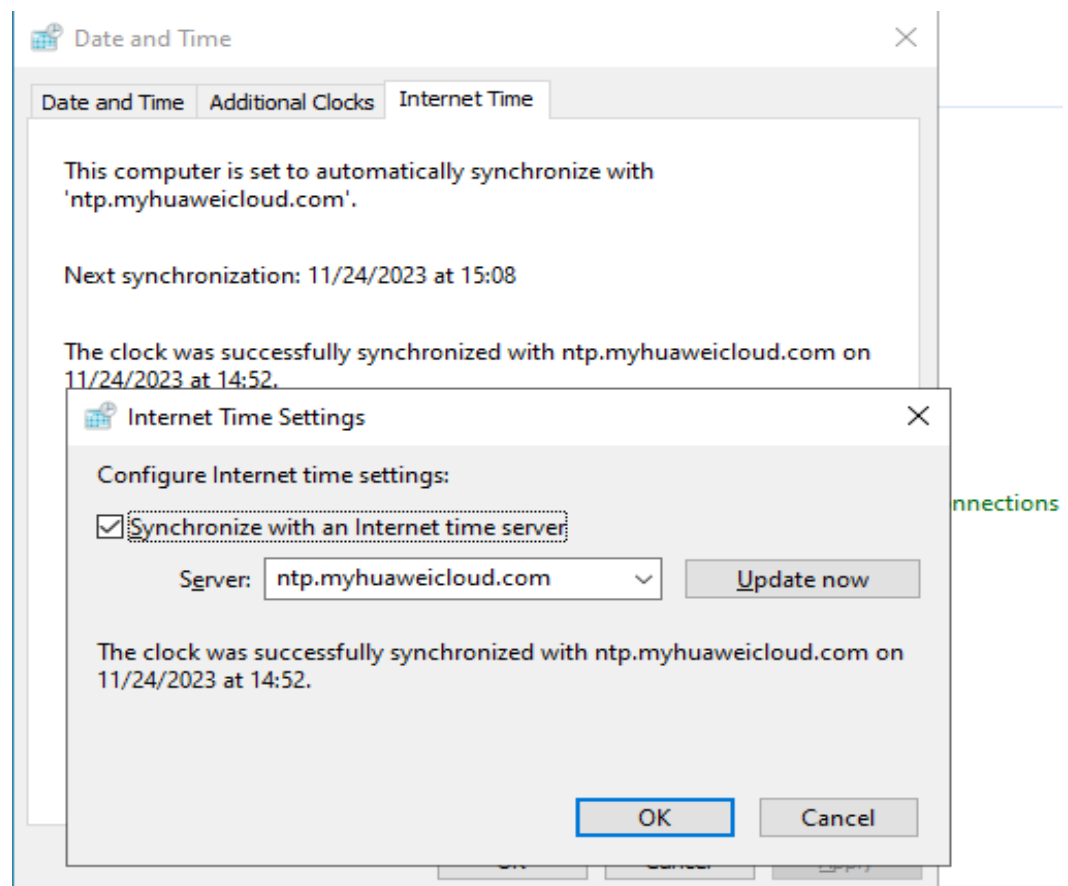
```
ntpdate -u ntp.myhuaweicloud.com
```

Or use another ntp address.

### Procedure (Windows)

Log in to the host as an administrator and ensure that the NTP service is normal. Choose **Control Panel > Date and Time > Internet Time > Change Settings**.

Enter the ntp address, for example, ntp.myhuaweicloud.com.



## 2.2 Metrics

## 2.2.1 Metrics Supported by the Agent

### OS metric: CPU

Metric	Name	Description	Unit	Supported Version	Monitoring Period (Raw Data)
cpu_usage	(Agent) CPU Usage	<p>Used to monitor CPU usage</p> <ul style="list-style-type: none"> <li>Collection method (Linux): Check the metric value changes in file <b>/proc/stat</b> in a collection period. You can run the <b>top</b> command to check the <b>%Cpu(s)</b> value.</li> <li>Collection method (Windows): Obtain the metric value using the API <b>GetSystemTimes</b>.</li> </ul>	%	2.4.1	1 minute
cpu_usage_idle	(Agent) Idle CPU Usage	<p>Percentage of the time that CPU is idle</p> <p>Unit: Percent</p> <ul style="list-style-type: none"> <li>Collection method (Linux): Check the metric value changes in file <b>/proc/stat</b> in a collection period.</li> <li>Collection method (Windows): Obtain the metric value using the API <b>GetSystemTimes</b>.</li> </ul>	%	2.4.5	1 minute

Metric	Name	Description	Unit	Supported Version	Monitoring Period (Raw Data)
cpu_usage_other	(Agent) Other Process CPU Usage	Other CPU usage of the monitored object <ul style="list-style-type: none"> <li>Collection method (Linux): <b>Other Process CPU Usage = 1- Idle CPU Usage - Kernel Space CPU Usage - User Space CPU Usage</b></li> <li>Collection method (Windows): <b>Other Process CPU Usage = 1- Idle CPU Usage - Kernel Space CPU Usage - User Space CPU Usage</b></li> </ul>	%	2.4.5	1 minute
cpu_usage_system	(Agent) Kernel Space CPU Usage	Percentage of time that the CPU is used by kernel space <ul style="list-style-type: none"> <li>Collection method (Linux): Check the metric value changes in file <b>/proc/stat</b> in a collection period. You can run the <b>top</b> command to check the <b>%Cpu(s) sy</b> value.</li> <li>Collection method (Windows): Obtain the metric value using the API <b>GetSystemTimes</b>.</li> </ul>	%	2.4.5	1 minute

Metric	Name	Description	Unit	Supported Version	Monitoring Period (Raw Data)
cpu_usage_user	(Agent) User Space CPU Usage	<p>Percentage of time that the CPU is used by user space</p> <ul style="list-style-type: none"> <li>Collection method (Linux): Check the metric value changes in file <b>/proc/stat</b> in a collection period. You can run the <b>top</b> command to check the <b>%Cpu(s) us</b> value.</li> <li>Collection method (Windows): Obtain the metric value using the API <b>GetSystemTimes</b>.</li> </ul>	%	2.4.5	1 minute
cpu_usage_nice	(Agent) Nice Process CPU Usage	<p>Percentage of the time that the CPU is in user mode with low-priority processes which can easily be interrupted by higher-priority processes</p> <ul style="list-style-type: none"> <li>Collection method (Linux): Check the metric value changes in file <b>/proc/stat</b> in a collection period. You can run the <b>top</b> command to check the <b>%Cpu(s) ni</b> value.</li> <li>Windows does not support this metric.</li> </ul>	%	2.4.5	1 minute

Metric	Name	Description	Unit	Supported Version	Monitoring Period (Raw Data)
cpu_usage_iowait	(Agent) iowait Process CPU Usage	<p>Percentage of time that the CPU is waiting for I/O operations to complete</p> <ul style="list-style-type: none"> <li>Collection method (Linux): Check the metric value changes in file <b>/proc/stat</b> in a collection period. You can run the <b>top</b> command to check the <b>%Cpu(s) wa</b> value.</li> <li>Windows does not support this metric.</li> </ul>	%	2.4.5	1 minute
cpu_usage_irq	(Agent) CPU Interrupt Time	<p>Percentage of time that the CPU is servicing interrupts</p> <ul style="list-style-type: none"> <li>Collection method (Linux): Check the metric value changes in file <b>/proc/stat</b> in a collection period. You can run the <b>top</b> command to check the <b>%Cpu(s) hi</b> value.</li> <li>Windows does not support this metric.</li> </ul>	%	2.4.5	1 minute
cpu_usage_softirq	(Agent) CPU Software Interrupt Time	<p>Percentage of time that the CPU is servicing software interrupts</p> <ul style="list-style-type: none"> <li>Collection method (Linux): Check the metric value changes in file <b>/proc/stat</b> in a collection period. You can run the <b>top</b> command to check the <b>%Cpu(s) si</b> value.</li> <li>Windows does not support this metric.</li> </ul>	%	2.4.5	1 minute



## OS Metric: CPU Load

Metric	Name	Description	Unit	Supported Version	Monitoring Period (Raw Data)
load_average1	(Agent) 1-Minute Load Average	<p>CPU load averaged from the last 1 minute</p> <ul style="list-style-type: none"> <li>Collection method (Linux): Obtain the metric value from the number of logic CPUs in <b>load1/</b> in file <b>/proc/loadavg</b>. You can run the <b>top</b> command to check the <b>load1</b> value.</li> </ul>	None	2.4.1	1 minute
load_average5	(Agent) 5-Minute Load Average	<p>CPU load averaged from the last 5 minutes</p> <ul style="list-style-type: none"> <li>Collection method (Linux): Obtain the metric value from the number of logic CPUs in <b>load5/</b> in file <b>/proc/loadavg</b>. You can run the <b>top</b> command to check the <b>load5</b> value.</li> </ul>	None	2.4.1	1 minute
load_average15	(Agent) 15-Minute Load Average	<p>CPU load averaged from the last 15 minutes</p> <ul style="list-style-type: none"> <li>Collection method (Linux): Obtain the metric value from the number of logic CPUs in <b>load15/</b> in file <b>/proc/loadavg</b>. You can run the <b>top</b> command to check the <b>load15</b> value.</li> </ul>	None	2.4.1	1 minute

## OS Metric: Memory

Metric	Name	Description	Unit	Supported Version	Monitoring Period (Raw Data)
mem_available	(Agent) Available Memory	<p>Amount of memory that is available and can be given instantly to processes</p> <ul style="list-style-type: none"> <li>Collection method (Linux): Obtain the metric value from <b>/proc/meminfo</b>. If <b>MemAvailable</b> is displayed in <b>/proc/meminfo</b>, obtain the value. If <b>MemAvailable</b> is not displayed in <b>/proc/meminfo</b>, <b>MemAvailable = MemFree + Buffers + Cached</b></li> <li>Collection method (Windows): It is calculated by available memory minuses used memory. The value is obtained by calling the Windows API GlobalMemoryStatusEx.</li> </ul>	GB	2.4.5	1 minute

Metric	Name	Description	Unit	Supported Version	Monitoring Period (Raw Data)
mem_usedPercent	(Agent) Memory Usage	<p>Memory usage of the instance</p> <ul style="list-style-type: none"> <li>Collection method (Linux): Obtain the metric value from the <code>/proc/meminfo</code> file (<b>MemTotal-MemAvailable</b>)/<b>MemTotal</b>. If <b>MemAvailable</b> is displayed in <code>/proc/meminfo</code>, <b>MemUsedPercent</b> = <b>(MemTotal-MemAvailable)/MemTotal</b>. If <b>MemAvailable</b> is not displayed in <code>/proc/meminfo</code>, <b>MemUsedPercent</b> = <b>(MemTotal - MemFree - Buffers - Cached)/MemTotal</b>.</li> <li>Collection method (Windows): The calculation formula is as follows: Used memory size/Total memory size*100%.</li> </ul>	%	2.4.1	1 minute
mem_free	(Agent) Idle Memory	<p>Amount of memory that is not being used</p> <ul style="list-style-type: none"> <li>Linux: Obtain the metric value from <code>/proc/meminfo</code>.</li> <li>Windows does not support this metric.</li> </ul>	GB	2.4.5	1 minute

Metric	Name	Description	Unit	Supported Version	Monitoring Period (Raw Data)
mem_buffers	(Agent) Buffer	Amount of memory that is being used for buffers <ul style="list-style-type: none"> <li>Collection method (Linux): Obtain the metric value from <b>/proc/meminfo</b>. You can run the <b>top</b> command to check the <b>KiB Mem:buffers</b> value.</li> <li>Windows does not support this metric.</li> </ul>	GB	2.4.5	1 minute
mem_cached	(Agent) Cache	Amount of memory that is being used for file caches <ul style="list-style-type: none"> <li>Collection method (Linux): Obtain the metric value from <b>/proc/meminfo</b>. You can run the <b>top</b> command to check the <b>KiB Swap:cached Mem</b> value.</li> <li>Windows does not support this metric.</li> </ul>	GB	2.4.5	1 minute
total_open_files	(Agent) Total File Handles	Total handles used by all processes <ul style="list-style-type: none"> <li>Collection method (Linux): Use the <b>/proc/{pid}/fd</b> file to summarize the handles used by all processes.</li> <li>Windows does not support this metric.</li> </ul>	None	2.4.5	1 minute

## OS Metric: Disk

### NOTE

Currently, CES Agent can collect only physical disk metrics and does not support disks mounted using the network file system protocol.

By default, CES Agent will not monitor Docker-related mount points. The prefix of the mount point is as follows:

```
/var/lib/docker/mnt/paas/kubernetes;/var/lib/mesos
```

Metric	Name	Description	Unit	Supported Version	Monitoring Period (Raw Data)
disk_free	(Agent) Available Disk Space	<p>Free space on the disks</p> <ul style="list-style-type: none"> <li>Collection method (Linux): Run the <b>df -h</b> command to check the value in the <b>Avail</b> column. The path of the mount point prefix cannot exceed 64 characters. It must start with a letter, and contain only digits, letters, hyphens (-), periods (.), and swung dashes (~).</li> <li>Collection method (Windows): Use the Windows Management Instrumentation (WMI) API GetDiskFreeSpaceExW to obtain disk space data. The path of the mount point prefix cannot exceed 64 characters. It must start with a letter, and contain only digits, letters, hyphens (-), periods (.), and swung dashes (~).</li> </ul>	GB	2.4 .1	1 minute

Metric	Name	Description	Unit	Supported Version	Monitoring Period (Raw Data)
disk_total	(Agent) Disk Storage Capacity	<p>Total disk capacity</p> <ul style="list-style-type: none"> <li>Collection method (Linux): Run the <b>df -h</b> command to check the value in the <b>Size</b> column. The path of the mount point prefix cannot exceed 64 characters. It must start with a letter, and contain only digits, letters, hyphens (-), periods (.), and swung dashes (~).</li> <li>Collection method (Windows): Use the WMI API GetDiskFreeSpaceExW to obtain disk space data. The path of the mount point prefix cannot exceed 64 characters. It must start with a letter, and contain only digits, letters, hyphens (-), periods (.), and swung dashes (~).</li> </ul>	GB	2.4.5	1 minute

Metric	Name	Description	Unit	Supported Version	Monitoring Period (Raw Data)
disk_used	(Agent) Used Disk Space	<p>Disk's used space</p> <ul style="list-style-type: none"> <li>Collection method (Linux): Run the <b>df -h</b> command to check the value in the <b>Used</b> column. The path of the mount point prefix cannot exceed 64 characters. It must start with a letter, and contain only digits, letters, hyphens (-), periods (.), and swung dashes (~).</li> <li>Collection method (Windows): Use the WMI API GetDiskFreeSpaceExW to obtain disk space data. The path of the mount point prefix cannot exceed 64 characters. It must start with a letter, and contain only digits, letters, hyphens (-), periods (.), and swung dashes (~).</li> </ul>	GB	2.4.5	1 minute

Metric	Name	Description	Unit	Supported Version	Monitoring Period (Raw Data)
disk_used Percent	(Agent) Disk Usage	<p>Percentage of used disk space. It is calculated as follows: <b>Disk Usage = Used Disk Space/Disk Storage Capacity.</b></p> <ul style="list-style-type: none"> <li>Collection method (Linux): It is calculated as follows: Used/Size. The path of the mount point prefix cannot exceed 64 characters. It must start with a letter, and contain only digits, letters, hyphens (-), periods (.), and swung dashes (~).</li> <li>Collection method (Windows): Use the WMI API GetDiskFreeSpaceExW to obtain disk space data. The path of the mount point prefix cannot exceed 64 characters. It must start with a letter, and contain only digits, letters, hyphens (-), periods (.), and swung dashes (~).</li> </ul>	%	2.4 .1	1 minute



## OS Metric: Disk I/O

Metric	Name	Description	Unit	Supported Version	Monitoring Period (Raw Data)
disk_agt_read_bytes_rate	(Agent) Disks Read Rate	<p>Volume of data read from the instance per second</p> <ul style="list-style-type: none"> <li>Collection method (Linux): Calculate the data changes in the sixth column of the corresponding device in file <b>/proc/diskstats</b> in a collection period. The path of the mount point prefix cannot exceed 64 characters. It must start with a letter, and contain only digits, letters, hyphens (-), periods (.), and swung dashes (~).</li> <li>Collection method (Windows): Use Win32_PerfFormattedData_PerfDisk_LogicalDisk object in WMI to obtain disk I/O data. The path of the mount point prefix cannot exceed 64 characters. It must start with a letter, and contain only digits, letters, hyphens (-), periods (.), and swung dashes (~). When the CPU usage is high, monitoring data obtaining timeout may occur and monitoring data cannot be obtained.</li> </ul>	Byte/s	2.4.5	1 minute

Metric	Name	Description	Unit	Supported Version	Monitoring Period (Raw Data)
disk_agt_read_requests_rate	(Agent) Disks Read Requests	<p>Number of read requests sent to the monitored disk per second</p> <ul style="list-style-type: none"> <li>Collection method (Linux): The disk read requests are calculated by calculating the data changes in the fourth column of the corresponding device in file <b>/proc/diskstats</b> in a collection period. The path of the mount point prefix cannot exceed 64 characters. It must start with a letter, and contain only digits, letters, hyphens (-), periods (.), and swung dashes (~).</li> <li>Collection method (Windows): Use Win32_PerfFormattedData_PerfDisk_LogicalDisk object in WMI to obtain disk I/O data. The path of the mount point prefix cannot exceed 64 characters. It must start with a letter, and contain only digits, letters, hyphens (-), periods (.), and swung dashes (~). When the CPU usage is high, monitoring data obtaining timeout may occur and monitoring data cannot be obtained.</li> </ul>	Request/s	2.4.5	1 minute

Metric	Name	Description	Unit	Supported Version	Monitoring Period (Raw Data)
disk_agt_write_bytes_rate	(Agent) Disks Write Rate	<p>Volume of data written to the instance per second</p> <ul style="list-style-type: none"> <li>Collection method (Linux): The disk write rate is calculated by calculating the data changes in the tenth column of the corresponding device in file <b>/proc/diskstats</b> in a collection period. The path of the mount point prefix cannot exceed 64 characters. It must start with a letter, and contain only digits, letters, hyphens (-), periods (.), and swung dashes (~).</li> <li>Collection method (Windows): Use Win32_PerfFormattedData_PerfDisk_LogicalDisk object in WMI to obtain disk I/O data. The path of the mount point prefix cannot exceed 64 characters. It must start with a letter, and contain only digits, letters, hyphens (-), periods (.), and swung dashes (~). When the CPU usage is high, monitoring data obtaining timeout may occur and the monitoring data cannot be obtained.</li> </ul>	Byte/s	2.4.5	1 minute

Metric	Name	Description	Unit	Supported Version	Monitoring Period (Raw Data)
disk_agt_write_requests_rate	(Agent) Disks Write Requests	<p>Number of write requests sent to the monitored disk per second</p> <ul style="list-style-type: none"> <li>Collection method (Linux): The disk write requests are calculated by calculating the data changes in the eighth column of the corresponding device in file <b>/proc/diskstats</b> in a collection period. The path of the mount point prefix cannot exceed 64 characters. It must start with a letter, and contain only digits, letters, hyphens (-), periods (.), and swung dashes (~).</li> <li>Collection method (Windows): Use Win32_PerfFormattedData_PerfDisk_LogicalDisk object in WMI to obtain disk I/O data. The path of the mount point prefix cannot exceed 64 characters. It must start with a letter, and contain only digits, letters, hyphens (-), periods (.), and swung dashes (~). When the CPU usage is high, monitoring data obtaining timeout may occur and the monitoring data cannot be obtained.</li> </ul>	Request/s	2.4.5	1 minute

Metric	Name	Description	Unit	Supported Version	Monitoring Period (Raw Data)
disk_read Time	(Agent) Average Read Request Time	<p>The average time taken for disk read operations</p> <ul style="list-style-type: none"> <li>Collection method (Linux): The average read request time is calculated by calculating the data changes in the seventh column of the corresponding device in file <b>/proc/diskstats</b> in a collection period.</li> </ul> <p>The path of the mount point prefix cannot exceed 64 characters. It must start with a letter, and contain only digits, letters, hyphens (-), periods (.), and swung dashes (~).</p> <ul style="list-style-type: none"> <li>Windows does not support this metric.</li> </ul>	ms/Count	2.4.5	1 minute

Metric	Name	Description	Unit	Supported Version	Monitoring Period (Raw Data)
disk_write Time	(Agent) Average Write Request Time	<p>The average time taken for disk write operations</p> <ul style="list-style-type: none"> <li>Collection method (Linux): The average write request time is calculated by calculating the data changes in the eleventh column of the corresponding device in file <b>/proc/diskstats</b> in a collection period.</li> </ul> <p>The path of the mount point prefix cannot exceed 64 characters. It must start with a letter, and contain only digits, letters, hyphens (-), periods (.), and swung dashes (~).</p> <ul style="list-style-type: none"> <li>Windows does not support this metric.</li> </ul>	ms/Count	2.4 .5	1 minute

Metric	Name	Description	Unit	Supported Version	Monitoring Period (Raw Data)
disk_ioUtils	(Agent) Disk I/O Usage	<p>Percentage of the time that the disk has had I/O requests queued to the total disk operation time</p> <ul style="list-style-type: none"> <li>Collection method (Linux): The disk I/O usage is calculated by calculating the data changes in the thirteenth column of the corresponding device in file <b>/proc/diskstats</b> in a collection period.</li> </ul> <p>The path of the mount point prefix cannot exceed 64 characters. It must start with a letter, and contain only digits, letters, hyphens (-), periods (.), and swung dashes (~).</p> <ul style="list-style-type: none"> <li>Windows does not support this metric.</li> </ul>	%	2.4.1	1 minute

Metric	Name	Description	Unit	Supported Version	Monitoring Period (Raw Data)
disk_queue_length	(Agent) Disk Queue Length	<p>Average number of read or write requests queued up for completion for the monitored disk in the monitoring period</p> <ul style="list-style-type: none"> <li>Collection method (Linux): The average disk queue length is calculated by calculating the data changes in the fourteenth column of the corresponding device in file <b>/proc/diskstats</b> in a collection period.</li> </ul> <p>The path of the mount point prefix cannot exceed 64 characters. It must start with a letter, and contain only digits, letters, hyphens (-), periods (.), and swung dashes (~).</p> <ul style="list-style-type: none"> <li>Windows does not support this metric.</li> </ul>	Count	2.4.5	1 minute



Metric	Name	Description	Unit	Supported Version	Monitoring Period (Raw Data)
disk_write_bytes_per_operation	(Agent) Average Disk Write Size	<p>Average number of bytes in an I/O write for the monitored disk in the monitoring period</p> <ul style="list-style-type: none"> <li>Collection method (Linux): The average disk write size is calculated by calculating the data changes in the tenth column of the corresponding device to divide that of the eighth column in file <b>/proc/diskstats</b> in a collection period.</li> </ul> <p>The path of the mount point prefix cannot exceed 64 characters. It must start with a letter, and contain only digits, letters, hyphens (-), periods (.), and swung dashes (~).</p> <ul style="list-style-type: none"> <li>Windows does not support this metric.</li> </ul>	Byte/op	2.4.5	1 minute

Metric	Name	Description	Unit	Supported Version	Monitoring Period (Raw Data)
disk_read_bytes_per_operation	(Agent) Average Disk Read Size	<p>Average number of bytes in an I/O read for the monitored disk in the monitoring period</p> <ul style="list-style-type: none"> <li>Collection method (Linux): The average disk read size is calculated by using the data changes in the sixth column of the corresponding device to divide that of the fourth column in file <b>/proc/diskstats</b> in a collection period. <p>The path of the mount point prefix cannot exceed 64 characters. It must start with a letter, and contain only digits, letters, hyphens (-), periods (.), and swung dashes (~).</p> </li> <li>Windows does not support this metric.</li> </ul>	Byte/op	2.4.5	1 minute

Metric	Name	Description	Unit	Supported Version	Monitoring Period (Raw Data)
disk_io_svc_tm	(Agent) Disk I/O Service Time	<p>Average time in an I/O read or write for the monitored disk in the monitoring period</p> <ul style="list-style-type: none"> <li>Collection method (Linux): The average disk I/O service time is calculated by using the data changes in the thirteenth column of the corresponding device to divide the sum of data changes in the fourth and eighth columns in file <b>/proc/diskstats</b> in a collection period. <p>The path of the mount point prefix cannot exceed 64 characters. It must start with a letter, and contain only digits, letters, hyphens (-), periods (.), and swung dashes (~).</p> </li> <li>Windows does not support this metric.</li> </ul>	ms/op	2.4.5	1 minute
disk_device_used_percent	Block Device Usage	<p>Percentage of total disk space that is used. The calculation formula is as follows: Used storage space of all mounted disk partitions/Total disk storage space.</p> <ul style="list-style-type: none"> <li>Collection mode (Linux): Summarize the disk usage of each mount point, calculate the total disk size based on the disk sector size and number of sectors, and calculate the overall disk usage.</li> <li>Currently, Windows does not support this metric.</li> </ul>	%	2.5.6	1 minute

## OS Metric: File System

Metric	Name	Description	Unit	Supported Version	Monitoring Period (Raw Data)
disk_fs_rw state	(Agent) File System Read/Write Status	<p>Read and write status of the mounted file system of the monitored object Possible statuses are <b>0</b> (read and write) and <b>1</b> (read only).</p> <ul style="list-style-type: none"> <li>Collection method (Linux): Check file system information in the fourth column in file <b>/proc/mounts</b>.</li> <li>Windows does not support this metric.</li> </ul>	None	2.4.5	1 minute
disk_inodesTotal	(Agent) Disk inode Total	<p>Total number of index nodes on the disk</p> <ul style="list-style-type: none"> <li>Collection method (Linux): Run the <b>df -i</b> command to check the value in the <b>Inodes</b> column. The path of the mount point prefix cannot exceed 64 characters. It must start with a letter, and contain only digits, letters, hyphens (-), periods (.), and swung dashes (~).</li> <li>Windows does not support this metric.</li> </ul>	None	2.4.5	1 minute

Metric	Name	Description	Unit	Supported Version	Monitoring Period (Raw Data)
disk_inodesUsed	(Agent) Total inode Used	<p>Number of used index nodes on the disk</p> <ul style="list-style-type: none"> <li>Collection method (Linux): Run the <b>df -i</b> command to check the value in the <b>IUsed</b> column. The path of the mount point prefix cannot exceed 64 characters. It must start with a letter, and contain only digits, letters, hyphens (-), periods (.), and swung dashes (~).</li> <li>Windows does not support this metric.</li> </ul>	None	2.4.5	1 minute
disk_inodesUsedPercent	(Agent) Percentage of Total inode Used	<p>Number of used index nodes on the disk</p> <ul style="list-style-type: none"> <li>Collection method (Linux): Run the <b>df -i</b> command to check the value in the <b>IUse%</b> column. The path of the mount point prefix cannot exceed 64 characters. It must start with a letter, and contain only digits, letters, hyphens (-), periods (.), and swung dashes (~).</li> <li>Windows does not support this metric.</li> </ul>	%	2.4.1	1 minute

## OS Metric: TCP

Metric	Metric	Description	Unit	Supported Version	Monitoring Period (Raw Data)
net_tcp_total	(Agent) Total Number of TCP Connections	Total number of TCP connections <ul style="list-style-type: none"> <li>Collection method (Linux): Obtain TCP connections in all states from the <code>/proc/net/tcp</code> file, and then collect the number of connections in each state.</li> <li>Collection method (Windows): Obtain the metric value using WindowsAPI GetTcpTable2.</li> </ul>	None	2.4.1	1 minute
net_tcp_established	(Agent) Number of connections in the ESTABLISHED state	Number of TCP connections in the ESTABLISHED state <ul style="list-style-type: none"> <li>Collection method (Linux): Obtain TCP connections in all states from the <code>/proc/net/tcp</code> file, and then collect the number of connections in each state.</li> <li>Collection method (Windows): Obtain the metric value using the GetTcpTable2 API.</li> </ul>	None	2.4.1	1 minute

Metric	Metric	Description	Unit	Supported Version	Monitoring Period (Raw Data)
net_tcp_sys_sent	(Agent) Number of connections in the TCP SYS_SENT state.	Number of TCP connections that are being requested by the client <ul style="list-style-type: none"><li>Collection method (Linux): Obtain TCP connections in all states from the <b>/proc/net/tcp</b> file, and then collect the number of connections in each state.</li><li>Collection method (Windows): Obtain the metric value using WindowsAPI GetTcpTable2.</li></ul>	None	2.4.5	1 minute
net_tcp_sys_rcv	(Agent) Number of connections in the TCP SYS_RECV state.	Number of pending TCP connections received by the server <ul style="list-style-type: none"><li>Collection method (Linux): Obtain TCP connections in all states from the <b>/proc/net/tcp</b> file, and then collect the number of connections in each state.</li><li>Collection method (Windows): Obtain the metric value using WindowsAPI GetTcpTable2.</li></ul>	None	2.4.5	1 minute

Metric	Metric	Description	Unit	Supported Version	Monitoring Period (Raw Data)
net_tcp_fin_wait1	(Agent) Number of TCP connections in the FIN_WAIT1 state.	<p>Number of TCP connections waiting for ACK packets when the connections are being actively closed by the client</p> <ul style="list-style-type: none"> <li>Collection method (Linux): Obtain TCP connections in all states from the <b>/proc/net/tcp</b> file, and then collect the number of connections in each state.</li> <li>Collection method (Windows): Obtain the metric value using WindowsAPI GetTcpTable2.</li> </ul>	None	2.4.5	1 minute
net_tcp_fin_wait2	(Agent) Number of TCP connections in the FIN_WAIT2 state.	<p>Number of TCP connections in the FIN_WAIT2 state</p> <ul style="list-style-type: none"> <li>Collection method (Linux): Obtain TCP connections in all states from the <b>/proc/net/tcp</b> file, and then collect the number of connections in each state.</li> <li>Collection method (Windows): Obtain the metric value using API GetTcpTable2.</li> </ul>	None	2.4.5	1 minute



Metric	Metric	Description	Unit	Supported Version	Monitoring Period (Raw Data)
net_tcp_time_wait	(Agent) Number of TCP connections in the TIME_WAIT state.	Number of TCP connections in the TIME_WAIT state <ul style="list-style-type: none"> <li>Collection method (Linux): Obtain TCP connections in all states from the <code>/proc/net/tcp</code> file, and then collect the number of connections in each state.</li> <li>Collection method (Windows): Obtain the metric value using the API <code>GetTcpTable2</code>.</li> </ul>	None	2.4.5	1 minute
net_tcp_close	(Agent) Number of TCP connections in the CLOSE state.	Number of closed TCP connections <ul style="list-style-type: none"> <li>Collection method (Linux): Obtain TCP connections in all states from the <code>/proc/net/tcp</code> file, and then collect the number of connections in each state.</li> <li>Collection method (Windows): Obtain the metric value using the API <code>GetTcpTable2</code>.</li> </ul>	None	2.4.5	1 minute
net_tcp_close_wait	(Agent) Number of TCP connections in the CLOSE_WAIT state.	Number of TCP connections in the CLOSE_WAIT state <ul style="list-style-type: none"> <li>Collection method (Linux): Obtain TCP connections in all states from the <code>/proc/net/tcp</code> file, and then collect the number of connections in each state.</li> <li>Collection method (Windows): Obtain the metric value using the API <code>GetTcpTable2</code>.</li> </ul>	None	2.4.5	1 minute

Metric	Metric	Description	Unit	Supported Version	Monitoring Period (Raw Data)
net_tcp_last_ack	(Agent) Number of TCP connections in the LAST_ACK state.	<p>Number of TCP connections waiting for ACK packets when the connections are being passively closed by the client</p> <ul style="list-style-type: none"> <li>Collection method (Linux): Obtain TCP connections in all states from the <code>/proc/net/tcp</code> file, and then collect the number of connections in each state.</li> <li>Collection method (Windows): Obtain the metric value using the API <code>GetTcpTable2</code>.</li> </ul>	None	2.4.5	1 minute
net_tcp_listen	(Agent) Number of TCP connections in the LISTEN state.	<p>Number of TCP connections in the LISTEN state</p> <ul style="list-style-type: none"> <li>Collection method (Linux): Obtain TCP connections in all states from the <code>/proc/net/tcp</code> file, and then collect the number of connections in each state.</li> <li>Collection method (Windows): Obtain the metric value using the API <code>GetTcpTable2</code>.</li> </ul>	None	2.4.5	1 minute

Metric	Metric	Description	Unit	Supported Version	Monitoring Period (Raw Data)
net_tcp_closing	(Agent) Number of TCP connections in the CLOSING state.	<p>Number of TCP connections to be automatically closed by the server and the client at the same time</p> <ul style="list-style-type: none"> <li>Collection method (Linux): Obtain TCP connections in all states from the <b>/proc/net/tcp</b> file, and then collect the number of connections in each state.</li> <li>Collection method (Windows): Obtain the metric value using the API GetTcpTable2.</li> </ul>	None	2.4.5	1 minute
net_tcp_retrans	(Agent) TCP Retransmission Rate	<p>Percentage of packets that are resent</p> <ul style="list-style-type: none"> <li>Collection method (Linux): Obtain the metric value from the <b>/proc/net/snmp</b> file. The value is the ratio of the number of sent packets to the number of retransmitted packages in a collection period.</li> <li>Collection method (Windows): Obtain the metric value using the API GetTcpStatistics.</li> </ul>	%	2.4.5	1 minute

## OS Metric: NIC

Metric	Name	Description	Unit	Supported Version	Monitoring Period (Raw Data)
net_bitRecv	(Agent) Outbound Bandwidth	<p>Number of bits sent by this NIC per second</p> <ul style="list-style-type: none"> <li>Collection method (Linux): Check metric value changes in file / <b>proc/net/dev</b> in a collection period.</li> <li>Collection method (Windows): Use the MibIfRow object in WMI to obtain network metric data.</li> </ul>	bit/s	2.4.1	1 minute
net_bitSent	(Agent) Inbound Bandwidth	<p>Number of bits received by this NIC per second</p> <ul style="list-style-type: none"> <li>Collection method (Linux): Check metric value changes in file / <b>proc/net/dev</b> in a collection period.</li> <li>Windows: Use the MibIfRow object in WMI to obtain network metric data.</li> </ul>	bit/s	2.4.1	1 minute
net_packetRecv	(Agent) NIC Packet Receive Rate	<p>Number of packets received by this NIC per second</p> <ul style="list-style-type: none"> <li>Collection method (Linux): Check metric value changes in file / <b>proc/net/dev</b> in a collection period.</li> <li>Collection method (Windows): Use the MibIfRow object in WMI to obtain network metric data.</li> </ul>	Count/s	2.4.1	1 minute

Metric	Name	Description	Unit	Supported Version	Monitoring Period (Raw Data)
net_packetSent	(Agent) NIC Packet Send Rate	<p>Number of packets sent by this NIC per second</p> <ul style="list-style-type: none"> <li>Collection method (Linux): Check metric value changes in file / <b>proc/net/dev</b> in a collection period.</li> <li>Collection method (Windows): Use the MibIfRow object in WMI to obtain network metric data.</li> </ul>	Count/s	2.4.1	1 minute
net_errin	(Agent) Receive Error Rate	<p>Percentage of receive errors detected by this NIC per second</p> <ul style="list-style-type: none"> <li>Collection method (Linux): Check metric value changes in file / <b>proc/net/dev</b> in a collection period.</li> <li>Windows does not support this metric.</li> </ul>	%	2.4.5	1 minute
net_errout	(Agent) Transmit Error Rate	<p>Percentage of transmit errors detected by this NIC per second</p> <ul style="list-style-type: none"> <li>Collection method (Linux): Check metric value changes in file / <b>proc/net/dev</b> in a collection period.</li> <li>Windows does not support this metric.</li> </ul>	%	2.4.5	1 minute

Metric	Name	Description	Unit	Supported Version	Monitoring Period (Raw Data)
net_dropin	(Agent) Received Packet Drop Rate	<p>Percentage of packets received by this NIC which were dropped per second</p> <ul style="list-style-type: none"> <li>Collection method (Linux): Check metric value changes in file / <b>proc/net/dev</b> in a collection period.</li> <li>Windows does not support this metric.</li> </ul>	%	2.4.5	1 minute
net_dropout	(Agent) Transmitted Packet Drop Rate	<p>Percentage of packets transmitted by this NIC which were dropped per second</p> <ul style="list-style-type: none"> <li>Collection method (Linux): Check metric value changes in file / <b>proc/net/dev</b> in a collection period.</li> <li>Windows does not support this metric.</li> </ul>	%	2.4.5	1 minute

### Process Monitoring Metrics

Metric	Name	Description	Unit	Supported Version	Monitoring Period (Raw Data)
proc_pHashId_cpu	(Agent) CPU Usage	<p>CPU consumed by a process. <b>pHashId</b> (process name and process ID) is the value of <b>md5</b>.</p> <ul style="list-style-type: none"> <li>Collection method (Linux): Check the metric value changes in file <b>/proc/pid/stat</b>.</li> <li>Collection method (Windows): Call the Windows API <code>GetProcessTimes</code> to obtain the CPU usage of the process.</li> </ul>	%	2.4 .1	1 minute

Metric	Name	Description	Unit	Supported Version	Monitoring Period (Raw Data)
proc_pHashId_mem	(Agent) Memory Usage	<p>Memory consumed by a process. <b>pHashId</b> (process name and process ID) is the value of <b>md5</b>.</p> <ul style="list-style-type: none"> <li>Collection method (Linux): <math>RSS * PAGESIZE / MemTotal</math> Obtain the <b>RSS</b> value by checking the second column of file <b>/proc/pid/statm</b>. Obtain the <b>PAGESIZE</b> value by running the <b>getconf PAGESIZE</b> command. Obtain the <b>MemTotal</b> value by checking file <b>/proc/meminfo</b>.</li> <li>Collection method (Windows): Call the Windows API <code>procGlobalMemoryStatusEx</code> to obtain the total memory size. Call <code>GetProcessMemoryInfo</code> to obtain the used memory size. Use the used memory size to divide the total memory size to get the memory usage.</li> </ul>	%	2.4 .1	1 minute
proc_pHashId_file	(Agent) Number of opened files	<p>Number of files opened by a process. <b>pHashId</b> (process name and process ID) is the value of <b>md5</b>.</p> <ul style="list-style-type: none"> <li>Collection method (Linux): Run the <b>ls -l /proc/pid/fd</b> command to view the number of opened files.</li> <li>Windows does not support this metric.</li> </ul>	Count	2.4 .1	1 minute



Metric	Name	Description	Unit	Supported Version	Monitoring Period (Raw Data)
proc_running_count	(Agent) Number of running processes	<p>Number of processes that are running</p> <ul style="list-style-type: none"> <li>Collection method (Linux): You can obtain the state of each process by checking the <b>Status</b> value in the <b>/proc/pid/status</b> file, and then collect the total number of processes in each state.</li> <li>Windows does not support this metric.</li> </ul>	None	2.4.1	1 minute
proc_idle_count	(Agent) Idle Processes	<p>Number of processes that are idle</p> <ul style="list-style-type: none"> <li>Collection method (Linux): You can obtain the state of each process by checking the <b>Status</b> value in the <b>/proc/pid/status</b> file, and then collect the total number of processes in each state.</li> <li>Windows does not support this metric.</li> </ul>	None	2.4.1	1 minute
proc_zombie_count	(Agent) Zombie Processes	<p>Number of zombie processes</p> <ul style="list-style-type: none"> <li>Collection method (Linux): You can obtain the state of each process by checking the <b>Status</b> value in the <b>/proc/pid/status</b> file, and then collect the total number of processes in each state.</li> <li>Windows does not support this metric.</li> </ul>	None	2.4.1	1 minute

Metric	Name	Description	Unit	Supported Version	Monitoring Period (Raw Data)
proc_blocked_count	(Agent) Blocked Processes	<p>Number of processes that are blocked</p> <ul style="list-style-type: none"> <li>Collection method (Linux): You can obtain the state of each process by checking the <b>Status</b> value in the <b>/proc/pid/status</b> file, and then collect the total number of processes in each state.</li> <li>Windows does not support this metric.</li> </ul>	None	2.4.1	1 minute
proc_sleeping_count	(Agent) Sleeping Processes	<p>Number of processes that are sleeping</p> <ul style="list-style-type: none"> <li>Collection method (Linux): You can obtain the state of each process by checking the <b>Status</b> value in the <b>/proc/pid/status</b> file, and then collect the total number of processes in each state.</li> <li>Windows does not support this metric.</li> </ul>	None	2.4.1	1 minute

Metric	Name	Description	Unit	Supported Version	Monitoring Period (Raw Data)
proc_total_count	(Agent) Total Processes	<p>Total number of processes on the monitored object</p> <ul style="list-style-type: none"> <li>Collection method (Linux): You can obtain the state of each process by checking the <b>Status</b> value in the <b>/proc/pid/status</b> file, and then collect the total number of processes in each state.</li> <li>Collection method (Windows): Obtain the total number of processes by using the system process status support module <b>psapi.dll</b>.</li> </ul>	None	2.4.1	1 minute
proc_specified_count	(Agent) Specified Processes	<p>Number of specified processes</p> <ul style="list-style-type: none"> <li>Collection method (Linux): You can obtain the state of each process by checking the <b>Status</b> value in the <b>/proc/pid/status</b> file, and then collect the total number of processes in each state.</li> <li>Collection method (Windows): Obtain the total number of processes by using the system process status support module <b>psapi.dll</b>.</li> </ul>	Count	2.4.1	1 minute

## GPU Specifications

Metric	Name	Description	Unit	Supported Version	Collection Method
GPU Specifications	gpu_status	Specifies the GPU health status of the VM. This is a comprehensive metric. <b>0</b> indicates healthy, <b>1</b> indicates subhealthy, and <b>2</b> indicates faulty.	-	2.4.5	Collection method (Linux): Invoke the libnvidia-ml.so.1 library file of the GPU card. Collection method (Windows): Invoke the nvml.dll library file of the GPU card.
	gpu_performance_state	Performance status of the GPU P0-P15, P32 <b>P0</b> indicates the maximum performance status. <b>P15</b> indicates the minimum performance status. <b>P32</b> indicates the unknown status.	-	2.4.1	
	gpu_power_draw	Power of the GPU.	W	2.4.5	
	gpu_temperature	Temperature of the GPU.	°C	2.4.5	
	gpu_usage_gpu	GPU computing power usage	%	2.4.1	
	gpu_usage_mem	GPU memory usage	%	2.4.1	
	gpu_used_mem	GPU memory usage	MB	2.4.5	
	gpu_free_mem	Remaining GPU memory	MB	2.4.5	
	gpu_usage_encoder	GPU encoding capability usage	%	2.4.5	
	gpu_usage_decoder	GPU decoding capability usage	%	2.4.5	
	gpu_graphics_clocks	Video card (shader) clock frequency of the GPU	MHz	2.4.5	
	gpu_sm_clocks	Streaming processor clock frequency of the GPU	MHz	2.4.5	

gpu_mem_clock	Memory clock frequency of the GPU	MHz	2.4.5
gpu_video_clocks	Video (including codec) clock frequency of the GPU	MHz	2.4.5
gpu_tx_throughput_pci	Outbound bandwidth of the GPU	MB/byte/s	2.4.5
gpu_rx_throughput_pci	Inbound bandwidth of the GPU	MB/byte/s	2.4.5
gpu_volatile_correctable	Number of correctable ECC errors since the GPU is reset. The value is reset to 0 each time the GPU is reset.	N/A	2.4.5
gpu_volatile_uncorrectable	Number of uncorrectable ECC errors since the GPU is reset. The value is reset to 0 each time the GPU is reset.	N/A	2.4.5
gpu_aggregate_correctable	Number of correctable ECC errors on the GPU	N/A	2.4.5
gpu_aggregate_uncorrectable	Number of uncorrectable ECC Errors on the GPU	N/A	2.4.5
gpu_retired_page_single_bit	Number of retired page single bit errors, which indicates the number of single-bit pages blocked by the graphics card	N/A	2.4.5
gpu_retired_page_double_bit	Number of errors, indicating the number of double-bit pages isolated by the current card.	N/A	2.4.5

## 2.2.2 Environment Constraints for GPU Monitoring

1. Only Linux OSs are supported, and only some Linux public image versions support GPU monitoring. For details, see [2.1.4 What OSs Does the Agent Support?](#)

2. Supported flavors: G6v, G6, P2s, P2v, P2vs, G5, Pi2, Pi1, ECSs of P1 series, the BMSs of the P, Pi, G, and KP series.
3. The lspci tool has been installed on the ECS. If the lspci tool is not installed on the ECS, GPU metric data cannot be collected and events cannot be reported.

To install the lspci tool, perform the following steps:

- a. Log in to the ECS.
- b. Update the image source to obtain the installation dependencies.  
**wget http://mirrors.myhuaweicloud.com/repo/mirrors\_source.sh && bash mirrors\_source.sh**

For more information, see [How Can I Use an Automated Tool to Configure a HUAWEI CLOUD Image Source \(x86\\_64 and Arm\)?](#)

- c. Run the following command to install the lspci tool:
  - CentOS:  
**yum install pciutils**
  - Ubuntu:  
**apt install pciutils**
- d. Run the following command to view the installation result:  
**lspci -d 10de:**

**Figure 2-16** Example installation result

```
[root@ecs ~]# lspci -d 10de:
00:0d.0 VGA compatible controller: NVIDIA Corporation TU104GL [Tesla T4] (rev a1)
```

4. GPU metric collection depends on the following driver files. Check whether there are corresponding driver files in the environment.
  - a. Linux driver file
 

```
nvmlUbuntuNvidiaLibraryPath = "/usr/lib/x86_64-linux-gnu/libnvidia-ml.so.1"
nvmlCentosNvidiaLibraryPath = "/usr/lib64/libnvidia-ml.so.1"
nvmlCceNvidiaLibraryPath = "/opt/cloud/cce/nvidia/lib64/libnvidia-ml.so.1"
```
  - b. Windows driver file
 

```
DefaultNvmlDLLPath = "C:\\Program Files\\NVIDIA Corporation\\NVSMI\\nvml.dll"
WHQLNvmlDLLPath = "C:\\Windows\\System32\\nvml.dll"
```

### 2.2.3 BMS Hardware Metrics

The following table describes BMS hardware monitoring metrics and how the metrics are collected.

Metrics	Description	Collected by
Server information	Includes the server SN, product name, manufacturer.	Running the <b>dmidecode</b> command

Metrics	Description	Collected by
Solid state drive (SSD) and hard disk drive (HDD) basic information and Self-Monitoring Analysis and Reporting Technology (SMART) information	Includes basic information (such as the SN, model, capacity, protocol type, and firmware version) and indicators (such as the health status, temperature, number of bad blocks, number of errors, and number of failures) in the SMART log of the SSD and HDD.	Running the <b>smartctl -a</b> <i>&lt;Drive letter&gt;</i> command
Basic information about the Non-Volatile Memory Express (NVMe) SSD	Includes SN, model, capacity, and firmware version.	Running the <b>nvme list</b> command
Standard SMART information of the NVMe SSD	Includes indicators in the SMART log of the NVMe SSD (such as the health status, temperature, service life, number of errors, and number of failures).	Running the <b>nvme smart-log</b> <i>&lt;NVMe device name&gt;</i> command
Additional SMART information of the Huawei NVMe SSD	Includes more detailed indicators and counts (such as power consumption, capacitor status, the number of bad blocks, and numbers of different errors).	Running the <b>hioadm info -d</b> <i>&lt;NVMe device name&gt;</i> <b>-a</b> and <b>hioadm info -d</b> <i>&lt;NVMe device name&gt;</i> <b>-e</b> commands
Additional SMART information of Intel NVMe SSDs	Includes more detailed error counts.	Run the <b>nvme intel smart-log-add</b> <i>&lt;NVMe device name&gt;</i> command
Network interface status information	Includes the MAC address, link status, and lost & wrong packets at the receiving and sending ends.	Running the <b>ifconfig</b> <i>&lt;Network interface name&gt;</i> command
Network port device information	Includes the port type, link status, and network rate.	Running the <b>ethtool</b> <i>&lt;Network interface name&gt;</i> command
Network interface driver information	Includes the firmware version, driver version, and bus number.	Running the <b>ethtool -i</b> <i>&lt;Network interface name&gt;</i> command

Metrics	Description	Collected by
Optical module information	Includes the basic device information (such as the SN, manufacturer, production date, connection type, encoding mode, and bandwidth) and device status information (such as offset current, input power, output power, voltage, and temperature).	Running the <b>ethtool -m</b> <i>&lt;Network interface name&gt;</i> command
Number of Huawei Intelligent NIC (HiNIC) port errors	HiLink errors, Base encoding errors, and RS encoding errors	Running the <b>hnicadm hilink_port -i &lt;dev_id&gt; -p &lt;port_id&gt; -s</b> and <b>hnicadm hilink_count -i &lt;dev_id&gt; -p &lt;port_id&gt;</b> commands
HiNIC card working mode	Current working mode and configured working mode	Running the <b>hnicadm mode -i &lt;dev_id&gt;</b> command
HiNIC card core temperature	Temperature of the HiNIC card core	Running the <b>hnicadm temperature -i &lt;dev_id&gt;</b> command
HiNIC card event records	Includes HiNIC card heartbeat losses, PCIe exceptions, chip errors, and chip health status.	Running the <b>hnicadm event -i &lt;dev_id&gt;</b> command
PCIe errors of the HiNIC card	Different PCIe errors of the HiNIC card	Running the <b>hnicadm counter -i &lt;dev_id&gt; -t 4</b> command
Memory information	Includes the DIMM SN, manufacturer, Part Number (PN), bit width, capacity, and frequency.	Running the <b>dmidecode -t 17</b> command
CPU information	Includes the CPU ID, name, frequency, architecture, and model.	Running the <b>dmidecode -t 4</b> and <b>lscpu</b> commands
Memory error records	Memory CE/UCE error records, including the error type, fault code, error location information (chip, rank, bank, column, row), MCI ADDR register, MCI MISC register, MCG CAP register, MCG STATUS register, retry registers, and other registers.	Reading files such as <b>/dev/mem</b> , <b>/dev/cpu/&lt;core_id&gt;/msr</b> , and <b>/sys/firmware/acpi/tables/HEST</b> to collect memory error records and chip register information



## 2.3 Agent Statuses

### 2.3.1 How Can I Quickly Restore Agent Configurations?

After the Agent is installed, you can configure **AK/SK**, **RegionID**, and **ProjectId** in one-click mode. This saves manual configuration steps 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 completed, 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 do not have the required permission, obtain the permission by referring to [6.3 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**.

### 2.3.2 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**.

The possible causes are:

- 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`

- If the DNS server is not a Huawei Cloud DNS server, run the **dig agent.ces.myhuaweicloud.com** command to obtain the IP address resolved by the Huawei Cloud DNS server over the intranet and then add the corresponding **hosts** file. For details, see [What Are the Private DNS Server Addresses Provided by Huawei Cloud?](#)

## 2.3.3 What Should I Do If the Agent Status Is Stopped?

### Viewing the Agent Version

1. Log in to an ECS as user **root**.
2. Run the following command to check the Agent version:

```
if [[ -f /usr/local/uniagent/extension/install/telescope/bin/telescope ]];  
then /usr/local/uniagent/extension/install/telescope/bin/telescope -v; elif  
[[ -f /usr/local/telescope/bin/telescope ]]; then echo "old agent"; else  
echo 0; fi
```

  - If **old agent** is displayed, the early version of the Agent is used.
  - If a version ID is returned, the new version of the Agent is used.
  - If **0** is returned, the Agent is not installed.

### Checking Agent Status (New Version)

Run the following command to start the Agent:

```
/usr/local/uniagent/extension/install/telescope/telescoped start
```

If a fault is reported, the Agent has been uninstalled or related files have been deleted. In this case, reinstall the Agent.

### Checking Agent Status (for Earlier Versions)

Run the following command to start the Agent:

```
service telescoped start
```

If a fault is reported, the Agent has been uninstalled or related files have been deleted. In this case, reinstall the Agent.

## 2.3.4 What Should I Do If the Agent Status Is Running But There Is No Monitoring Data?

After the Agent is installed, wait for 10 minutes. If there is still no monitoring data, **InstanceID** in the **conf** file may be incorrectly configured.

- Correct the configuration by performing operations described in [\(Optional\) Manually Configuring the Agent \(Linux\)](#).

## 2.3.5 What Can I Do If No Monitoring Data Is Displayed After One-Click Agent Restoration? (Old Agent)

### Symptom

The Agent is running normally after being restored, but no monitoring data is generated.

### Possible Causes

If no OS monitoring data is available for an ECS or BMS with the Agent installed, the possible causes are as follows:

- There is a problem with the Agent process.
- There is a problem with agency configurations.
- Temporary AK/SK cannot be obtained due to incorrect route configurations.
- The network is not well connected.

Check the Agent version.

1. Log in to an ECS as user **root**.
2. Run the following command to check the Agent version:  

```
if [[ -f /usr/local/uniagent/extension/install/telescope/bin/telescope ]];  
then /usr/local/uniagent/extension/install/telescope/bin/telescope -v; elif  
[[ -f /usr/local/telescope/bin/telescope ]]; then echo "old agent"; else  
echo 0; fi
```

  - If **old agent** is displayed, the early version of the Agent is used.
  - If a version ID is returned, the new version of the Agent is used.
  - If **0** is returned, the Agent is not installed.

### Procedure (Linux)

1. Log in to the ECS or BMS as user **root**.
2. Run the following command to check whether the **telescope** process is running:

```
ps -ef |grep telescope
```

The following information indicates that the telescope process is normal.

**Figure 2-17** Viewing the telescope processes

```
[root@ ~]# ps -ef |grep telescope  
root      3635      1   0 Jun21 ?        00:00:06  ./telescope  
root      3826    3635   0 Jun21 ?        00:19:24  ./telescope  
root      22829  22805   0 15:17 tty1    00:00:00  grep --color=auto telescope  
[root@ ~]# _
```

- If the telescope process is normal, go to [4](#).
  - If the telescope process is abnormal, go to [3](#).
3. Run the following command to start the Agent:

**/usr/local/telescope/telescoped start**

4. Run the following command to check whether an agency has been created for the server:

**curl http://169.254.169.254/openstack/latest/securitykey**

- If data is returned, the agency is normal and AK/SK can be obtained. No further action is required.
- If the request fails or the following information is displayed, go to [5](#).

**Figure 2-18** Failing to obtain the AK/SK

```
<html>
<head>
  <title>401 Unauthorized</title>
</head>
<body>
  <h1>401 Unauthorized</h1>
  agency_name is empty in metadata<br /><br />
</body>
```

5. On the Cloud Eye console, choose **Server Monitoring > Elastic Cloud Server**, select the target ECS, and click **Restore Agent Configurations**.
  - If the problem is resolved, no further action is required.
  - Otherwise, go to [6](#).
6. Run the following command to check the route:

**route -n**

The following information indicates that the route is normal.

**Figure 2-19** Normal route configuration-Linux

Kernel IP routing table							
Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
0.0.0.0	192.168.0.1	0.0.0.0	UG	100	0	0	eth0
169.254.169.254	192.168.0.1	255.255.255.255	UGH	100	0	0	eth0
192.168.0.0	0.0.0.0	255.255.255.0	U	100	0	0	eth0

- If the route is normal, no further action is required.
  - Otherwise, go to [7](#).
7. If the route does not exist, run the following command to add a route:

**route add -host 169.254.169.254 gw 192.168.0.1**

**NOTE**

Replace *192.168.0.1* in the example command with the gateway of the server. Check whether monitoring data can be reported normally.

- If yes, no further action is required.
  - If no, go to [8](#).
8. Run the following command to open the telescope configuration file:

**cat /usr/local/telescope/bin/conf\_ces.json**

- Obtain the endpoint from the configuration file.

**Figure 2-20** Querying the telescope endpoint

```
[root@hss log]# cat /usr/local/telescope/bin/conf_ces.json
{
  "Endpoint": "https://ces.cn-south-1.myhuaweicloud.com"
}[root@hss log]#
```

- Run the following command to check whether the DNS service is normal:  
**ping ces.cn-south-1.myhuaweicloud.com**
  - If the network is normal, no further action is required.
  - Otherwise, modify the **DNS server address** or the Cloud Eye endpoint.

**NOTE**

For details about Cloud Eye endpoints for each region, see [Regions and Endpoints](#).

### Procedure (Windows)

- Log in to the ECS or BMS as an administrator.
- Open the **Task Manager** and check whether the telescope process is running. If there are [Figure 2-21](#) and [Figure 2-22](#), the telescope process is running.

**Figure 2-21** agent process (Windows)

Processes			
Performance			
Name		47% CPU	31% Memory
agent		0%	3.0 MB
> Antimalware Service Executable		0.6%	92.1 MB

**Figure 2-22** telescope process (Windows)

Task Manager			
Performance			
Name	Status	52% CPU	47% Memory
telescope		0%	3.3 MB

- If the telescope process is normal, go to [4](#).
  - If the telescope process is abnormal, go to [3](#).
- Double-click **start.bat** to start the Agent.
  - Access [http://169.254.169.254/openstack/latest/meta\\_data.json](http://169.254.169.254/openstack/latest/meta_data.json) and check whether the agency has been created.

- If the website is accessible, the agency is normal. No further action is required.
  - Otherwise, go to [6](#).
5. Run the following command to check the route:

**route print**

The following information indicates that the route is normal.

**Figure 2-23** Normal route configuration-Windows

```

IPv4
=====
          0.0.0.0          0.0.0.0          192.168.10.1          192.168.10.228          5
          127.0.0.0          255.0.0.0          127.0.0.1          127.0.0.1          331
          127.0.0.1          255.255.255.255          127.0.0.1          127.0.0.1          331
          127.255.255.255          255.255.255.255          127.0.0.1          127.0.0.1          331
          169.254.169.254          255.255.255.255          192.168.10.254          192.168.10.228          6
          192.168.10.0          255.255.255.0          192.168.10.228          192.168.10.228          261
          192.168.10.228          255.255.255.255          192.168.10.228          192.168.10.228          261
          192.168.10.255          255.255.255.255          192.168.10.228          192.168.10.228          261
          224.0.0.0          240.0.0.0          127.0.0.1          127.0.0.1          331
          224.0.0.0          240.0.0.0          192.168.10.228          192.168.10.228          261
          255.255.255.255          255.255.255.255          127.0.0.1          127.0.0.1          331
          255.255.255.255          255.255.255.255          192.168.10.228          192.168.10.228          261
=====
  
```

- If the route is normal, no further action is required.
  - Otherwise, go to [7](#).
6. If the route does not exist, run the following command to add a route:
- route add -host 169.254.169.254 gw 192.168.0.1**

**NOTE**

Replace *192.168.0.1* in the example command with the gateway of the server. Check whether monitoring data can be reported normally.

- If yes, no further action is required.
  - If no, go to [7](#).
7. Open the configuration file in **bin/conf\_ces.json** in the directory where the telescope installation package is stored.
8. Obtain the endpoint from the telescope configuration file.  
{"Endpoint": "https://ces.cn-north-4.myhuaweicloud.com"}
9. Run the following command to check whether the DNS service is normal:

**ping ces.cn-north-4.myhuaweicloud.com**

- If the network is normal, no further action is required.
- Otherwise, modify the **DNS server address** or the Cloud Eye endpoint.

**NOTE**

For details about Cloud Eye endpoints for each region, see [Regions and Endpoints](#).

## 2.3.6 How Can I Enable the OS Monitoring for a New ECS?

### 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 with this private image.

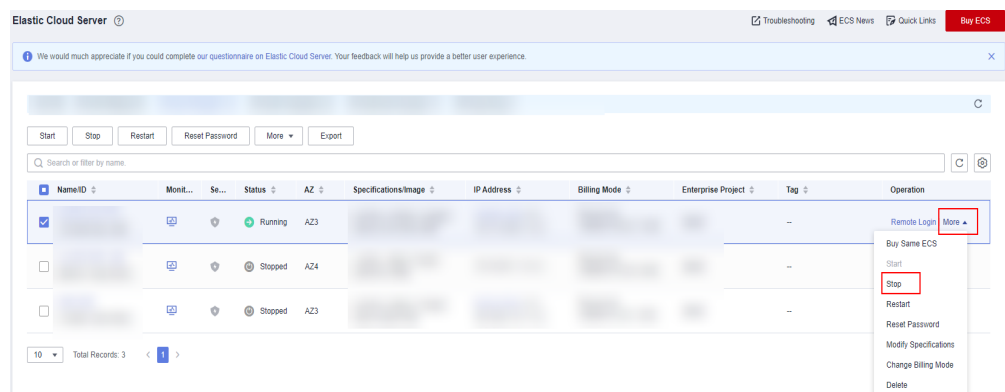
### Prerequisites

An ECS with the Agent installed is available.

### Procedure

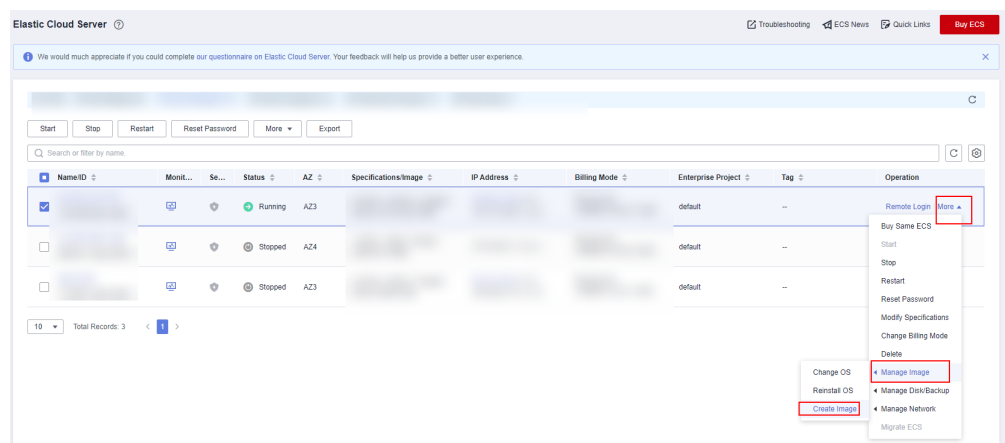
1. Log in to the ECS console. In the ECS list, locate a target ECS with the Agent installed, choose **More > Stop** in the **Operation** column, and click **OK**.

**Figure 2-24** Stopping an ECS



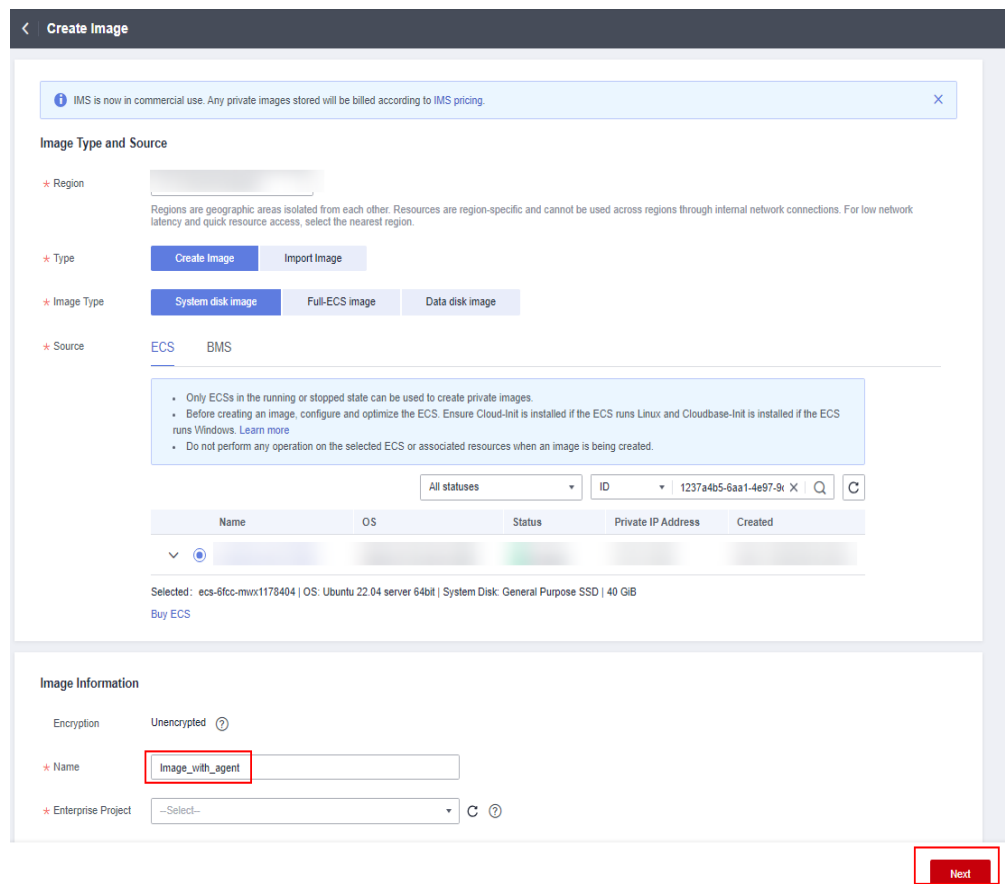
2. Choose **More > Manage Image/Disk > Create Image**.

**Figure 2-25** Create an image



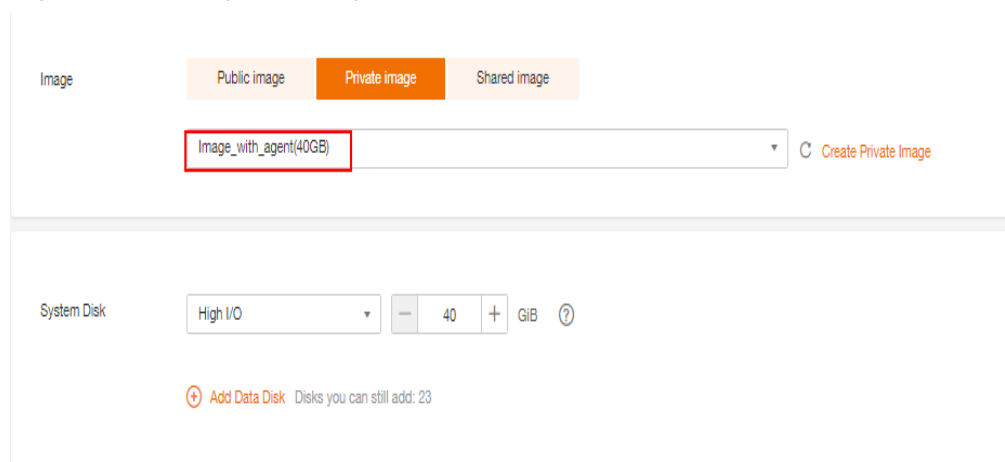
3. Set the private image name to **Image\_with\_agent** and click **Next**.

Figure 2-26 Image\_with\_agent



4. Purchase a new ECS and select the newly created private image **Image\_with\_agent (40GB)**.

Figure 2-27 Image\_with\_agent



5. Log in to the ECS. In the `/usr/local/telescope/bin/conf.json` file, set **Instanceid** to the ECS ID.



**Figure 2-28** Modifying the Agent configuration file

```
{
  "InstanceId": "3f94413d-0b77-4f7a-a0e0-8xxxx38dc2a6",
  "ProjectId": "68438a86d98xxxxxxxxxxxxx35d48",
  "AccessKey": "AXBxxxxxxxxxxxxL97VT4",
  "SecretKey": "Bwrzbxxxxxxxxxxxxxxxxxxxxu1M6ZZLbFnPg",
  "RegionId": "cn-north-1"
}
```

## 2.3.7 Agent Status Description and Troubleshooting Methods

The Agent can be in any of the following states:

- Running: The Agent is running properly with monitoring data properly reported.
- Not installed:
  - The Agent has not been installed. For details about how to install the Agent, see section of agent installation in the *Cloud Eye User Guide*.
  - If the Agent has been installed, but the agency has not been configured, configure the agency based on [2.1.2 How Do I Configure an Agency?](#)
  - If the Agent has been installed, but the network configurations are abnormal, fix the problem based on [Modifying the DNS Server Address and Adding Security Group Rules \(Linux\)](#) and [Modifying the DNS Server Address and Adding Security Group Rules \(Windows\)](#).
- Stopped:
  - The Agent is manually stopped. For details about how to start the Agent, see [Managing the Agent](#).
- Faulty: The Agent fails to send heartbeat messages to Cloud Eye for 3 minutes.
  - If the Agent domain name cannot be resolved, rectify the fault by referring to [Modifying the DNS Server Address and Adding Security Group Rules \(Linux\)](#) and [Modifying the DNS Server Address and Adding Security Group Rules \(Windows\)](#).
  - The account is in arrears.
  - If the Agent process is faulty, restart the Agent. For details about how to restart the Agent, see [Managing the Agent](#). If the status is still faulty after the restart, the Agent files may be damaged. In this case, reinstall the Agent. For details, see [Agent Installation and Configuration](#)
  - The server time is inconsistent with the local standard time.
  - If the DNS server is not a Huawei Cloud DNS server, run a command in the pattern: **dig** plus domain name, to obtain the resolved IP address of **agent.ces.myhuaweicloud.com**, which is resolved by the Huawei Cloud DNS server over the intranet. Then, add the IP address into the corresponding **hosts** file. For details about the private DNS addresses provided by Huawei Cloud, see [What Are Huawei Cloud Private DNS Server Addresses?](#)
  - Upgrade the Agent to the latest version.

## 2.3.8 How Do I Obtain Debug Logs of the Agent?

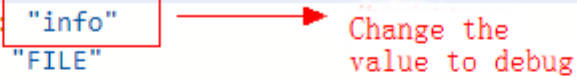
### Procedure

1. Locate and modify the Agent log configuration file. Change **info** to **debug** in the `<ces>` and `<ces_new>` sections. If there is only one of the `<ces>` or the `<ces_new>` sections, you only need to modify one section.
  - Linux: `/usr/local/uniagent/extension/install/telescope/bin/logs_config.xml`
  - Windows: `C:\Program Files\uniagent\extension\install\telescope\bin\logs_config.xml`

```
]]>
</common_new>
<ces>
  <![CDATA[
    <seelog minlevel="info">
      <outputs formatid="ces">
        <rollingfile type="size" filename="../log/ces.log" maxsize="20000000" maxrolls="5"/>
      </outputs>
      <formats>
        <format id="ces" format="%Date/%Time [%LEV] [%File:%Line] %Msg%r%n" />
      </formats>
    </seelog>
  ]]>
</ces>
<ces_new>
  <![CDATA[
    <seelog minlevel="info">
      <outputs formatid="ces_new">
        <rollingfile type="size" filename="../log/ces.log" maxsize="20000000" maxrolls="5"/>
      </outputs>
      <formats>
        <format id="ces_new" format="%Date/%Time [%LEV] [%File:%Line] %CleanMsg%r%n" />
      </formats>
    </seelog>
  ]]>
</ces_new>
</hardware>
```

2. If the configuration file in 1 is not found, modify the other configuration file.
  - Linux: `/usr/local/uniagent/extension/install/telescope/conf/logs.yaml`
  - Windows: `C:\Program Files\uniagent\extension\install\telescope\conf\logs.yaml`

```
ces:
- level: "info"
  type: "FILE"
  filename: "../log/ces.log"
  time_format: "2006-01-02 15:04:05 Z07:00"
  max_size: 20
  max_backups: 5
  max_age: 90
  enabled: true
  compress: true
hardware:
- level: "info"
  type: "FILE"
  filename: "../log/hardware.log"
  time_format: "2006-01-02 15:04:05 Z07:00"
  max_size: 5
  max_backups: 5
  max_age: 90
  enabled: true
  compress: true
```



3. Restart the Agent based on [Managing the Agent](#).
4. After obtaining the debug logs, restore the modified configurations and restart the Agent based on [Managing the Agent](#).

# 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?](#)

[3.2 What Alarm Status Does Cloud Eye Support?](#)

[3.3 What Alarm Severities Does Cloud Eye Support?](#)

[3.4 When Will an "Insufficient data" Alarm Be Triggered?](#)

[3.5 How Do I Monitor and View the Disk Usage?](#)

[3.6 How Can I Change the Phone Number and Email Address for Receiving Alarm Notifications?](#)

[3.7 How Can a User Account Receive Alarm Notifications?](#)

[3.8 Why Did I Receive a Bandwidth Overflow Notification While There Being No Bandwidth Overflow Record in the Monitoring Data?](#)

## 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, 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?

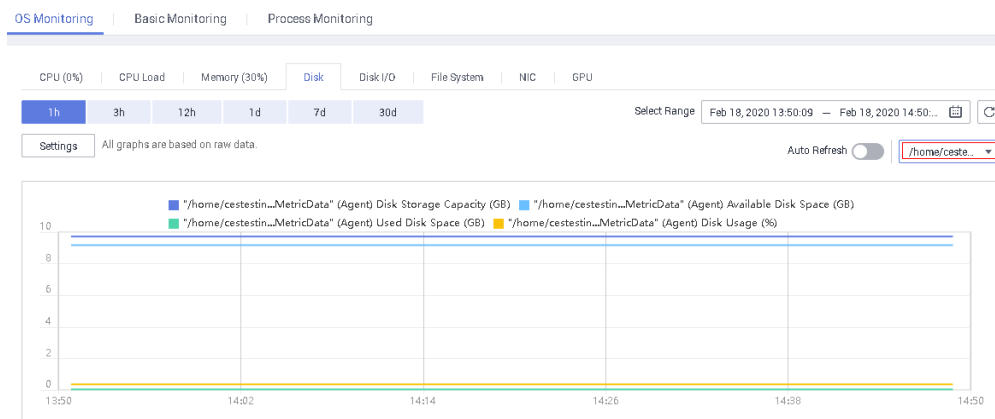
When monitoring data of a metric is not reported to Cloud Eye for three consecutive hours, the alarm rule status changes to **Insufficient data**.

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.

**Figure 3-1** Viewing the data disk usage on the **OS Monitoring** page

## 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?](#)
- [4.2 Why I Cannot See the Monitoring Data on the Cloud Eye Console After Purchasing Cloud Service Resources?](#)
- [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?](#)
- [4.4 Why Is Basic Monitoring Data Inconsistent with Data Monitored by the OS?](#)
- [4.5 Why Are the Network Traffic Metric Values in Cloud Eye Different from Those Detected in ECS?](#)
- [4.6 Why Is the Metric Collection Point Lost During Certain Periods of Time?](#)
- [4.7 Why Are the Four Metrics Memory Usage, Disk Usage, Inband Incoming Rate, and Inband Outgoing Rate Not Displayed for an ECS?](#)
- [4.8 What Are the Impacts on ECS Metrics If UVP VMTools Is Not Installed on ECSs?](#)
- [4.9 Why Are the Inbound Bandwidth and Outbound Bandwidth Negative?](#)

## 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?

The cloud platform is 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. 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**, wait for 2 minutes. It takes about 2 minutes before monitoring data is displayed on the Cloud Eye console.

If **Agent Status** is **Running**, 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.

### NOTE

Run the command `timedatectl set-timezone 'Asia/Shanghai'` to change the BMS time to the Cloud Eye time.

## 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 monitoring metrics supported by different OSs, see [Basic ECS Metrics](#).

To monitor the memory usage, disk usage, inband incoming rate, and inband outgoing rate, see [Installing the Agent on a Linux Server](#).

## 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](#).

## 4.9 Why Are the Inbound Bandwidth and Outbound Bandwidth Negative?

If Docker is installed, the early version of the Agent cannot collect statistics on the inbound and outbound bandwidth of virtual NICs when the container is restarted. As a result, a negative value is generated because the difference is calculated.

To update the Agent, see [Managing the Agent](#).

# 5 Metric Descriptions

## 5.1 What Are Outband Incoming Rate and Outband Outgoing Rate?

### 5.1 What Are Outband Incoming Rate and Outband Outgoing Rate?

#### Concept Explanation

You need to understand the meaning of outband and inband:

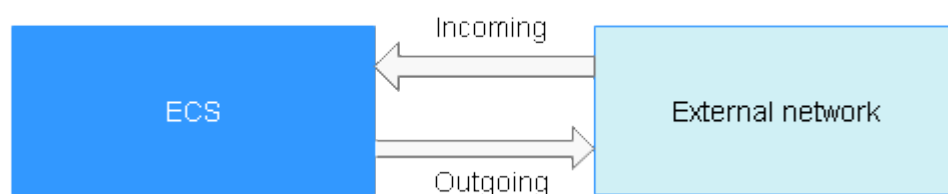
#### Outband

- Outband is the opposite to inband. Inband indicates that the monitored object is an ECS. Outband indicates that the monitored object is the physical server at the virtualization layer.

#### Incoming and Outgoing

- Incoming indicates traffic comes to an ECS per second.
- Outgoing indicates traffic sent from an ECS to an external network or client per second.

The following figure shows the traffic directions.



## Metric Description

**Table 5-1** Outband incoming/outgoing rate

Item	Description
Outband incoming rate	Traffic coming into an ECS per second For example, traffic generated when you download resources to an ECS from an external network or upload files to the ECS. Unit: byte/s
Outband outgoing rate	Traffic going out of an ECS per second For example, traffic generated when users access an ECS via the internet or when the ECS functions as an FTP server for users to download resources. Unit: byte/s

**Table 5-2** Outband incoming/outgoing rate

Item	Description
Outband incoming rate	Traffic coming to an ECS per second at the virtualization layer. Generally, the outband incoming rate is slightly larger than the traffic coming to the ECS because the virtualization layer will filter some unnecessary packets. Unit: byte/s
Outband outgoing rate	Traffic going out of an ECS per second at the virtualization layer. Generally, the outband outgoing rate is slightly larger than the traffic sent from the ECS because the virtualization layer will filter some unnecessary packets. Unit: byte/s

# 6 User Permissions

- [6.1 What Should I Do If the IAM Account Permissions Are Abnormal?](#)
- [6.2 What Can I Do If the System Displays a Message Indicating Insufficient Permissions When I Access Cloud Eye?](#)
- [6.3 What Can I Do If the System Displays a Message Indicating Insufficient Permissions When I Click Configure on the Server Monitoring Page?](#)

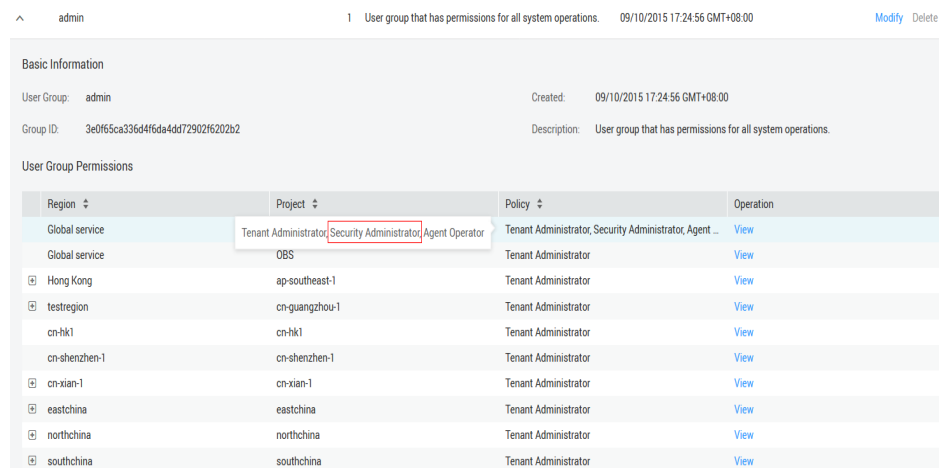
## 6.1 What Should I Do If the IAM Account Permissions Are Abnormal?

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](#).

**Figure 6-1** Checking the permissions



Region	Project	Policy	Operation
Global service	Tenant Administrator, Security Administrator, Agent Operator	Tenant Administrator, Security Administrator, Agent ...	<a href="#">View</a>
Global service	OBS	Tenant Administrator	<a href="#">View</a>
Hong Kong	ap-southeast-1	Tenant Administrator	<a href="#">View</a>
testregion	cn-guangzhou-1	Tenant Administrator	<a href="#">View</a>
cn-hk1	cn-hk1	Tenant Administrator	<a href="#">View</a>
cn-shenzhen-1	cn-shenzhen-1	Tenant Administrator	<a href="#">View</a>
cn-xian-1	cn-xian-1	Tenant Administrator	<a href="#">View</a>
eastchina	eastchina	Tenant Administrator	<a href="#">View</a>
northchina	northchina	Tenant Administrator	<a href="#">View</a>
southchina	southchina	Tenant Administrator	<a href="#">View</a>

## 6.2 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. Grant permissions to the user group which the IAM user belongs to.

For details, see [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](#).

## 6.3 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 6-2** Create Custom Policy

★ Policy Name

Policy View Visual editor JSON

★ Policy Content

```
1 {  
2   "Version": "1.1",  
3   "Statement": [  
4     {  
5       "Effect": "Allow",  
6       "Action": [  
7         "iam:roles:listRoles",  
8         "iam:permissions:listRolesForAgencyOnProject",  
9         "iam:agencies:listAgencies",  
10        "iam:agencies:getAgency"  
11      ]  
12    }  
13  ]  
14 }
```

Description

Scope Global services

**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 6-3 Assign Permissions**

**Region-based Authorization**

You can grant permissions to users so that they can access resources of projects in different regions.

Scope

**Global service project**  
Select this option to assign permissions for global services, such as OBS, based on the global service project. Users in the user group do not need to switch regions when accessing these services. [Learn more](#)

**Region-specific projects**  
Select this option to assign permissions for project-level services, such as ECS, based on region-specific projects. Users in the user group can access these services only in the selected projects. If you want to assign permissions for all projects, select "All projects". [Learn more](#)

Permissions Can't find the permissions you need?

View Selected (0) Custom policies

<input type="checkbox"/>	Policy/Role Name	Description	Type
<input type="checkbox"/>	test	--	Custom policy

----End