Cloud Eye

FAQs

Issue 01

Date 2025-11-14

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Trademarks and Permissions


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

Notice

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

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

Huawei Cloud Computing Technologies Co., Ltd.

Address: Huawei Cloud Data Center Jiaoxinggong Road
Qianzhong Avenue
Gui'an New District
Gui Zhou 550029
People's Republic of China

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

Contents

1 Product Usage 1
1.1 Server Monitoring 1
1.1.1 How Do I Configure DNS and Security Groups? 1
1.1.2 How Do I Configure an Agency? 3
1.1.3 How Does the Cloud Eye Agent Obtain a Temporary AK/SK? 4
1.1.4 What OSs Does the Agent Support? 5
1.1.5 What Are Resource Usage and Circuit Breaker Pattern of Agent? 9
1.1.6 Will the Agent Affect the Server Performance? 9
1.1.7 What Statuses Does the Agent Have? 10
1.1.8 What Metrics Are Supported by the Agent? 11
1.1.9 Environment Constraints for GPU Monitoring 110
1.1.10 BMS Hardware Metrics 111
1.1.11 How Can I Quickly Restore Agent Configurations? 113
1.1.12 How Can I Enable OS Monitoring for a New ECS? 114
1.1.13 What Are Agent Statuses and Troubleshooting Methods? 116
1.1.14 Why Is Basic Monitoring Data Inconsistent with OS Monitoring Data? 117
1.1.15 Why Are the Network Traffic Values on Cloud Eye Different from Those in ECS? 117
1.1.16 What Are the Impacts on ECS Metrics If UVP VMTools Is Not Installed on ECSs? 118
1.1.17 Why Are Memory Usage, Disk Usage, Inband Incoming Rate, and Inband Outgoing Rate Not Displayed for an ECS? 118
1.1.18 What Should I Do If There Are No GPU Monitoring Records? 118
1.1.19 What Should I Do If an Error Is Reported When I Run the Agent Installation Command? 119
1.1.20 How Do I Enable or Disable Metric Collection by Modifying the Configuration File? 120
1.1.21 How Do I Change the Agent Resource Usage Threshold by Modifying the Configuration File? 121
1.1.22 How Do I Change the Process Collection Frequency by Modifying the Configuration File? 123
1.2 Cloud Service Monitoring 124
1.2.1 What Is Aggregation? 125
1.2.2 How Long Is Metric Data Retained? 125
1.2.3 What Aggregation Methods Does Cloud Eye Support? 126
1.2.4 How Can I Export Collected Data? 126
1.2.5 What Are Outband Incoming Rate and Outband Outgoing Rate? 127
1.2.6 Why Is the Total Number of Resources for the Same Cloud Service Inconsistent on Different Monitoring Pages? 128
1.3 Alarm Management 129

1.3.1 What Are Alarm Notifications? How Many Types of Alarm Notifications Are There? 129
1.3.2 What Alarm Status Does Cloud Eye Support? 130
1.3.3 What Alarm Severities Are Available on Cloud Eye? 130
1.3.4 How Do I Monitor and View the Disk Usage? 130
1.3.5 How Can I Change the Phone Number and Email Address for Receiving Alarm Notifications? 130
1.3.6 How Can an IAM User Receive Alarm Notifications? 131
1.3.7 Why Are Resource Names Not Displayed in Alarm Notifications? 131
1.3.8 Why Are Unreached Cloud Services Displayed on the Cloud Eye Console? 132
2 Troubleshooting 134
2.1 Permissions Management 134
2.1.1 What Should I Do If the IAM Account Permissions Are Abnormal? 134
2.1.2 What Can I Do If the System Displays a Message Indicating Insufficient Permissions When I Access Cloud Eye? 134
2.1.3 What Can I Do If the System Displays a Message Indicating Insufficient Permissions When I Click Configure on the Server Monitoring Page? 135
2.2 Server Monitoring 138
2.2.1 What Should I Do If the Monitoring Is Periodically Interrupted or the Agent Status Keeps Changing? 138
2.2.2 What Should I Do If a Service Port Is Used by the Agent? 140
2.2.3 Troubleshooting Agent One-Click Restoration Failures 141
2.2.4 Why Is No Monitoring Data Displayed After Performing a One-Click Restoration for the Agent? 143
2.2.5 How Can I Troubleshoot the Issue of Reported Metrics Being Discarded? 146
2.2.6 What Should I Do If the Agent Status Is Faulty? 147
2.2.7 What Should I Do If the Agent Is Stopped? 148
2.2.8 What Should I Do If the Agent Status Is Running But There Is No Monitoring Data? 149
2.2.9 What Can I Do If No Monitoring Data Is Displayed After One-Click Agent Restoration? (Old Agent) 149
2.2.10 How Do I Obtain Debug Logs of the Agent? 152
2.2.11 Why Is OS Monitoring Data Not Displayed Immediately After the Agent Is Installed and Configured or Not Displayed at All? 154
2.2.12 Why Is the Metric Collection Point Lost During Certain Periods of Time? 154
2.2.13 Why Are the Inbound Bandwidth and Outbound Bandwidth Negative? 154
2.2.14 Why Is There No Block Device Usage Metric for One of the Two Disks on a Server? 154
2.2.15 Why Is the Agent Status Abnormal on the Cloud Eye Server Monitoring Page While OS Monitoring Metrics Are Displayed as Normal? 156
2.3 Cloud Service Monitoring 156
2.3.1 What Should I Do If I See Garbled Chinese Characters in an Exported CSV File? 156
2.3.2 Why Is the Monitoring Data Not Displayed on the Cloud Eye Console? 157
2.3.3 Why I Cannot See the Monitoring Data on the Cloud Eye Console After Purchasing Cloud Service Resources? 157
2.4 Alarm Management 158
2.4.1 When Will an "Insufficient data" Alarm Be Triggered? 158
2.4.2 Why Did I Receive a Bandwidth Overflow Notification While There Is No Bandwidth Overflow Record in the Monitoring Data? 158

2.4.3 Why Can't an Alarm Be Triggered After a 5-Minute Aggregated Metric Alarm Rule Is Configured? 158
2.4.4 Why Is an Alarm Triggered Contrary to the Alarm Rule That Both the Disk Read and Write Metrics Must Reach the Thresholds 158
2.5 Data Dump 159
2.5.1 What Should I Do When There Is an Abnormal Dump Destination? 159

1 Product Usage

1.1 Server Monitoring
1.2 Cloud Service Monitoring
1.3 Alarm Management

1.1 Server Monitoring

1.1.1 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

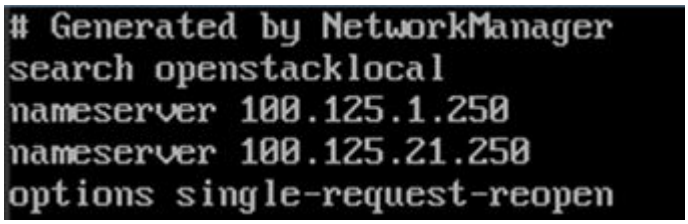
- **Modifying a DNS Server Address (Command Lines)**

  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 **resolv.conf** file.
  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 1-1 Adding DNS server addresses (Linux)



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. This topic takes an ECS as an example. The operations for BMSs are similar.

  a. Log in to the management console.
  b. In the upper left corner, select a region and project.
  c. Click **Service List** in the upper left corner. Under **Compute**, select **Elastic Cloud Server**.

     In the ECS list, click an ECS name to view its details.
  d. In the **ECS Information** area of the **Summary** tab, click the VPC name.

     The **Virtual Private Cloud** page is displayed.
  e. Click the VPC name.
  f. In the **Networking Components** area, click the number next to **Subnets**.

     The **Subnets** page is displayed.
  g. In the subnet list, locate the target subnet and click its name.
  h. 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.
  i. Click **OK**.

     NOTE

     The new DNS server address is applied 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 1-1**.

Table 1-1 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.
TCP	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.
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.

1.1.2 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, the system will perform 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**), select a server, and click **Configure**, the system will create an agency named **cesagency** on IAM. The agency permissions are automatically granted to Cloud Eye internal account **op_svc_ces**.

  NOTE

  If the system displays a message indicating that the tenant does not have insufficient permissions, see **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. This way, 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.

1.1.3 How Does the Cloud Eye Agent Obtain a Temporary AK/SK?

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 **cesgency** for **Agency** in **Advanced Options** when creating an ECS. The system automatically authorizes the Agent and provides a temporary AK/SK for the Agent. New ECSs or BMSs in this region will automatically get this authorization, which is detailed as follows:

- Authorization object

  On the Cloud Eye console, if you choose **Server Monitoring** > **Elastic Cloud Server** (or **Bare Metal Server**), select an ECS (or BMS), and click **Configure**, the system will create an agency named **cesagency** on IAM. The agency permissions are 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, see **2.1.3 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 Administrator** permission 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. This way, you can query the ECS or BMS monitoring data on the Cloud Eye console or by calling the Cloud Eye APIs.

  – Secure: The AK/SK used by the Agent is temporary and has only the **CES Administrator** permissions to allow you to operate Cloud Eye resources.

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

If **cesagency** cannot be found on the IAM **Agencies** page after authorization, you can manually create it on the IAM console. For details about how to create an agency, 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**.

1.1.4 What OSs Does the Agent Support?

The following table lists OSs that are proven to be compatible with the Agent. More OSs will be supported soon.

NOTICE

The following systems are created using public images or those provided by Huawei Cloud Image Management Service (IMS). Using an unverified external system may lead to dependency issues or introduce other instability factors.

Operating System	Version	Agent Installation (ECS)	Agent Installation (BMS)
Windows	Windows 2012	Supported	Supported
	Windows 2016	Supported	Supported
	Windows 2019	Supported	Supported
	Windows 2022	Supported	Supported
CentOS	CentOS 6.9 64bit	Supported	Not supported
	CentOS 6.10 64bit	Supported	Not supported
	CentOS 7.2 64bit	Supported	Supported
	CentOS 7.3 64bit	Supported	Supported

Operating System	Version	Agent Installation (ECS)	Agent Installation (BMS)
	CentOS 7.4 64bit	Supported	Supported
	CentOS 7.5 64bit	Supported	Not supported
	CentOS 7.6 64bit	Supported	Supported
	CentOS 7.6 64bit(ARM)	Not supported	√
	CentOS 7.7 64bit	Supported	Not supported
	CentOS 7.8 64bit	Supported	Not supported
	CentOS 7.9 64bit	Supported	Supported
	CentOS 8.0 64bit	Supported	Not supported
	CentOS 8.1 64bit	Supported	Not supported
	CentOS 8.2 64bit	Supported	Not supported
	CentOS Stream 8/x86	Supported	Not supported
	CentOS Stream 8/Arm	√	Not supported
	CentOS Stream 9/x86	Supported	Not supported
Alma Linux	AlmaLinux 8.3 64bit	Supported	Not supported
	AlmaLinux 8.4 64bit	Supported	Not supported
	AlmaLinux 8.6 64bit	Supported	Not supported
	AlmaLinux 8.7	Supported	Not supported
	AlmaLinux 9.1	Supported	Not supported
	AlmaLinux 9.0 64bit	Supported	Not supported
Debian	Debian 9.0.0 64bit	Supported	Not supported
	Debian 8.8.0 64bit	Supported	Not supported
	Debian 8.2.0 64bit	Supported	Not supported
	Debian 10.0.0 64bit	Supported	Not supported
	Debian 10.2.0 64bit(ARM)	√	Not supported
	Debian 10.5 64bit	Supported	Not supported
	Debian 10.6 64bit	Supported	Not supported

Operating System	Version	Agent Installation (ECS)	Agent Installation (BMS)
	Debian11.10 64bit	Supported	Not supported
	Debian 11.4 64bit	Supported	Not supported
	Debian 11.5 64bit	Supported	Not supported
	Debian 12.0.0 64bit	Supported	Not supported
EulerOS	EulerOS 2.8 64bit	Not supported	Supported
	EulerOS 2.5 64bit	Supported	Not supported
	EulerOS 2.3 64bit	Not supported	Supported
	EulerOS 2.2 64bit	Supported	Not supported
	EulerOS 2.8 64bit(ARM)	√	√
	EulerOS 2.9 64bit	Supported	Supported
	EulerOS 2.9 64bit(ARM)	√	Not supported
	EulerOS 2.10 64bit	Supported	Supported
Fedora	Fedora 30 64bit	Supported	Not supported
	Fedora 31 64bit	Supported	Not supported
	Fedora 36 64bit	Supported	Not supported
	Fedora 37 64bit	Supported	Not supported
	Fedora 38 64bit	Supported	Not supported
Huawei Cloud EulerOS	Huawei Cloud EulerOS 1.0 64bit	Supported	Not supported
	Huawei Cloud EulerOS 1.1 64bit	Supported	Not supported
	Huawei Cloud EulerOS 2.0 64bit	Supported	Supported
	Huawei Cloud EulerOS 2.0 ARM 64bit	Supported	Supported
KylinOS	Kylin Linux Advanced Server for Kunpeng V1	Supported	Not supported

Operating System	Version	Agent Installation (ECS)	Agent Installation (BMS)
	Kylin-Server-10-SP2-20210524-x86.iso	Supported	Not supported
	Kylin-Server-10-SP2-20210524-arm.iso	√	Not supported
openEuler	openEuler 20.03 64bit	Supported	Not supported
	openEuler 20.03 LTS SP3 64bit	Supported	Not supported
	openEuler 22.03 LTS(ARM)	Not supported	√
	openEuler 22.03 LTS 64bit	Supported	Not supported
OpenSUSE	OpenSUSE 15.0 64bit	Supported	Not supported
	SUSE 15 SP5 X86	Supported	Not supported
	SUSE 15 SP6 X86	Supported	Not supported
Redhat	Redhat Linux Enterprise 6.9 64bit	Not supported	Supported
	Redhat Linux Enterprise 7.4 64bit	Not supported	Supported
Rocky Linux	Rocky Linux 8.4 64bit	Supported	Not supported
	Rocky Linux 8.5 64bit	Supported	Not supported
	Rocky Linux 8.6 64 bit	Supported	Not supported
	Rocky Linux 9.0 64bit	Supported	Not supported
	Rocky Linux 9.1	Supported	Not supported
	Rocky Linux 8.7-X86	Supported	Not supported
	Rocky Linux 9.3-X86	Supported	Not supported
	Rocky Linux 8.7-ARM	√	Not supported

Operating System	Version	Agent Installation (ECS)	Agent Installation (BMS)
Ubuntu	Ubuntu 22.04 server 64bit	Supported	Not supported
	Ubuntu 20.04 server 64bit	Supported	Supported
	Ubuntu 18.04 server 64bit	Supported	Supported
	Ubuntu 18.04 server 64bit(ARM)	Not supported	√
	Ubuntu 16.04 server 64bit	Supported	Supported
	Ubuntu 14.04 server 64bit	Not supported	Supported
	Ubuntu 18.04.6 server 64bit	Supported	Not supported
UnionTechOS	UnionTech OS Server 20 Euler (1000) 64bit(ARM)	√	Not supported
	UnionTech OS-Server-20-1050e-amd64-UFU.iso	Supported	Not supported

1.1.5 What Are 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 three times in a row, the Agent will implement the circuit breaker pattern, and server metrics will not be collected. The Agent will restart it later.

1.1.6 Will the Agent Affect the 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 MB of memory. Generally, the CPU usage of a single core is less than 5%, and the memory 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 MB of memory. Generally, the CPU usage of a single core is less than 5%, and the memory is less than 100 MB.

1.1.7 What Statuses Does the Agent Have?

The Agent has the following statuses:

- **Not installed or started**: The Agent is not installed on an ECS or BMS or has been manually stopped.
- **Running**: The Agent is running and can report monitoring data.
- **Installing**: The Agent is being installed.
- **Faulty**: The Agent failed to send a heartbeat message to Cloud Eye for three consecutive minutes. In this case:
  - The domain name of the Agent cannot be resolved. Check whether the DNS server address is correct by referring to **Modifying the DNS Server Address and Adding Security Group Rules (Linux)**. If it is, 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 the Agent by referring to **Managing the Agent**. If the Agent cannot be restarted, related files are deleted by mistake. In this case, reinstall the Agent.
- **Configuration error**:
  - No agency has been configured for the ECS or BMS.
  - Permissions of the current agency are abnormal
  - The current agency is invalid.
  - The security group rule of the default NIC is incorrect, or the DNS configuration is incorrect.
- **Stopped**: The Agent is manually stopped. To start it, see **Managing the Agent**.

1.1.8 What Metrics Are Supported by the Agent?

OS metric: CPU

Metric	Name	Description	Value Range	Unit	Conversion Rule	Earliest Agent Version Required	Monitoring Period (Raw Data)
cpu_usage	(Agent) CPU Usage	Used to monitor CPU usage • Collection method (Linux): Check the metric value changes in file **/proc/stat** in a collection period. You can run the **top** command to check the **%Cpu(s)** value. • Collection method (Windows): Obtain the metric value using the API **GetSystemTimes**.	0-100	%	N/A	2.4.1	1 minute

Metric	Name	Description	Value Range	Unit	Conversion Rule	Earliest Agent Version Required	Monitoring Period (Raw Data)
cpu_usage_idle	(Agent) Idle CPU Usage	Percentage of the time that CPU is idle Unit: Percent • Collection method (Linux): Check the metric value changes in file **/proc/stat** in a collection period. • Collection method (Windows): Obtain the metric value using the API **GetSystemTimes**.	0-100	%	N/A	2.4.5	1 minute

Metric	Name	Description	Value Range	Unit	Conversion Rule	Earliest Agent Version Required	Monitoring Period (Raw Data)
cpu_usage_other	(Agent) Other Process CPU Usage	Other CPU usage of the monitored object • Collection method (Linux): **Other Process CPU Usage** = 1– **Idle CPU Usage** – **Kernel Space CPU Usage** – **User Space CPU Usage** • Collection method (Windows): **Other Process CPU Usage** = 1– **Idle CPU Usage** – **Kernel Space CPU Usage** – **User Space CPU Usage**	0-100	%	N/A	2.4.5	1 minute

Metric	Name	Description	Value Range	Unit	Conversion Rule	Earliest Agent Version Required	Monitoring Period (Raw Data)
cpu_usage_system	(Agent) Kernel Space CPU Usage	Percentage of time that the CPU is used by kernel space • Collection method (Linux): Check the metric value changes in file **/proc/stat** in a collection period. You can run the **top** command to check the **%Cpu(s) sy** value. • Collection method (Windows): Obtain the metric value using the API **GetSystemTimes**.	0-100	%	N/A	2.4.5	1 minute

Metric	Name	Description	Value Range	Unit	Conversion Rule	Earliest Agent Version Required	Monitoring Period (Raw Data)
cpu_usage_user	(Agent) User Space CPU Usage	Percentage of time that the CPU is used by user space • Collection method (Linux): Check the metric value changes in file **/proc/stat** in a collection period. You can run the **top** command to check the **%Cpu(s) us** value. • Collection method (Windows): Obtain the metric value using the API **GetSystemTimes**.	0-100	%	N/A	2.4.5	1 minute

Metric	Name	Description	Value Range	Unit	Conversion Rule	Earliest Agent Version Required	Monitoring Period (Raw Data)
cpu_usage_nice	(Agent) Nice Process CPU Usage	Percentage of the time that the CPU is in user mode with low-priority processes which can easily be interrupted by higher-priority processes • Collection method (Linux): Check the metric value changes in file **/proc/stat** in a collection period. You can run the **top** command to check the **%Cpu(s) ni** value. • Collection method (Windows): not supported	0-100	%	N/A	2.4.5	1 minute

Metric	Name	Description	Value Range	Unit	Conversion Rule	Earliest Agent Version Required	Monitoring Period (Raw Data)
cpu_usage_iowait	(Agent) iowait Process CPU Usage	Percentage of time that the CPU is waiting for I/O operations to complete • Collection method (Linux): Check the metric value changes in file **/proc/stat** in a collection period. You can run the **top** command to check the **%Cpu(s) wa** value. • Collection method (Windows): not supported	0-100	%	N/A	2.4.5	1 minute

Metric	Name	Description	Value Range	Unit	Conversion Rule	Earliest Agent Version Required	Monitoring Period (Raw Data)
cpu_usage_irq	(Agent) CPU Interrupt Time	Percentage of time that the CPU is servicing interrupts • Collection method (Linux): Check the metric value changes in file **/proc/stat** in a collection period. You can run the **top** command to check the **%Cpu(s) hi** value. • Collection method (Windows): not supported	0-100	%	N/A	2.4.5	1 minute

Metric	Name	Description	Value Range	Unit	Conversion Rule	Earliest Agent Version Required	Monitoring Period (Raw Data)
cpu_usage_softirq	(Agent) CPU Software Interrupt Time	Percentage of time that the CPU is servicing software interrupts • Collection method (Linux): Check the metric value changes in file **/proc/stat** in a collection period. You can run the **top** command to check the **%Cpu(s) si** value. • Collection method (Windows): not supported	0-100	%	N/A	2.4.5	1 minute

OS Metric: CPU Load

Metric	Name	Description	Value Range	Unit	Conversion Rule	Earliest Agent Version Required	Monitoring Period (Raw Data)
load_average1	(Agent) 1-Minute Load Average	CPU load averaged from the last 1 minute • Collection method (Linux): The value of this metric is the result of the value of **load1** in **/proc/loadavg** divided by the number of logical CPUs. You can run the **top** command to check the value of **load1**. • Collection method (Windows): not supported	≥ 0	None	N/A	2.4.1	1 minute

Metric	Name	Description	Value Range	Unit	Conversion Rule	Earliest Agent Version Required	Monitoring Period (Raw Data)
load_average5	(Agent) 5-Minute Load Average	CPU load averaged from the last 5 minutes • Collection method (Linux): The value of this metric is the result of the value of **load5** in **/proc/loadavg** divided by the number of logical CPUs. You can run the **top** command to check the value of **load5**. • Collection method (Windows): not supported	≥ 0	None	N/A	2.4.1	1 minute

Metric	Name	Description	Value Range	Unit	Conversion Rule	Earliest Agent Version Required	Monitoring Period (Raw Data)
load_average15	(Agent) 15-Minute Load Average	CPU load averaged from the last 15 minutes • Collection method (Linux): The value of this metric is the result of the value of **load15** in **/proc/loadavg** divided by the number of logical CPUs. You can run the **top** command to check the value of **load15**. • Collection method (Windows): not supported	≥ 0	None	N/A	2.4.1	1 minute

OS Metric: Memory

Metric	Name	Description	Value Range	Unit	Conversion Rule	Earliest Agent Version Required	Monitoring Period (Raw Data)
mem_available	(Agent) Available Memory	Amount of memory that is available and can be given instantly to processes • Collection method (Linux): Obtain the metric value from **/proc/meminfo**. If **MemAvailable** is displayed in **/proc/meminfo**, obtain the value. If **MemAvailable** is not displayed in **/proc/meminfo**, **MemAvailable** = **MemFree** + **Buffers** +**Cached** • Collection method (Windows): formula (Available memory – Used memory) The value is obtained by calling the Windows API GlobalMemoryStatusEx.	≥ 0	GB	N/A	2.4.5	1 minute

Metric	Name	Description	Value Range	Unit	Conversion Rule	Earliest Agent Version Required	Monitoring Period (Raw Data)
mem_usedPercent	(Agent) Memory Usage	Memory usage of the instance • Collection method (Linux): Obtain the metric value from the **/proc/meminfo** file (**MemTotal**-**MemAvailable**)/**MemTotal**. If **MemAvailable** is displayed in **/proc/meminfo**, **MemUsedPercent** = (**MemTotal**-**MemAvailable**)/**MemTotal** If **MemAvailable** is not displayed in **/proc/meminfo**, **MemUsedPercent** = (**MemTotal** – **MemFree** – **Buffers** – **Cached**)/**MemTotal** • Collection method (Windows): formula (Used memory size/Total memory size x 100%)	0-100	%	N/A	2.4.1	1 minute

Metric	Name	Description	Value Range	Unit	Conversion Rule	Earliest Agent Version Required	Monitoring Period (Raw Data)
mem_free	(Agent) Idle Memory	Amount of memory that is not being used • Collection method (Linux): Obtain the metric value from **/proc/meminfo**. • Collection method (Windows): not supported	≥ 0	GB	N/A	2.4.5	1 minute
mem_buffers	(Agent) Buffer	Amount of memory that is being used for buffers • Collection method (Linux): Obtain the metric value from **/proc/meminfo**. You can run the **top** command to check the **KiB Mem:buffers** value. • Collection method (Windows): not supported	≥ 0	GB	N/A	2.4.5	1 minute

Metric	Name	Description	Value Range	Unit	Conversion Rule	Earliest Agent Version Required	Monitoring Period (Raw Data)
mem_cached	(Agent) Cache	Amount of memory that is being used for file caches • Collection method (Linux): Obtain the metric value from **/proc/meminfo**. You can run the **top** command to check the **KiB Swap:cached Mem** value. • Collection method (Windows): not supported	≥ 0	GB	N/A	2.4.5	1 minute
total_open_files	(Agent) Total File Handles	Total handles used by all processes • Collection method (Linux): Use the **/proc/{pid}/fd** file to summarize the handles used by all processes. • Collection method (Windows): not supported	≥ 0	Count	N/A	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	Value Range	Unit	Conversion Rule	Earliest Agent Version Required	Monitoring Period (Raw Data)
disk_free	(Agent) Available Disk Space	Free space on the disks • Collection method (Linux): Run the **df -h** command to check the value in the **Avail** 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 (~). • Collection method (Windows): Use the Windows Management Instrumentation (WMI) API GetDiskFreeSpaceExW to obtain disk space data. The path of	≥ 0	GB	N/A	2.4.1	1 minute

Metric	Name	Description	Value Range	Unit	Conversion Rule	Earliest Agent Version Required	Monitoring Period (Raw Data)
		the mount point prefix cannot exceed 64 characters. It must start with a letter, and contain only digits, letters, hyphens (-), periods (.), and swung dashes (~).					

Metric	Name	Description	Value Range	Unit	Conversion Rule	Earliest Agent Version Required	Monitoring Period (Raw Data)
disk_total	(Agent) Disk Storage Capacity	Total disk capacity • Collection method (Linux): Run the **df -h** command to check the value in the **Size** 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 (~). • Collection method (Windows): Use the WMI API GetDiskFreeSpaceExW to obtain disk space data. The path of the mount point prefix cannot exceed	≥ 0	GB	N/A	2.4.5	1 minute

Metric	Name	Description	Value Range	Unit	Conversion Rule	Earliest Agent Version Required	Monitoring Period (Raw Data)
		64 characters. It must start with a letter, and contain only digits, letters, hyphens (-), periods (.), and swung dashes (~).					

Metric	Name	Description	Value Range	Unit	Conversion Rule	Earliest Agent Version Required	Monitoring Period (Raw Data)
disk_used	(Agent) Used Disk Space	Disk's used space • Collection method (Linux): Run the **df -h** command to check the value in the **Used** 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 (~). • Collection method (Windows): Use the WMI API GetDiskFreeSpaceExW to obtain disk space data. The path of the mount point prefix cannot exceed 64 characters.	≥ 0	GB	N/A	2.4.5	1 minute

Metric	Name	Description	Value Range	Unit	Conversion Rule	Earliest Agent Version Required	Monitoring Period (Raw Data)
		It must start with a letter, and contain only digits, letters, hyphens (-), periods (.), and swung dashes (~).					

Metric	Name	Description	Value Range	Unit	Conversion Rule	Earliest Agent Version Required	Monitoring Period (Raw Data)
disk_usedPercent	(Agent) Disk Usage	Percentage of used disk space. It is calculated as follows: **Disk Usage** = **Used Disk Space**/**Disk Storage Capacity**. • 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 (~). • Collection method (Windows): Use the WMI API GetDiskFreeSpaceExW to obtain disk space data. The path of	0-100	%	N/A	2.4.1	1 minute

Metric	Name	Description	Value Range	Unit	Conversion Rule	Earliest Agent Version Required	Monitoring Period (Raw Data)
		the mount point prefix cannot exceed 64 characters. It must start with a letter, and contain only digits, letters, hyphens (-), periods (.), and swung dashes (~).					
disk_rwstate	(Agent) Disk Read/ Write Status	Read and write status of the disk attached to the monitored object. The status can be **0** (read and write) or **1** (read-only). • Collection method (Linux): Obtain the disk attachment status from the **/proc/1/mountinfo** file. • Collection method (Windows): not supported	• **0**: read and write • **1**: read-only	None	N/A	2.5.6	1 minute

OS Metric: Disk I/O

Metric	Name	Description	Value Range	Unit	Conversion Rule	Earliest Agent Version Required	Monitoring Period (Raw Data)
disk_agt_read_bytes_rate	(Agent) Disks Read Rate	Volume of data read from the instance per second • Collection method (Linux): Calculate the data changes in the sixth column of the corresponding device in file **/proc/diskstats** 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 (~). • Collection method (Windows): Use Win32_PerfFormattedData_PerfDisk_LogicalDisk object in WMI to obtain disk I/O data.	≥ 0	byte/s	1024(IEC)	2.4.5	1 minute

Metric	Name	Description	Value Range	Unit	Conversion Rule	Earliest Agent Version Required	Monitoring Period (Raw 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.					

Metric	Name	Description	Value Range	Unit	Conversion Rule	Earliest Agent Version Required	Monitoring Period (Raw Data)
disk_agt_read_requests_rate	(Agent) Disks Read Requests	Number of read requests sent to the monitored disk per second • Collection method (Linux): The disk read requests are calculated by calculating the data changes in the fourth column of the corresponding device in file **/proc/diskstats** 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 (~). • Collection method (Windows): Use Win32_PerfFormattedData_PerfDisk_LogicalDisk object in WMI to obtain disk I/O data.	≥ 0	Request/s	N/A	2.4.5	1 minute

Metric	Name	Description	Value Range	Unit	Conversion Rule	Earliest Agent Version Required	Monitoring Period (Raw 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.					

Metric	Name	Description	Value Range	Unit	Conversion Rule	Earliest Agent Version Required	Monitoring Period (Raw Data)
disk_agt_write_bytes_rate	(Agent) Disks Write Rate	Volume of data written to the instance per second • Collection method (Linux): The disk write rate is calculated by calculating the data changes in the tenth column of the corresponding device in file **/proc/diskstats** 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 (~). • Collection method (Windows): Use Win32_PerfFormattedData_PerfDisk_LogicalDisk object in WMI to obtain disk I/O data.	≥ 0	byte/s	1024(IEC)	2.4.5	1 minute

Metric	Name	Description	Value Range	Unit	Conversion Rule	Earliest Agent Version Required	Monitoring Period (Raw 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.					

Metric	Name	Description	Value Range	Unit	Conversion Rule	Earliest Agent Version Required	Monitoring Period (Raw Data)
disk_agt_write_requests_rate	(Agent) Disks Write Requests	Number of write requests sent to the monitored disk per second • Collection method (Linux): The disk write requests are calculated by calculating the data changes in the eighth column of the corresponding device in file **/proc/diskstats** 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 (~). • Collection method (Windows): Use Win32_PerfFormattedData_PerfDisk_Logical	≥ 0	Request/s	N/A	2.4.5	1 minute

Metric	Name	Description	Value Range	Unit	Conversion Rule	Earliest Agent Version Required	Monitoring Period (Raw Data)
		Disk 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.					

Metric	Name	Description	Value Range	Unit	Conversion Rule	Earliest Agent Version Required	Monitoring Period (Raw Data)
disk_readTime	(Agent) Average Read Request Time	The average time taken for disk read operations • 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 **/proc/diskstats** 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 (~). • Collection method (Windows): not supported	≥ 0	ms/count	N/A	2.4.5	1 minute

Metric	Name	Description	Value Range	Unit	Conversion Rule	Earliest Agent Version Required	Monitoring Period (Raw Data)
disk_writeTime	(Agent) Average Write Request Time	The average time taken for disk write operations • 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 **/proc/diskstats** 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 (~). • Collection method (Windows): not supported	≥ 0	ms/count	N/A	2.4.5	1 minute

Metric	Name	Description	Value Range	Unit	Conversion Rule	Earliest Agent Version Required	Monitoring Period (Raw Data)
disk_ioUtils	(Agent) Disk I/O Usage	Percentage of the time that the disk has had I/O requests queued to the total disk operation time • 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 **/proc/diskstats** 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 (~). • Collection method (Windows): not supported	0-100	%	N/A	2.4.1	1 minute

Metric	Name	Description	Value Range	Unit	Conversion Rule	Earliest Agent Version Required	Monitoring Period (Raw Data)
disk_queue_length	(Agent) Disk Queue Length	Average number of read or write requests queued up for completion for the monitored disk in the monitoring period • 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 **/proc/diskstats** 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 (~). • Collection method (Windows): not supported	≥ 0	count	N/A	2.4.5	1 minute

Metric	Name	Description	Value Range	Unit	Conversion Rule	Earliest Agent Version Required	Monitoring Period (Raw Data)
disk_write_bytes_per_operation	Disk Bytes Per Write Operation	Average number of bytes in an I/O write for the monitored disk in the monitoring period • 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 **/proc/diskstats** 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 (~). • Collection method (Windows): not supported	≥ 0	Byte/op	N/A	2.4.5	1 minute

Metric	Name	Description	Value Range	Unit	Conversion Rule	Earliest Agent Version Required	Monitoring Period (Raw Data)
disk_read_bytes_per_operation	Disk Bytes Per Read Operation	Average number of bytes in an I/O read for the monitored disk in the monitoring period • 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 **/proc/diskstats** 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 (~). • Collection method (Windows): not supported	≥ 0	Byte/op	N/A	2.4.5	1 minute

Metric	Name	Description	Value Range	Unit	Conversion Rule	Earliest Agent Version Required	Monitoring Period (Raw Data)
disk_io_svctm	(Agent) Disk I/O Service Time	Average time in an I/O read or write for the monitored disk in the monitoring period • 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 **/proc/diskstats** 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 (~).	≥ 0	ms/op	N/A	2.4.5	1 minute

Metric	Name	Description	Value Range	Unit	Conversion Rule	Earliest Agent Version Required	Monitoring Period (Raw Data)
		• Collection method (Windows): not supported					
disk_device_used_percent	Block Device Usage	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. • Collection method (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. • Currently, Windows does not support this metric.	0-100	%	N/A	2.5.6	1 minute

OS Metric: File System

Metric	Name	Description	Value Range	Unit	Conversion Rule	Earliest Agent Version Required	Monitoring Period (Raw Data)
disk_fs_rwstate	(Agent) File System Read/ Write Status	Read and write status of the mounted file system of the monitored object The status can be **0** (read and write) or **1** (read-only). • Collection method (Linux): Check file system information in the fourth column in file **/proc/mounts**. • Collection method (Windows): not supported	• **0**: read and write • **1**: read-only	None	N/A	2.4.5	1 minute

Metric	Name	Description	Value Range	Unit	Conversion Rule	Earliest Agent Version Required	Monitoring Period (Raw Data)
disk_inodesTotal	(Agent) Disk inode Total	Total number of index nodes on the disk • Collection method (Linux): Run the **df -i** command to check the value in the **Inodes** 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 (~). • Collection method (Windows): not supported	≥ 0	None	N/A	2.4.5	1 minute

Metric	Name	Description	Value Range	Unit	Conversion Rule	Earliest Agent Version Required	Monitoring Period (Raw Data)
disk_inodesUsed	(Agent) Total inode Used	Number of used index nodes on the disk • Collection method (Linux): Run the **df -i** command to check the value in the **IUsed** 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 (~). • Collection method (Windows): not supported	≥ 0	None	N/A	2.4.5	1 minute

Metric	Name	Description	Value Range	Unit	Conversion Rule	Earliest Agent Version Required	Monitoring Period (Raw Data)
disk_inodesUsedPercent	(Agent) Percentage of Total inode Used	Number of used index nodes on the disk • Collection method (Linux): Run the **df -i** command to check the value in the **IUse %** 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 (~). • Collection method (Windows): not supported	0-100	%	N/A	2.4.1	1 minute

OS Metric: NTP

Metric	Name	Description	Value Range	Unit	Conversion Rule	Earliest Agent Version Required	Monitoring Period (Raw Data)
ntp_offset	(Agent) NTP Offset	NTP offset of the monitored object • Collection method (Linux): Run the **ntpq -p** or **chronyc sources -v** command. • Collection method (Windows): not supported	≥ 0	ms	N/A	2.7.1	1 minute

OS Metric: TCP Connections

By default, two basic metrics related to TCP connections are collected: (Agent) TCP TOTAL and (Agent) TCP ESTABLISHED.

Metric	Name	Description	Value Range	Unit	Conversion Rule	Earliest Agent Version Required	Monitoring Period (Raw Data)
net_tcp_total	(Agent) Total Number of TCP Connections	Total number of TCP connections • Collection method (Linux): Run the **ss -s** command to view the total number of TCP connections. **NOTE** The number of TCP connections refers to the number of all active TCP connections on an ECS. • Collection method (Windows): Obtain the metric value using the **GetTcpTable2** API.	≥ 0	count	N/A	2.4.1	1 minute

Metric	Name	Description	Value Range	Unit	Conversion Rule	Earliest Agent Version Required	Monitoring Period (Raw Data)
net_tcp_established	(Agent) Number of connections in the ESTABLISHED state	Number of TCP connections in the ESTABLISHED state • Collection method (Linux): Obtain TCP connections in all states from the **/proc/net/tcp** file, and then collect the number of connections in each state. • Collection method (Windows): Obtain the metric value using the **GetTcpTable2** API.	≥ 0	count	N/A	2.4.1	1 minute

Metric	Name	Description	Value Range	Unit	Conversion Rule	Earliest Agent Version Required	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 • Collection method (Linux): Obtain TCP connections in all states from the **/proc/net/tcp** file, and then collect the number of connections in each state. • Collection method (Windows): Obtain the metric value using the **GetTcpTable2** API.	≥ 0	count	N/A	2.4.5	1 minute

Metric	Name	Description	Value Range	Unit	Conversion Rule	Earliest Agent Version Required	Monitoring Period (Raw Data)
net_tcp_sys_recv	(Agent) Number of connections in the TCP SYS_RECV state.	Number of pending TCP connections received by the server • Collection method (Linux): Obtain TCP connections in all states from the **/proc/net/tcp** file, and then collect the number of connections in each state. • Collection method (Windows): Obtain the metric value using the **GetTcpTable2** API.	≥ 0	count	N/A	2.4.5	1 minute

Metric	Name	Description	Value Range	Unit	Conversion Rule	Earliest Agent Version Required	Monitoring Period (Raw Data)
net_tcp_fin_wait1	(Agent) Number of TCP connections in the FIN_WAIT1 state.	Number of TCP connections waiting for ACK packets when the connections are being actively closed by the client • Collection method (Linux): Obtain TCP connections in all states from the **/proc/net/tcp** file, and then collect the number of connections in each state. • Collection method (Windows): Obtain the metric value using the **GetTcpTable2** API.	≥ 0	count	N/A	2.4.5	1 minute

Metric	Name	Description	Value Range	Unit	Conversion Rule	Earliest Agent Version Required	Monitoring Period (Raw Data)
net_tcp_fin_wait2	(Agent) Number of TCP connections in the FIN_WAIT2 state.	Number of TCP connections in the FIN_WAIT2 state • Collection method (Linux): Obtain TCP connections in all states from the **/proc/net/tcp** file, and then collect the number of connections in each state. • Collection method (Windows): Obtain the metric value using the **GetTcpTable2** API.	≥ 0	count	N/A	2.4.5	1 minute

Metric	Name	Description	Value Range	Unit	Conversion Rule	Earliest Agent Version Required	Monitoring Period (Raw Data)
net_tcp_time_wait	(Agent) TCP TIME_WAIT Connections	Number of TCP connections in the TIME_WAIT state • Collection method (Linux): Obtain TCP connections in all states from the **/proc/net/tcp** file, and then collect the number of connections in each state. • Collection method (Windows): Obtain the metric value using the **GetTcpTable2** API.	≥ 0	count	N/A	2.4.5	1 minute

Metric	Name	Description	Value Range	Unit	Conversion Rule	Earliest Agent Version Required	Monitoring Period (Raw Data)
net_tcp_close	(Agent) Number of TCP connections in the CLOSE state.	Number of closed TCP connections • Collection method (Linux): Obtain TCP connections in all states from the **/proc/net/tcp** file, and then collect the number of connections in each state. • Collection method (Windows): Obtain the metric value using the **GetTcpTable2** API.	≥ 0	count	N/A	2.4.5	1 minute

Metric	Name	Description	Value Range	Unit	Conversion Rule	Earliest Agent Version Required	Monitoring Period (Raw Data)
net_tcp_close_wait	(Agent) TCP CLOSE_WAIT Connections	Number of TCP connections in the CLOSE_WAIT state • Collection method (Linux): Obtain TCP connections in all states from the **/proc/net/tcp** file, and then collect the number of connections in each state. • Collection method (Windows): Obtain the metric value using the **GetTcpTable2** API.	≥ 0	count	N/A	2.4.5	1 minute

Metric	Name	Description	Value Range	Unit	Conversion Rule	Earliest Agent Version Required	Monitoring Period (Raw Data)
net_tcp_last_ack	(Agent) Number of TCP connections in the LAST_ACK state.	Number of TCP connections waiting for ACK packets when the connections are being passively closed by the client • Collection method (Linux): Obtain TCP connections in all states from the **/proc/net/tcp** file, and then collect the number of connections in each state. • Collection method (Windows): Obtain the metric value using the **GetTcpTable2** API.	≥ 0	count	N/A	2.4.5	1 minute

Metric	Name	Description	Value Range	Unit	Conversion Rule	Earliest Agent Version Required	Monitoring Period (Raw Data)
net_tcp_listen	(Agent) Number of TCP connections in the LISTEN state.	Number of TCP connections in the LISTEN state • Collection method (Linux): Obtain TCP connections in all states from the **/proc/net/tcp** file, and then collect the number of connections in each state. • Collection method (Windows): Obtain the metric value using the **GetTcpTable2** API.	≥ 0	count	N/A	2.4.5	1 minute

Metric	Name	Description	Value Range	Unit	Conversion Rule	Earliest Agent Version Required	Monitoring Period (Raw Data)
net_tcp_closing	(Agent) Number of TCP connections in the CLOSING state.	Number of TCP connections to be automatically closed by the server and the client at the same time • Collection method (Linux): Obtain TCP connections in all states from the **/proc/net/tcp** file, and then collect the number of connections in each state. • Collection method (Windows): Obtain the metric value using the **GetTcpTable2** API.	≥ 0	count	N/A	2.4.5	1 minute

Metric	Name	Description	Value Range	Unit	Conversion Rule	Earliest Agent Version Required	Monitoring Period (Raw Data)
net_tcp_retrans	(Agent) TCP Retransmission Rate	Percentage of packets that are resent • Collection method (Linux): Obtain the metric value from the **/proc/net/snmp** file. The value is the ratio of the number of sent packets to the number of retransmitted packages in a collection period. • Collection method (Windows): Obtain the metric value using the **GetTcpStatistics** API.	0-100	%	N/A	2.4.5	1 minute

OS Metric: NIC

Metric	Name	Description	Value Range	Unit	Conversion Rule	Earliest Agent Version Required	Monitoring Period (Raw Data)
net_bitRecv	(Agent) Outbound Bandwidth	Number of bits sent by this NIC per second • Collection method (Linux): Check metric value changes in file **/proc/net/dev** in a collection period. • Collection method (Windows): Use the MibIfRow object in WMI to obtain network metric data.	≥ 0	bit/s	1024(IEC)	2.4.1	1 minute
net_bitSent	(Agent) Inbound Bandwidth	Number of bits received by this NIC per second • Collection method (Linux): Check metric value changes in file **/proc/net/dev** in a collection period. • Collection method (Windows): Use the MibIfRow object in WMI to obtain network metric data.	≥ 0	bit/s	1024(IEC)	2.4.1	1 minute

Metric	Name	Description	Value Range	Unit	Conversion Rule	Earliest Agent Version Required	Monitoring Period (Raw Data)
net_packetRecv	(Agent) NIC Packet Receive Rate	Number of packets received by this NIC per second • Collection method (Linux): Check metric value changes in file **/proc/net/dev** in a collection period. • Collection method (Windows): Use the MibIfRow object in WMI to obtain network metric data.	≥ 0	Count/s	N/A	2.4.1	1 minute
net_packetSent	(Agent) NIC Packet Send Rate	Number of packets sent by this NIC per second • Collection method (Linux): Check metric value changes in file **/proc/net/dev** in a collection period. • Collection method (Windows): Use the MibIfRow object in WMI to obtain network metric data.	≥ 0	Count/s	N/A	2.4.1	1 minute

Metric	Name	Description	Value Range	Unit	Conversion Rule	Earliest Agent Version Required	Monitoring Period (Raw Data)
net_errin	(Agent) Receive Error Rate	Percentage of receive errors detected by this NIC per second • Collection method (Linux): Check metric value changes in file **/proc/net/dev** in a collection period. • Collection method (Windows): not supported	0-100	%	N/A	2.4.5	1 minute
net_errout	(Agent) Transmit Error Rate	Percentage of transmit errors detected by this NIC per second • Collection method (Linux): Check metric value changes in file **/proc/net/dev** in a collection period. • Collection method (Windows): not supported	0-100	%	N/A	2.4.5	1 minute

Metric	Name	Description	Value Range	Unit	Conversion Rule	Earliest Agent Version Required	Monitoring Period (Raw Data)
net_dropin	(Agent) Received Packet Drop Rate	Percentage of packets received by this NIC which were dropped per second • Collection method (Linux): Check metric value changes in file **/proc/net/dev** in a collection period. • Collection method (Windows): not supported	0-100	%	N/A	2.4.5	1 minute
net_dropout	(Agent) Transmitted Packet Drop Rate	Percentage of packets transmitted by this NIC which were dropped per second • Collection method (Linux): Check metric value changes in file **/proc/net/dev** in a collection period. • Collection method (Windows): not supported	0-100	%	N/A	2.4.5	1 minute

Process Monitoring Metrics

Metric	Name	Description	Value Range	Unit	Conversion Rule	Earliest Agent Version Required	Monitoring Period (Raw Data)
proc_pHashId_cpu	(Agent) CPU Usage	CPU consumed by a process. **pHashId** (process name and process ID) is the value of **md5**. • Collection method (Linux): Check the metric value changes in file **/proc/pid/stat**. • Collection method (Windows): Call the Windows API GetProcessTimes to obtain the CPU usage of the process.	0–1 x Number of vCPUs	%	N/A	2.4.1	1 minute

Metric	Name	Description	Value Range	Unit	Conversion Rule	Earliest Agent Version Required	Monitoring Period (Raw Data)
proc_pHashId_mem	(Agent) Memory Usage	Memory consumed by a process. **pHashId** (process name and process ID) is the value of **md5**. • Collection method (Linux): RSS*PAGESIZE/ MemTotal Obtain the **RSS** value by checking the second column of file **/proc/pid/statm**. Obtain the **PAGESIZE** value by running the **getconf PAGESIZE** command. Obtain the **MemTotal** value by checking file **/proc/meminfo**. • Collection method (Windows): Call the Windows API **procGlobalMemoryStatusEx** to obtain the total memory size. Call **GetProcessMemoryInfo** to obtain the	0-100	%	N/A	2.4.1	1 minute

Metric	Name	Description	Value Range	Unit	Conversion Rule	Earliest Agent Version Required	Monitoring Period (Raw Data)
		used memory size. Use the used memory size to divide the total memory size to get the memory usage.					
proc_pHashId_file	(Agent) Number of opened files	Number of files opened by a process. **pHashId** (process name and process ID) is the value of **md5**. • Collection method (Linux): Run the **ls -l /proc/pid/fd** command to view the number of opened files. • Collection method (Windows): not supported	≥ 0	Count	N/A	2.4.1	1 minute

Metric	Name	Description	Value Range	Unit	Conversion Rule	Earliest Agent Version Required	Monitoring Period (Raw Data)
proc_running_count	(Agent) Running processes	Number of processes that are running • Collection method (Linux): You can obtain the state of each process by checking the **Status** value in the **/proc/pid/status** file, and then collect the total number of processes in each state. • Collection method (Windows): not supported	≥ 0	None	N/A	2.4.1	1 minute

Metric	Name	Description	Value Range	Unit	Conversion Rule	Earliest Agent Version Required	Monitoring Period (Raw Data)
proc_idle_count	(Agent) Idle Processes	Number of processes that are idle • Collection method (Linux): You can obtain the state of each process by checking the **Status** value in the **/proc/pid/status** file, and then collect the total number of processes in each state. • Collection method (Windows): not supported	≥ 0	None	N/A	2.4.1	1 minute

Metric	Name	Description	Value Range	Unit	Conversion Rule	Earliest Agent Version Required	Monitoring Period (Raw Data)
proc_zombie_count	(Agent) Zombie Processes	Number of zombie processes • Collection method (Linux): You can obtain the state of each process by checking the **Status** value in the **/proc/pid/status** file, and then collect the total number of processes in each state. • Collection method (Windows): not supported	≥ 0	None	N/A	2.4.1	1 minute

Metric	Name	Description	Value Range	Unit	Conversion Rule	Earliest Agent Version Required	Monitoring Period (Raw Data)
proc_blocked_count	(Agent) Blocked Processes	Number of processes that are blocked • Collection method (Linux): You can obtain the state of each process by checking the **Status** value in the **/proc/pid/status** file, and then collect the total number of processes in each state. • Collection method (Windows): not supported	≥ 0	None	N/A	2.4.1	1 minute

Metric	Name	Description	Value Range	Unit	Conversion Rule	Earliest Agent Version Required	Monitoring Period (Raw Data)
proc_sleeping_count	(Agent) Sleeping Processes	Number of processes that are sleeping • Collection method (Linux): You can obtain the state of each process by checking the **Status** value in the **/proc/pid/status** file, and then collect the total number of processes in each state. • Collection method (Windows): not supported	≥ 0	None	N/A	2.4.1	1 minute

Metric	Name	Description	Value Range	Unit	Conversion Rule	Earliest Agent Version Required	Monitoring Period (Raw Data)
proc_total_count	(Agent) Total Processes	Total number of processes on the monitored object • Collection method (Linux): You can obtain the state of each process by checking the **Status** value in the **/proc/pid/status** file, and then collect the total number of processes in each state. • Collection method (Windows): Obtain the total number of processes by using the system process status support module **psapi.dll**.	≥ 0	None	N/A	2.4.1	1 minute

Metric	Name	Description	Value Range	Unit	Conversion Rule	Earliest Agent Version Required	Monitoring Period (Raw Data)
proc_specified_count	(Agent) Specified Processes	Number of specified processes • Collection method (Linux): You can obtain the state of each process by checking the **Status** value in the **/proc/pid/status** file, and then collect the total number of processes in each state. • Collection method (Windows): Obtain the total number of processes by using the system process status support module **psapi.dll**.	≥ 0	None	N/A	2.4.1	1 minute

GPU Specifications

NOTE

If a GPU server has eight GPU cards and the PM mode is disabled, data may fail to be collected. You can enable the PM mode and restart the monitoring process.

Category	Metric Name	Description	Value Range	Unit	Conversion Rule	Earliest Agent Version Required	Collection Interval
GPU Specifications	gpu_status	GPU health status of the VM. This metric is a composite metric. • Possible causes: 1. The ECC exceeded the threshold. 2. The GPU memory address failed to be remapped. 3. The GPU card is in the **rev ff** state. 4. infoROM error. 5. There are pages to be isolated. 6. The remapped rows are incorrect. (For details, see the following detailed metrics.) • Collection method (Linux): Call APIs from the GPU driver library file **libnvidia-ml.so.1** to obtain the GPU status. • Collection method (Windows): Call APIs from the GPU driver library file **nvml.dll** to obtain the GPU status.	• **0**: healthy • **1**: subhealthy • **2**: faulty	None	N/A	2.4.5	1 minute

Category	Metric Name	Description	Value Range	Unit	Conversion Rule	Earliest Agent Version Required	Collection Interval
	gpu_performance_state	Performance status of the GPU • P0-P15, P32 • **P0** indicates the maximum performance status. **P15** indicates the minimum performance status. **P32** indicates the unknown status. • Collection mode (Linux): Call the **NvmlDeviceGetPerformanceState** API from the GPU driver library file **libnvidia-ml.so.1** to obtain the GPU performance level. • Collection method (Windows): Call the **NvmlDeviceGetPerformanceState** API from the GPU driver library file **nvml.dll** to obtain the GPU performance level.	• P0-P15: **P0** indicates the maximum performance status, and **P15** indicates the minimum performance status. • **P32** indicates the unknown status.	None	N/A	2.4.1	1 minute

Category	Metric Name	Description	Value Range	Unit	Conversion Rule	Earliest Agent Version Required	Collection Interval
	gpu_power_draw	Power of the GPU. • If the power exceeds the maximum power or is an incorrect value, the GPU hardware may be faulty. • Collection method (Linux): Call the **NvmlDeviceGetPowerUsage** API from the GPU driver library file **libnvidia-ml.so.1** to obtain the GPU power. • Collection method (Windows): Call the **NvmlDeviceGetPowerUsage** API from the GPU driver library file **nvml.dll** to obtain the GPU power.	≥ 0	W	N/A	2.4.5	1 minute

Category	Metric Name	Description	Value Range	Unit	Conversion Rule	Earliest Agent Version Required	Collection Interval
	gpu_temperature	Temperature of the GPU. • If the temperature exceeds the maximum operating temperature threshold or is an incorrect value, the GPU hardware may be faulty. • Collection method (Linux): Call the **NvmlDeviceGetTemperature** API from the GPU driver library file **libnvidia-ml.so.1** to obtain the GPU temperature. • Collection method (Windows): Call the **NvmlDeviceGetTemperature** API from the GPU driver library file **nvml.dll** to obtain the GPU temperature.	≥ 0	°C	N/A	2.4.5	1 minute

Category	Metric Name	Description	Value Range	Unit	Conversion Rule	Earliest Agent Version Required	Collection Interval
	gpu_usage_gpu	GPU computing power usage. • The GPU computing power usage is displayed in percentage. The value is an instantaneous value at the sampling point. • Collection method (Linux): Call the **NvmlDeviceGetUtilizationRates** API from the GPU driver library file **libnvidia-ml.so.1** to obtain the GPU computing power usage. • Collection method (Windows): Call the **NvmlDeviceGetUtilizationRates** API from **nvml.dll** to obtain the GPU computing power usage.	0-100	%	N/A	2.4.1	1 minute

Category	Metric Name	Description	Value Range	Unit	Conversion Rule	Earliest Agent Version Required	Collection Interval
	gpu_usage_mem	GPU memory usage. • The GPU memory usage is displayed in percentage. The value is an instantaneous value at the sampling point. • Collection method (Linux): Call the **NvmlDeviceGetUtilizationRates** API from the GPU driver library file **libnvidia-ml.so.1** to obtain the GPU memory usage. • Collection method (Windows): Call the **NvmlDeviceGetUtilizationRates** API from **nvml.dll** to obtain the GPU memory usage.	0-100	%	N/A	2.4.1	1 minute

Category	Metric Name	Description	Value Range	Unit	Conversion Rule	Earliest Agent Version Required	Collection Interval
	gpu_used_mem	Used GPU memory. • The used GPU memory is displayed in percentage. The value is an instantaneous value at the sampling point. • Collection method (Linux): Call the **NvmlDeviceGetMemoryInfo** API from the GPU driver library file **libnvidia-ml.so.1** to obtain the used GPU memory. • Collection method (Windows): Call the **NvmlDeviceGetMemoryInfo** API from the GPU driver library file **nvml.dll** to obtain the used GPU memory.	≥ 0	MB	N/A	2.4.5	1 minute

Category	Metric Name	Description	Value Range	Unit	Conversion Rule	Earliest Agent Version Required	Collection Interval
	gpu_free_mem	Remaining GPU memory. • The idle GPU memory data is displayed. • Collection method (Linux): Call the **NvmlDeviceGetMemoryInfo** API from the GPU driver library file **libnvidia-ml.so.1** to obtain the remaining GPU memory. • Collection method (Windows): Call the **NvmlDeviceGetMemoryInfo** API from **nvml.dll** to obtain the remaining GPU memory.	≥ 0	MB	N/A	2.4.5	1 minute

Category	Metric Name	Description	Value Range	Unit	Conversion Rule	Earliest Agent Version Required	Collection Interval
	gpu_usage_encoder	GPU encoder usage. • The GPU encoder usage is displayed in percentage. The value is an instantaneous value at the sampling point. • Collection method (Linux): Call the **NvmlDeviceGetEncoderUtilization** API from the GPU driver library file **libnvidia-ml.so.1** to obtain the GPU encoding capability usage. • Collection method (Windows): Call the **NvmlDeviceGetEncoderUtilization** API from **nvml.dll** to obtain the GPU encoding capability usage.	0-100	%	N/A	2.4.5	1 minute

Category	Metric Name	Description	Value Range	Unit	Conversion Rule	Earliest Agent Version Required	Collection Interval
	gpu_usage_decoder	GPU decoder usage. • The GPU decoder usage is displayed in percentage. The value is an instantaneous value at the sampling point. • Collection method (Linux): Call the **NvmlDeviceGetDecoderUtilization** API from the GPU driver library file **libnvidia-ml.so.1** to obtain the GPU decoding capability usage. • Collection method (Windows): Call the **NvmlDeviceGetDecoderUtilization** API from **nvml.dll** to obtain the GPU decoding capability usage.	0-100	%	N/A	2.4.5	1 minute

Category	Metric Name	Description	Value Range	Unit	Conversion Rule	Earliest Agent Version Required	Collection Interval
	gpu_graphics_clocks	GPU graphics (shader) clock frequency. • Displays the GPU clock frequencies related to graphics performance. If no graphics capability is used, you can ignore it. • Collection method (Linux): Call the **NvmlDeviceGetClockInfo** API from the GPU driver library file **libnvidia-ml.so.1** to obtain the GPU graphics clock frequency. • Collection method (Windows): Call the **NvmlDeviceGetClockInfo** API from the GPU driver library file **nvml.dll** to obtain the GPU graphics clock frequency.	≥ 0	MHz	N/A	2.4.5	1 minute

Category	Metric Name	Description	Value Range	Unit	Conversion Rule	Earliest Agent Version Required	Collection Interval
	gpu_sm_clocks	Streaming processor clock frequency of the GPU. • Clock frequency for controlling the GPU memory running speed. • Collection method (Linux): Call the **NvmlDeviceGetClockInfo** API from the GPU driver library file **libnvidia-ml.so.1** to obtain the streaming processor clock frequency of the GPU. • Collection method (Windows): Call the **NvmlDeviceGetClockInfo** API from the GPU driver library file **nvml.dll** to obtain the streaming processor clock frequency of the GPU.	≥ 0	MHz	N/A	2.4.5	1 minute

Category	Metric Name	Description	Value Range	Unit	Conversion Rule	Earliest Agent Version Required	Collection Interval
	gpu_mem_clocks	Memory clock frequency of the GPU. • Displays the clock frequency closely related to CUDA core computing of the GPU. • Collection method (Linux): Call the **NvmlDeviceGetClockInfo** API from the GPU driver library file **libnvidia-ml.so.1** to obtain the GPU memory clock frequency. • Collection method (Windows): Call the **NvmlDeviceGetClockInfo** API from the GPU driver library file **nvml.dll** to obtain the GPU memory clock frequency.	≥ 0	MHz	N/A	2.4.5	1 minute

Category	Metric Name	Description	Value Range	Unit	Conversion Rule	Earliest Agent Version Required	Collection Interval
	gpu_video_clocks	Video (including codec) clock frequency of the GPU. • Displays the codec clock frequency of the current GPU. • Collection method (Linux): Call the **NvmlDeviceGetClockInfo** API from the GPU driver library file **libnvidia-ml.so.1** to obtain the video clock frequency of the GPU. • Collection method (Windows): Call the **NvmlDeviceGetClockInfo** API from the GPU driver library file **nvml.dll** to obtain the GPU video clock frequency.	≥ 0	MHz	N/A	2.4.5	1 minute

Category	Metric Name	Description	Value Range	Unit	Conversion Rule	Earliest Agent Version Required	Collection Interval
	gpu_tx_throughput_pci	Outbound bandwidth of the GPU. • Displays the amount of data sent by the GPU to the host via PCIe. • Collection method (Linux): Call the **NvmlDeviceGetPcieThroughput** API from **libnvidia-ml.so.1** to obtain the outbound bandwidth of the GPU. • Collection method (Windows): Call the **NvmlDeviceGetPcieThroughput** API from **nvml.dll** to obtain the outbound bandwidth of the GPU.	≥ 0	Mbyte/s	N/A	2.4.5	1 minute

Category	Metric Name	Description	Value Range	Unit	Conversion Rule	Earliest Agent Version Required	Collection Interval
	gpu_rx_throughput_pci	Inbound bandwidth of the GPU. • Displays the amount of data sent by the host to the GPU via PCIe. • Collection method (Linux): Call the **NvmlDeviceGetPcieThroughput** API from **libnvidia-ml.so.1** to obtain the inbound bandwidth of the GPU. • Collection method (Windows): Call the **NvmlDeviceGetPcieThroughput** API from **nvml.dll** to obtain the inbound bandwidth of the GPU.	≥ 0	Mbyte/s	N/A	2.4.5	1 minute

Category	Metric Name	Description	Value Range	Unit	Conversion Rule	Earliest Agent Version Required	Collection Interval
	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. • Collection method (Linux): Call the **NvmlDeviceGetPcieThroughput** API from the GPU driver library file **libnvidia-ml.so.1** to obtain the number of correctable ECC errors since the GPU is reset. • Collection method (Windows): Call the **NvmlDeviceGetPcieThroughput** API from the GPU driver library file **nvml.dll** to obtain the number of correctable ECC errors since the GPU is reset.	≥ 0	count	N/A	2.4.5	1 minute

Category	Metric Name	Description	Value Range	Unit	Conversion Rule	Earliest Agent Version Required	Collection Interval
	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. • Collection method (Linux): Call the **NvmlDeviceGetTotalEccErrors** and **NvmlDeviceGetMemoryErrorCounter** APIs from the GPU driver library file **libnvidia-ml.so.1** to obtain the number of uncorrectable ECC errors since the GPU is reset. • Collection method (Windows): Call the **NvmlDeviceGetTotalEccErrors** and **NvmlDeviceGetMemoryErrorCounter** APIs from the GPU driver library file **nvml.dll** to obtain the number of uncorrectable ECC errors since the GPU is reset.	≥ 0	count	N/A	2.4.5	1 minute

Category	Metric Name	Description	Value Range	Unit	Conversion Rule	Earliest Agent Version Required	Collection Interval
	gpu_aggregate_correctable	Number of correctable ECC errors on the GPU. • Collection method (Linux): Call the **NvmlDeviceGetTotalEccErrors** and **NvmlDeviceGetMemoryErrorCounter** APIs from the GPU driver library file **libnvidia-ml.so.1** to obtain the number of correctable ECC errors on the GPU. • Collection method (Windows): Call the **NvmlDeviceGetTotalEccErrors** and **NvmlDeviceGetMemoryErrorCounter** APIs from the GPU driver library file **nvml.dll** to obtain the number of correctable ECC errors on the GPU.	≥ 0	count	N/A	2.4.5	1 minute

Category	Metric Name	Description	Value Range	Unit	Conversion Rule	Earliest Agent Version Required	Collection Interval
	gpu_aggregate_uncorrectable	Number of uncorrectable ECC errors on the GPU. • Collection method (Linux): Call the **NvmlDeviceGetTotalEccErrors** and **NvmlDeviceGetMemoryErrorCounter** APIs from the GPU driver library file **libnvidia-ml.so.1** to obtain the number of uncorrectable ECC errors on the GPU. • Collection method (Windows): Call the **NvmlDeviceGetTotalEccErrors** and **NvmlDeviceGetMemoryErrorCounter** APIs from the GPU driver library file **nvml.dll** to obtain the number of uncorrectable ECC errors on the GPU.	≥ 0	count	N/A	2.4.5	1 minute

Category	Metric Name	Description	Value Range	Unit	Conversion Rule	Earliest Agent Version Required	Collection Interval
	gpu_retired_page_single_bit	Number of retired page single bit errors, which indicates the number of single-bit pages isolated by the GPU. • Collection method (Linux): Call the **NvmlDeviceGetRetiredPages** API from the GPU driver library file **libnvidia-ml.so.1** to obtain the number of single-bit pages isolated by the GPU. • Collection method (Windows): Call the **NvmlDeviceGetRetiredPages** API from the GPU driver library file **nvml.dll** to obtain the number of single-bit pages isolated by the GPU.	≥ 0	count	N/A	2.4.5	1 minute

Category	Metric Name	Description	Value Range	Unit	Conversion Rule	Earliest Agent Version Required	Collection Interval
	gpu_retired_page_double_bit	Number of retired page double bit errors, which indicates the number of double-bit pages isolated by the GPU. • Collection method (Linux): Call the **NvmlDeviceGetRetiredPages** API from the GPU driver library file **libnvidia-ml.so.1** to obtain the number of double-bit pages isolated by the GPU. • Collection method (Windows): Call the **NvmlDeviceGetRetiredPages** API from the GPU driver library file **nvml.dll** to obtain the number of double-bit pages isolated by the GPU.	≥ 0	count	N/A	2.4.5	1 minute

Category	Metric Name	Description	Value Range	Unit	Conversion Rule	Earliest Agent Version Required	Collection Interval
	gpu_lnkcap_speed	Maximum speed supported by the PCIe link of the GPU. ● Maximum data throughput capability of the GPU on the PCIe bus. ● Collection method (Linux): Use **lspci -d 10de: -vv | grep -i lnkcap** to query the maximum speed supported by the PCIe link of the GPU. ● Collection method (Windows): Use **gwmi Win32_Bus -Filter 'DeviceID like "PCI %"').GetRelated('Win32_PnPEntity')** to query the maximum speed supported by the PCIe link of the GPU.	≥ 0	GT/s	N/A	2.6.7	1 minute

Category	Metric Name	Description	Value Range	Unit	Conversion Rule	Earliest Agent Version Required	Collection Interval
	gpu_lnkcap_width	Link width of the PCIe link. • Maximum number of PCIe lanes supported by the GPU. • Collection method (Linux): Use **lspci -d 10de: -vv | grep -i lnksta** to query the maximum speed supported by the PCIe link of the GPU. • Collection method (Windows): Use **gwmi Win32_Bus -Filter 'DeviceID like "PCI %"').GetRelated('Win32_PnPEntity')** to query the maximum speed supported by the PCIe link of the GPU.	≥ 0	count	N/A	2.6.7	1 minute

Category	Metric Name	Description	Value Range	Unit	Conversion Rule	Earliest Agent Version Required	Collection Interval
	gpu_lnksta_speed	PCIe connection speed of the GPU. • Maximum PCIe link speed supported by the GPU. • Collection method (Linux): Use **lspci -d 10de: -vv | grep -i lnkcap** to query the PCIe connection speed of the GPU. • Collection method (Windows): not supported	≥ 0	GT/s	N/A	2.6.7	1 minute
	gpu_lnksta_width	PCIe link width of the GPU. • Maximum number of lanes in the PCIe link supported by the GPU. • Collection method (Linux): Use **lspci -d 10de: -vv | grep -i lnksta** to query the PCIe link bandwidth of the GPU. • Collection method (Windows): not supported	≥ 0	count	N/A	2.6.7	1 minute

Category	Metric Name	Description	Value Range	Unit	Conversion Rule	Earliest Agent Version Required	Collection Interval
	gpu_nvlink_number	Number of NVLink links of the GPU. • Number of NVLink links supported by the GPU. For example, A100 supports 12 NVLink links. • Collection method (Linux): Call the **nvmlDeviceGetFieldValue** API from the GPU driver library file **libnvidia-ml.so.1** to obtain the number of NVLink links of the GPU. • Collection method (Windows): not supported	≥ 0	count	N/A	2.6.7	1 minute

Category	Metric Name	Description	Value Range	Unit	Conversion Rule	Earliest Agent Version Required	Collection Interval
	gpu_nvlink_bandwidth	NVLink link width of the GPU. • Indicates the total bandwidth for data transmission used by the GPU. • Collection method (Linux): Call the **nvmlDeviceGetFieldValue** API from the GPU driver library file **libnvidia-ml.so.1** to obtain the NVLink link width of the GPU. • Collection method (Windows): not supported	≥ 0	GB/s	N/A	2.6.7	1 minute

1.1.9 Environment Constraints for GPU Monitoring

1. Only Linux OSs are supported, and only some Linux public image versions support GPU monitoring. For details, see **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. You have installed the Agent of the enhanced edition. For details, see **Installing the Agent**. **Table 1-2** describes the differences between Agents of the basic edition and enhanced edition.

Table 1-2 Basic edition and enhanced edition of Cloud Eye Agent

Edition	Description
Basic edition	Provides basic OS monitoring metrics, such as CPU, memory, disk, and NIC metrics, helping you improve system performance. Generally, the version number consists of three digits, for example, 2.7.5.
Enhanced edition	Provides GPU, NPU, and BMS hardware monitoring, in addition to the capabilities provided in the basic edition. Generally, the version number consists of four digits, for example, 2.7.5.1. **CAUTION** Install the Agent of the enhanced edition if you indeed need it because it collects more metrics, which may occupy more server resources.

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"
   ```

1.1.10 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 **dmidecode** command
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 **smartctl -a** *<Drive letter>* command

Metrics	Description	Collected by
Basic information about the Non-Volatile Memory Express (NVMe) SSD	Includes SN, model, capacity, and firmware version.	Running the **nvme list** 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 **nvme smart-log** *<NVMe device name>* 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 **hioadm info -d** *<NVMe device name>* **-a** and **hioadm info -d** *<NVMe device name>* **-e** commands
Additional SMART information of Intel NVMe SSDs	Includes more detailed error counts.	Run the **nvme intel smart-log-add** *<NVMe device name>* command
Network interface status information	Includes the MAC address, link status, and lost & wrong packets at the receiving and sending ends.	Running the **ifconfig** *<Network interface name>* command
Network port device information	Includes the port type, link status, and network rate.	Running the **ethtool** *<Network interface name>* command
Network interface driver information	Includes the firmware version, driver version, and bus number.	Running the **ethtool -i** *<Network interface name>* command
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 **ethtool -m** *<Network interface name>* command
Number of Huawei Intelligent NIC (HiNIC) port errors	HiLink errors, Base encoding errors, and RS encoding errors	Running the **hinicadm hilink_port -i** *<dev_id>* **-p** *<port_id>* **-s** and **hinicadm hilink_count -i** *<dev_id>* **-p** *<port_id>* commands

Metrics	Description	Collected by
HiNIC card working mode	Current working mode and configured working mode	Running the **hinicadm mode -i** *<dev_id>* command
HiNIC card core temperature	Temperature of the HiNIC card core	Running the **hinicadm temperature -i** *<dev_id>* command
HiNIC card event records	Includes HiNIC card heartbeat losses, PCIe exceptions, chip errors, and chip health status.	Running the **hinicadm event -i** *<dev_id>* command
PCIe errors of the HiNIC card	Different PCIe errors of the HiNIC card	Running the **hinicadm counter -i** *<dev_id>* **-t 4** command
Memory information	Includes the DIMM SN, manufacturer, Part Number (PN), bit width, capacity, and frequency.	Running the **dmidecode -t 17** command
CPU information	Includes the CPU ID, name, frequency, architecture, and model.	Running the **dmidecode -t 4** and **lscpu** 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 **/dev/mem**, **/dev/cpu/***<core_id>***/msr**, and **/sys/firmware/acpi/tables/HEST** to collect memory error records and chip register information

1.1.11 How Can I Quickly Restore Agent Configurations?

After the Agent is installed, you can configure the AK/SK, region ID, or project ID with a few clicks. This improves configuration efficiency.

- One-click configuration restoration is available in most regions. 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 permissions, see **2.1.3 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**.

1.1.12 How Can I Enable 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.

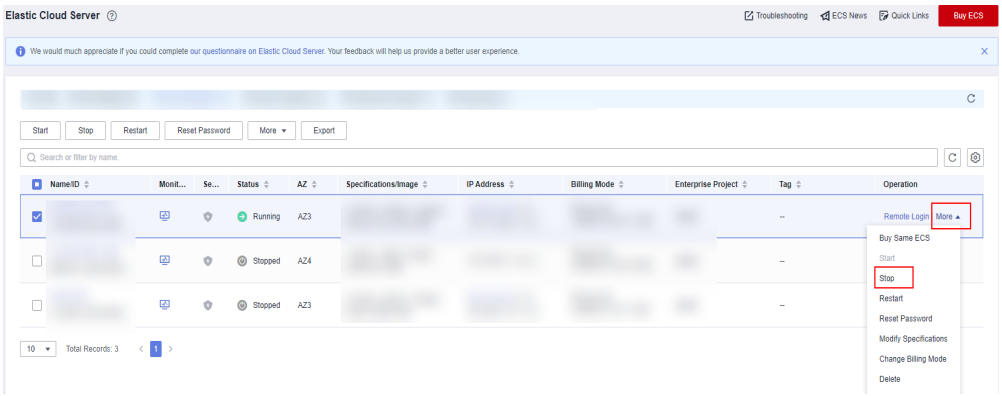
Prerequisites

An ECS with the Agent installed is available.

Procedure

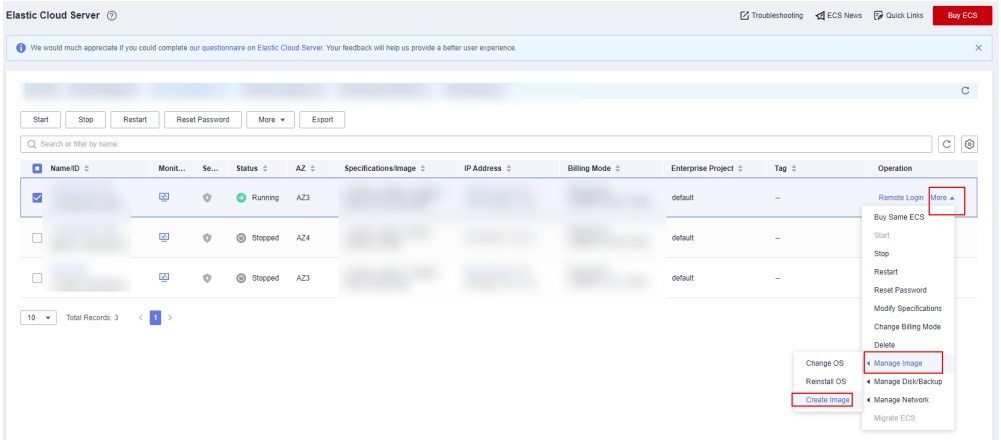
1. Log in to the ECS console. In the ECS list, locate a target ECS with the Agent installed, choose **More** > **Stop** in the **Operation** column, and click **OK**.

Figure 1-2 Stopping an ECS



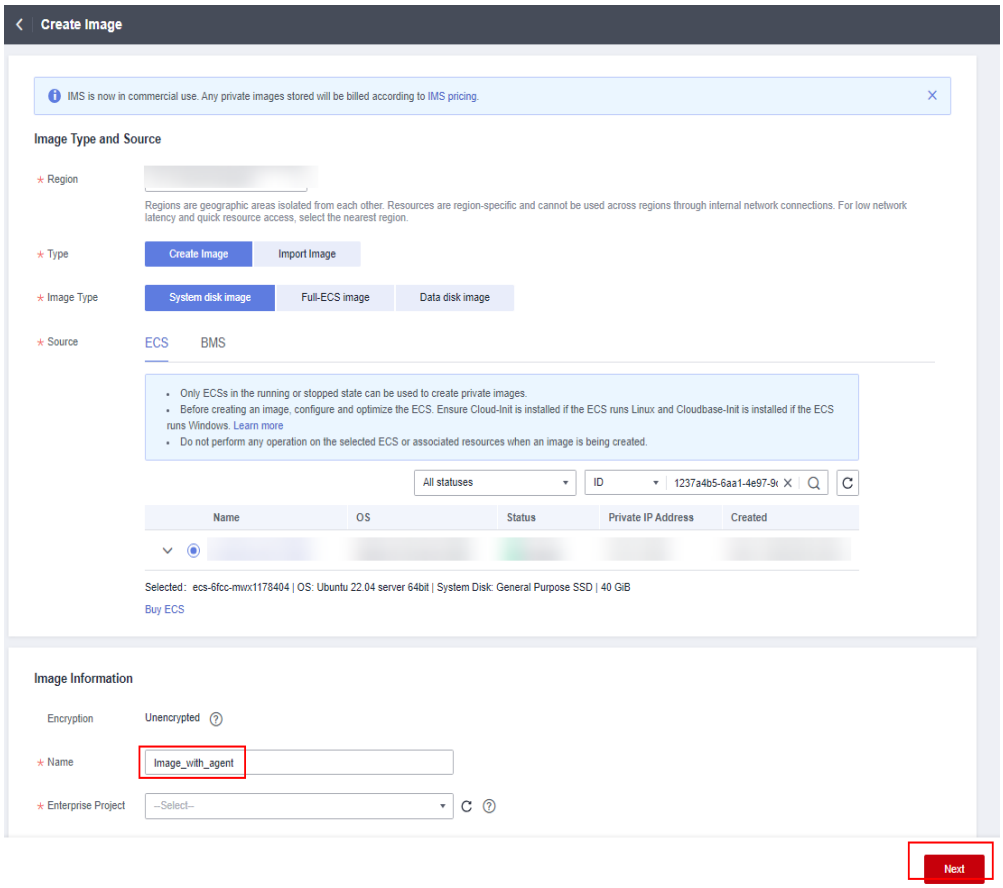
2. Choose **More** > **Manage Image/Disk** > **Create Image**.

Figure 1-3 Creating an image



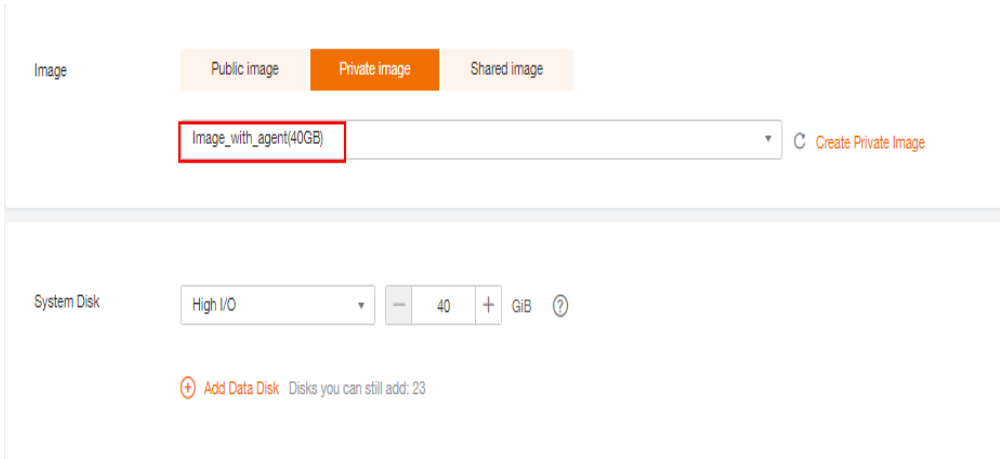
3. Set the private image name to **Image_with_agent** and click **Next**.

Figure 1-4 Image_with_agent



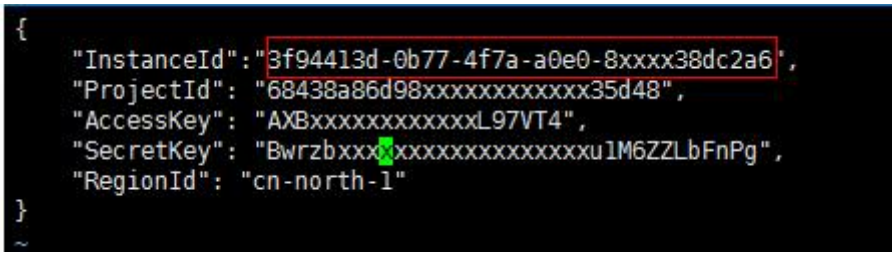
4. Purchase a new ECS and select the newly created private image **Image_with_agent (40GB)**.

Figure 1-5 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 1-6 Modifying the Agent configuration file



1.1.13 What Are Agent Statuses 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 **1.1.2 How Do I Configure an Agency?**
  - If the Agent has been installed, but the network configuration is abnormal, rectify the fault by referring to **Modifying the DNS Server Address and Adding Security Group Rules (Linux)** or **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 failed to send a heartbeat message to Cloud Eye for three consecutive minutes. In this case:
  - 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)** or **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 fault persists after the restart, the Agent files may be damaged. In this case, reinstall the Agent. For details, see **Installing and Configuring the Agent**.
  - The server time is inconsistent with the local standard time.
  - Upgrade the Agent to the latest version.

1.1.14 Why Is Basic Monitoring Data Inconsistent with OS Monitoring Data?

Symptoms

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

Possible Causes

1. Setting **idle** to **poll** in the guest operating system (guest OS) causes it to enter the **polling** state while idling. This results in the guest OS consuming compute resources and not proactively releasing CPU resources, leading to abnormal CPU usage.
2. If you set **idle** to **mwait** in the guest OS for an SAP HANA ECS, the guest OS will enter the **mwait** state when idling. This results in the guest OS using fewer compute resources than it does when **idle** is set to **poll**. However, it still does not release CPU resources proactively, leading to abnormal CPU usage.

   NOTE

   - You can run the **cat /proc/cmdline** command to check whether **idle** is set to **poll** for your guest OS.
   - If you want to check whether **idle** is set to **mwait** for your guest OS, contact technical support.
   - SAP High-Performance Analytic Appliance (HANA) is a high-performance real-time data computing platform based on memory computing technologies. The cloud platform offers high-performance IaaS services that meet SAP HANA requirements. These services help you rapidly request for SAP HANA resources (such as applying for HANA ECSs and public IP addresses) and install and configure SAP HANA. This improves operation efficiency, reduces costs, and enhances your experience.

     HANA ECSs are dedicated for SAP HANA. If you have deployed SAP HANA on cloud servers, you can purchase HANA ECSs.

Solution

Install and configure the Agent to view OS monitoring data.

1.1.15 Why Are the Network Traffic Values on Cloud Eye Different from Those 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 data is collected in ECS 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.

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

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

If UVP VMTools is 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 lowers the CPU monitoring accuracy.

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

1.1.17 Why Are Memory Usage, Disk Usage, Inband Incoming Rate, and Inband Outgoing Rate Not Displayed for an ECS?

Linux ECSs do not support the four metrics, but Windows ECSscan.

To learn more about basic 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**.

1.1.18 What Should I Do If There Are No GPU Monitoring Records?

If no GPU monitoring records are displayed on the OS monitoring page when you view server monitoring metrics, check whether your server supports GPUs. If your server supports GPUs and the driver is running properly, perform the following steps to upgrade the Agent to the enhanced edition:

Step 1 Uninstall the Agent of the basic edition.

- Linux: Log in to a server and run the **bash /usr/local/uniagent/script/uninstall.sh** command.
- Windows: In the **C:\Program Files\uniagent\script** directory where the Agent installation package is stored, double-click the **uninstall.bat** script.

Step 2 Install the Agent of the enhanced edition: Add **.1** to the **-t** value in the installation command. For example, change **-t a.b.c** to **-t a.b.c.1**.

----End

Table 1-3 Basic edition and enhanced edition of Cloud Eye Agent

Edition	Description
Basic edition	Provides basic OS monitoring metrics, such as CPU, memory, disk, and NIC metrics, helping you improve system performance. Generally, the version number consists of three digits, for example, 2.7.5.

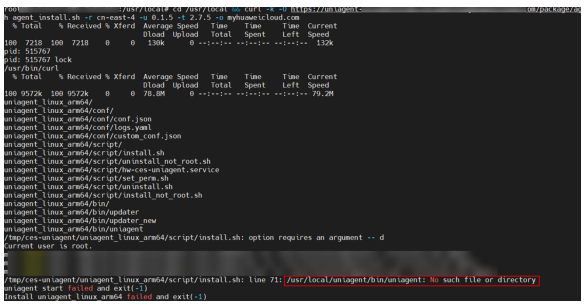
Edition	Description
Enhanced edition	Provides GPU, NPU, and BMS hardware monitoring, in addition to the capabilities provided in the basic edition. Generally, the version number consists of four digits, for example, 2.7.5.1. **CAUTION** Install the Agent of the enhanced edition if you indeed need it because it collects more metrics, which may occupy more server resources.

1.1.19 What Should I Do If an Error Is Reported When I Run the Agent Installation Command?

Symptom

When you run the Cloud Eye Agent installation command, the error message "/usr/local/uniagent/bin/uniagent: No such file or directory" is displayed. The installation fails, as shown in **Figure 1-7**.

Figure 1-7 Agent installation failed



Possible Causes

The earlier version of Cloud Eye Agent is incompatible with some Arm images.

Solution

Step 1 Uninstall the Agent.

```
bash /usr/local/uniagent/script/uninstall.sh
```

Step 2 Modify the **-u** and **-t** parameters in the Agent installation command. Change the value of **-u** to **0.2.1** and that of **-t** to **2.7.5**.

For CN East 2:

Command before modification

```
cd /usr/local && curl -k -O https://uniagent-cn-east-4.obs.cn-east-4.myhuaweicloud.com/package/agent_install.sh && bash agent_install.sh -r cn-east-4 -u 0.1.5 -t 2.5.6 -o myhuaweicloud.com
```

Command after modification


```
cd /usr/local && curl -k -O https://uniagent-cn-east-4.obs.cn-east-4.myhuaweicloud.com/package/agent_install.sh && bash agent_install.sh -r cn-east-4 -u 0.2.1 -t 2.7.5 -o myhuaweicloud.com
```

----End

1.1.20 How Do I Enable or Disable Metric Collection by Modifying the Configuration File?

This following describes how to enable or disable metric collection by modifying the configuration file.

Modifying the Configuration File to Enable Metric Collection

1. Log in to a server as the root user (Linux) or as an administrator (Windows).
2. Modify the **custom_conf.json** file.
   a. Go to the configuration file directory.

      Windows:
      ```
      cd C:\Program Files\uniagent\extension\install\telescope\conf
      ```

      Linux:
      ```
      cd /usr/local/uniagent/extension/install/telescope/conf
      ```

   b. Open the **custom_conf.json** file.
      ```
      vi custom_conf.json
      ```

   c. Enter the following configuration content in {}. Replace **metric_name1** and **metric_name2** with the metric values in **OS Monitoring Metrics Supported by ECSs with the Agent Installed**.
      ```
      "telescope.metric.metric_name1.enable": "true",
      "telescope.metric.metric_name2.enable": "true"
      ```

      Example: **Figure 1-8** shows the configuration content for enabling metric collection for cpu_usage and cpu_usage_idle.

      Figure 1-8 Enabling metric collection for cpu_usage and cpu_usage_idle

      ```
      [root@ec          conf]# pwd
      /usr/local/uniagent/extension/install/telescope/conf
      [root             conf]# cat custom_conf.json
      {
              "telescope.metric.cpu_usage.enable": "true",
              "telescope.metric.cpu_usage_idle.enable": "true"
      }
      ```

3. Restart the Agent.
   - Windows:
     i. In the **C:\Program Files\uniagent\extension\install\telescope** directory, double-click **shutdown.bat** to stop the Agent, and then run **start.bat** to start the Agent.
     ii. In the **C:\Program Files\uniagent\script** directory, double-click **shutdown.bat** to stop the Agent, and then run **start.bat** to start the Agent.
   - Linux:
     ```
     service ces-uniagent stop
     service ces-uniagent start
     /usr/local/uniagent/extension/install/telescope/telescoped restart
     ```


Modifying the Configuration File to Disable Metric Collection

1. Log in to the server as the root user (Linux) or as an administrator (Windows).
2. Modify the **custom_conf.json** file.
   a. Go to the configuration file directory.

      Windows:
      ```
      cd C:\Program Files\uniagent\extension\install\telescope\conf
      ```

      Linux:
      ```
      cd /usr/local/uniagent/extension/install/telescope/conf
      ```

   b. Open the **custom_conf.json** file.
      ```
      vi custom_conf.json
      ```

   c. Enter the following configuration content in {}. Replace **metric_name1** and **metric_name2** with the metric values in **OS Monitoring Metrics Supported by ECSs with the Agent Installed**.
      ```
      "telescope.metric.metric_name1.enable": "false",
      "telescope.metric.metric_name2.enable": "false"
      ```

      Example: **Figure 1-9** shows the configuration content for disabling metric collection for cpu_usage and cpu_usage_idle.

      Figure 1-9 Disabling metric collection for cpu_usage and cpu_usage_idle

      ```
      [root@e                r conf]# pwd
      /usr/local/uniagent/extension/install/telescope/conf
      [root@e                conf]# cat custom_conf.json
      {
              "telescope.metric.cpu_usage.enable": "false",
              "telescope.metric.cpu_usage_idle.enable": "false"
      }
      ```

3. Restart the Agent.
   - Windows:
     i. In the **C:\Program Files\uniagent\extension\install\telescope** directory, double-click **shutdown.bat** to stop the Agent, and then run **start.bat** to start the Agent.
     ii. In the **C:\Program Files\uniagent\script** directory, double-click **shutdown.bat** to stop the Agent, and then run **start.bat** to start the Agent.
   - Linux:
     ```
     service ces-uniagent stop
     service ces-uniagent start
     /usr/local/uniagent/extension/install/telescope/telescoped restart
     ```

1.1.21 How Do I Change the Agent Resource Usage Threshold by Modifying the Configuration File?

This section describes how to modify the configuration file to change the Agent resource usage threshold.

Procedure

1. Use the **root** account to log in to the ECS or BMS for which the Agent does not report data.
2. Modify the **conf.json** configuration file.

a. Go to the Agent installation path **bin** by running the following command:

Windows:
```
cd C:\Program Files\uniagent\extension\install\telescope\bin
```

Linux:
```
cd /usr/local/uniagent/extension/install/telescope/bin
```

b. Open **conf.json**.
```
vi conf.json
```

c. Add the following parameters to the **conf.json** file.
```
{
   "cpu_first_pct_threshold": xx,
   "memory_first_threshold": xxx,
   "cpu_second_pct_threshold": xx,
   "memory_second_threshold": xxx
}
```

Table 1-4 Parameters in the **conf.json** file

Parameter	Description	How to Query Parameter Values
cpu_first_pct_threshold	Tier-1 threshold of CPU usage. The default value is 10 (%).	To query the CPU usage and memory usage of the Agent process, use either of the following methods: • Linux: **top -p** *telescope PID* • Windows: View the details of the Agent process in **Task Manager**.
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.	

d. Save the **conf.json** file and exit.
```
:wq
```

3. Modify the **manifest.json** configuration file.

a. Switch to the **manifest.json** file directory.

Windows:
```
cd C:\Program Files\uniagent\extension\holder\telescope
```

Linux:
```
cd /usr/local/uniagent/extension/holder/telescope
```

b. Open **manifest.json**.
```
vi manifest.json
```

c. Modify the parameters **mem** and **cpuUsage** in **resourceLimit**, three parameter sets in total. Retain the default values of other parameters.
```
[
   {
```



```
        "arch": "amd64",
        ...
        "resourceLimit": {
            "mem": 200,
            "cpuUsage": 10
        }
    },
    {
        "arch": "arm64",
        ...
        "resourceLimit": {
            "mem": 200,
            "cpuUsage": 10
        }
    },
    {
        "arch": "amd64",
        "os": "linux",
        ...
        "resourceLimit": {
            "mem": 200,
            "cpuUsage": 10
        }
    }
]
```

Table 1-5 Parameters in the **manifest.json** file

Parameter	Description

"resourceLimit": {
"mem": 200,
"cpuUsage": 10
}
	mem: memory threshold. The default value is **200**, in MB.
	cpuUsage: CPU usage threshold (%). The default value is **10**.

d. Save the **manifest.json** file and exit.

```
:wq
```

4. Restart the Agent.
   - Windows:
     i. In the **C:\Program Files\uniagent\extension\install\telescope** directory, double-click **shutdown.bat** to stop the Agent, and then run **start.bat** to start the Agent.
     ii. In the **C:\Program Files\uniagent\script** directory, double-click **shutdown.bat** to stop the Agent, and then run **start.bat** to start the Agent.
   - Linux:

```
service ces-uniagent stop
service ces-uniagent start
/usr/local/uniagent/extension/install/telescope/telescoped restart
```

1.1.22 How Do I Change the Process Collection Frequency by Modifying the Configuration File?

The following describes how to modify the configuration file to change the process collection frequency.

Linux

Step 1 Log in to a server as user **root**.

Step 2 Modify the configuration file.

```
cd /usr/local/uniagent/extension/install/telescope/conf && vi custom_conf.json
```

Enter the following configuration content in {} to change the number of processes updated per minute. The calculation method is as follows: (*${telescope.metric.proc.flush_metric_batch_size}* x *${telescope.metric.proc.flush_metric_period}*)/60

```
"telescope.metric.proc.flush_metric_batch_size":"num1",
"telescope.metric.proc.flush_metric_period":"num2"
```

Configurations for updating 50 processes per minute

```
[root@ conf]# pwd
/usr/local/uniagent/extension/install/telescope/conf
[root@e nf]# cat custom_conf.json
{
        "telescope.metric.proc.flush_metric_batch_size":"50",
        "telescope.metric.proc.flush_metric_period":"60"
}
```

Step 3 Restart the Agent.

```
service ces-uniagent stop
service ces-uniagent start
/usr/local/uniagent/extension/install/telescope/telescoped restart
```

----End

Windows

Step 1 Log in to a server.

Step 2 Modify the **custom_conf.json** configuration file in **C:\Program Files\uniagent\extension\install\telescope\conf** to change the number of processes updated per minute. The calculation method is as follows: (*${telescope.metric.proc.flush_metric_batch_size}* x *${telescope.metric.proc.flush_metric_period}*)/60

Example: If you want to update 50 processes every minute, enter the following content in {}:

```
"telescope.metric.proc.flush_metric_batch_size":"50",
"telescope.metric.proc.flush_metric_period":"60"
```

Step 3 In the **C:\Program Files\uniagent\extension\install\telescope** directory, restart the Agent.

1. Double-click **shutdown.bat** to stop the Agent process.
2. Double-click **start.bat** to start the Agent process.

----End

1.2 Cloud Service Monitoring

1.2.1 What Is Aggregation?

Aggregation is a process where Cloud Eye aggregates the maximum, minimum, average, sum, or variance value of raw data sampled for different periods, and this process repeats for each subsequent period. Each period is called an aggregation period. A calculation period is called an aggregation period.

During the aggregation, data sets are smoothed. A longer aggregation period means more smoothing and precise data, enabling you to predict trends more precisely. On the contrary, a shorter aggregation period means more accurate alarms.

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

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

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

For example, the instance quantity in Auto Scaling is an integer. If the aggregation period is 5 minutes, and the current time is 10:35, Cloud Eye will aggregate the raw data generated between 10:30 and 10:35 to the time point of 10:30. If the raw data 1 and 4, after aggregation, 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 aggregation method best meets your service requirements.

1.2.2 How Long Is Metric Data Retained?

Metric data includes raw data and rolled-up data.

- Raw data is retained for 2 days.
- Rolled-up data is data aggregated based on raw data. The retention period for rolled-up data depends on the rollup period.

Table 1-6 Retention periods for rolled-up data

Rollup Period	Retention Period
1 minute	2 days
5 minutes	10 days
20 minutes	20 days
1 hour	155 days
4 hours	155 days
24 hours	155 days

If an instance is disabled, stopped, or deleted, its metrics will be deleted one hour after the raw data reporting of those metrics stops. When the instance is enabled or restarted, raw data reporting 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 metric data generated before these metrics were deleted.

1.2.3 What Aggregation Methods Does Cloud Eye Support?

Cloud Eye supports the following aggregation methods:

- Average

  The arithmetic average of metrics collected during an aggregation period. It helps identify long-term trends in cloud product performance, serves as a baseline reference for anomaly detection, and supports capacity planning based on average load. However, average values can obscure extreme fluctuations. When data is unevenly distributed, the average may not accurately reflect reality. You need to analyze the average along with the maximum and minimum values.

- Maximum

  The highest value of metrics collected during an aggregation period. This metric is crucial for identifying spikes and possible issues in the monitoring system.

- Minimum

  The minimum value of metrics collected during an aggregation period. This metric is crucial for identifying abnormally low values (for example, traffic dropping to zero) and potential issues in the monitoring system.

- Sum

  The sum of metric data collected during an aggregation period. This is a key statistical value used for analyzing resource consumption metrics, such as traffic volume and storage usage.

  NOTE

  During an aggregation process, data generated within a specified time range is consolidated to the start point of the aggregation period using the relevant aggregation algorithm. Take a 5-minute period as an example. If the current time is 10:35, the raw data generated between 10:30 and 10:35 will be aggregated to 10:30.

An intelligent report supports the following aggregation methods: Maximum, Minimum, Average, P50, P90, and P95.

- P50: The median value after the metric data is sorted in ascending order within an aggregation period. It indicates that 50% of the data points are less than or equal to this value, while the remaining 50% are greater.
- P90: The value at the 90% position after the metric data is sorted in ascending order. It means 90% of the data points are less than or equal to this value, and 10% are greater.
- P95: The value at the 95% position after the metric data is sorted in ascending order within an aggregation period. It indicates that 95% of the data points are less than or equal to this value, while the remaining 5% are greater.

1.2.4 How Can I Export Collected Data?

You can export monitoring data from Cloud Eye. The procedure is as follows:

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 file displays the username, region, service, instance name, instance ID, metric name, metric data, time, and timestamp. You can view historical monitoring data.
- To convert the time using a Unix timestamp to the time of the target time zone, perform the following steps:
  a. Use Excel to open a CSV file.
  b. Use the following formula to convert the time:
     Target time = [Unix timestamp/1000 + (Target time zone) x 3600]/86400 + 70 x 365 + 19
  c. Set the cell format to **Date**.

1.2.5 What Are Outband Incoming Rate and Outband Outgoing Rate?

Concept Explanation

You need to understand the meaning of outband and inband:

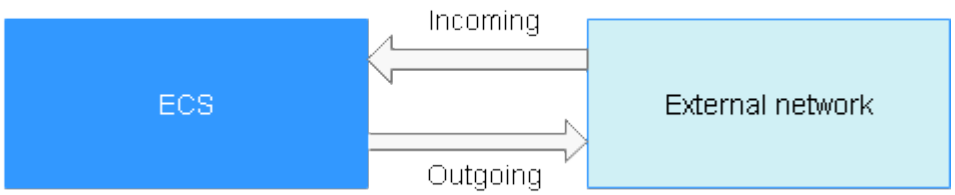
Outband

- 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 1-7 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 1-8 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

1.2.6 Why Is the Total Number of Resources for the Same Cloud Service Inconsistent on Different Monitoring Pages?

Cloud service resource data sources and cache modes differ based on monitoring scenarios, so the number of queried resources varies. For details about the data sources of cloud services, see **Table 1-9**.

Table 1-9 Data sources of cloud services

Cloud Service	Data Source of Total Resources on the Overview Page	Data Source of Total Resources in the Cloud Service Monitoring List	Data Source of the Cloud Service Monitoring Instance List
Multi-layer cloud services (such as iMetal, RDS_MYSQL_CLUSTER, CC, ModelArts, NoSQL, ROMA, ELB, ER,GA, DDS, ES, CPH, DDMS, GaussDBV5, DBProxy, RES, APIC, HTAP, MRS, LTS, EdgeGateway, MSGSMS, ICA, EC, BMS, DDoS, BFS, CODEARTS_LINK, EG, ANC, IES, VPN and OBS)	Cloud Eye metric database, cached for 10 minutes	Cloud Eye metric database, cached for 10 minutes	Cloud service, without cache
Key cloud services (such as ECS, EIP, DMS, DCS, RDS, TaurusDB, AS, and CBR)	Cloud service, cached for 10 minutes	Cloud service, cached for 10 minutes	Cloud service, without cache
Other single-layer cloud services	Cloud Eye metric database, cached for 10 minutes	Cloud Eye metric database, cached for 10 minutes	CES metric database, without cache

1.3 Alarm Management

1.3.1 What Are Alarm Notifications? How Many Types of Alarm Notifications Are There?

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 emails, or send HTTP/HTTPS requests to servers.
- Work with Auto Scaling to trigger the system to automatically add or remove servers.

1.3.2 What Alarm Status Does Cloud Eye Support?

Alarm, **Resolved**, **Insufficient data**, **Triggered**, **Expired**, and **Resolved (forcible clear)** are supported.

- **Alarm**: The metric value reached the alarm threshold, and an alarm has been triggered but not cleared for the resource.
- **Resolved**: The metric value went back to the normal range, and the resource alarm was cleared.
- **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.
- **Triggered**: The monitored resource has triggered the event configured in the alarm policy.
- **Expired**: The monitored resources or alarm policies in the alarm rule were adjusted, so the original alarm record status expired.
- **Resolved (forcible clear)**: You can forcibly clear alarms in the **Triggered**, **Alarm**, or **Insufficient data** state.

1.3.3 What Alarm Severities Are Available on Cloud Eye?

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.

1.3.4 How Do I Monitor and View the Disk Usage?

To monitor the disk usage, install the 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.

1.3.5 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 **Recipient** to **Account contact**, alarm notifications will be sent to the phone 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 phone number or email address as prompted.

SMN Topic Subscribers

If you set **Recipient** to an SMN topic, perform the following steps to change the phone numbers:

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

1.3.6 How Can an IAM User Receive Alarm Notifications?

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

1.3.7 Why Are Resource Names Not Displayed in Alarm Notifications?

In alarm notifications of Cloud Eye, instance names are not displayed for some cloud services. The possible causes are as follows:

- Cloud services are not properly interconnected in accordance with Cloud Eye specifications.
- Cloud services are not interconnected with RMS, so Cloud Eye cannot obtain the resource names from RMS.
- Other: The resources have been deleted, or some resources do not have names.

Table 1-10 lists the cloud services whose resource information, such as resource names and enterprise projects, is not reported in the current alarm notification.

Table 1-10 Cloud services with no resource names reported

Cause	Namespace	Cloud Service
Non-standard cloud service interconnection	SYS.SFS	Scalable File Service
	SYS.VOD	Video on Demand
	SYS.DBSS	Database Security Service
	SYS.OBS	Object Storage Service
	SYS.FunctionGraph	FunctionGraph
	SYS.ROMA	ROMA Connect
	SYS.Maas	Marketplace as a Service
The cloud service not interconnected with the RMS	SYS.APIG	API Gateway
	SYS.CloudTable	CloudTable Service
	SYS.DDOS	Anti-DDoS
	SYS.EG	EventGrid
	SYS.GA	Global Accelerator
	SYS.LIVE	Live
	SYS.DAYU	Database Security Service
	SYS.WAF	Web Application Firewall
Other cases (resources being deleted, unnamed, or of a special type)	SYS.GAUSSDB	TaurusDB
	SYS.RMS	Config
	SYS.RDS	Relational Database Service

The preceding statistics will be regularly updated. If the resource name information is not displayed in the alarm notification, log in to the Cloud Eye console and search for the resource name in the alarm record based on the resource ID.

1.3.8 Why Are Unreached Cloud Services Displayed on the Cloud Eye Console?

When you select cloud services, you'll see all those interconnected with Cloud Eye. Choose the cloud services available at your site. **Table 1-11** lists related functions.

Table 1-11 Functions of cloud services interconnected with Cloud Eye

Feature	Applied Scenario
Creating an Alarm Rule	On the **Create Alarm Rule** page, if you set **Alarm Type** to **Event** and **Event Type** to **System event**, you will see all cloud services interconnected with Cloud Eye in the event source list.
One-Click Monitoring	On the one-click monitoring page, you can see all cloud services interconnected with Cloud Eye.
Alarm Masking	On the **Create Alarm Masking** page, if you set **Masked By** to **Event**, you will see all cloud services interconnected with Cloud Eye in the event source list.
Resource Groups	On the **Create Resource Group** page, if **Add Resources** is set to **Automatically**, you will see all cloud services interconnected with Cloud Eye in the cloud product list.
	On the **Create Resource Group** page, if you set **Add Resources** to **Automatically** and **Resource Level** to **Specific dimension** and click **View monitored dimensions**, you will see all cloud services interconnected with Cloud Eye on the **Types of Resources That Can Be Added Automatically** page.
	On the **Create Resource Group** page, if you set **Add Resources** to **Manually** and **Resource Level** to **Cloud product**, you will see all cloud services interconnected with Cloud Eye in the cloud product list.
	On the **Create Resource Group** page, if you set **Add Resources** to **Manually** and **Resource Level** to **Specific dimension**, you will see all cloud services interconnected with Cloud Eye in the resource selection list.
Alarm Templates	On the **Create a Custom Alarm or Event Template** page, if you click **Add Resource Types**, you will see all cloud services interconnected with Cloud Eye in the resource type list.
	In the default alarm or event template list, you can see all cloud services interconnected with Cloud Eye.

2 Troubleshooting

2.1 Permissions Management
2.2 Server Monitoring
2.3 Cloud Service Monitoring
2.4 Alarm Management
2.5 Data Dump

2.1 Permissions Management

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

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

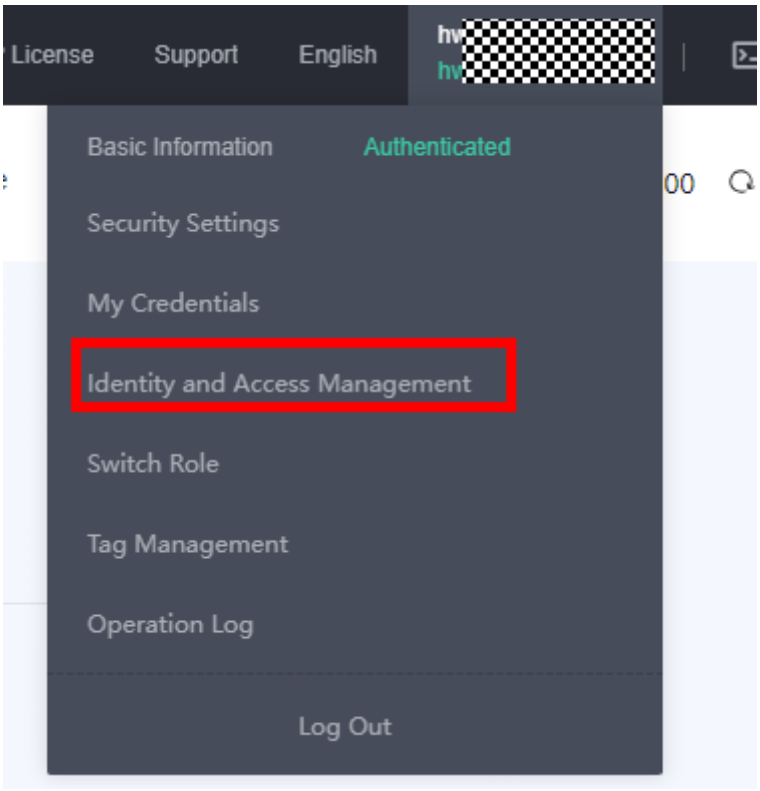
NOTE

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

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

This is because that you use an IAM user account, which 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, choose **User Groups**.
4. Expand details of the user group the user belongs to.
5. Grant permissions to the user group that 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**.

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

Symptoms

When an IAM user clicked **Configure** on the **Server Monitoring** page, a message indicating insufficient permissions was displayed.

Possible Causes

The IAM agency permissions are not configured for the IAM user.

Procedure

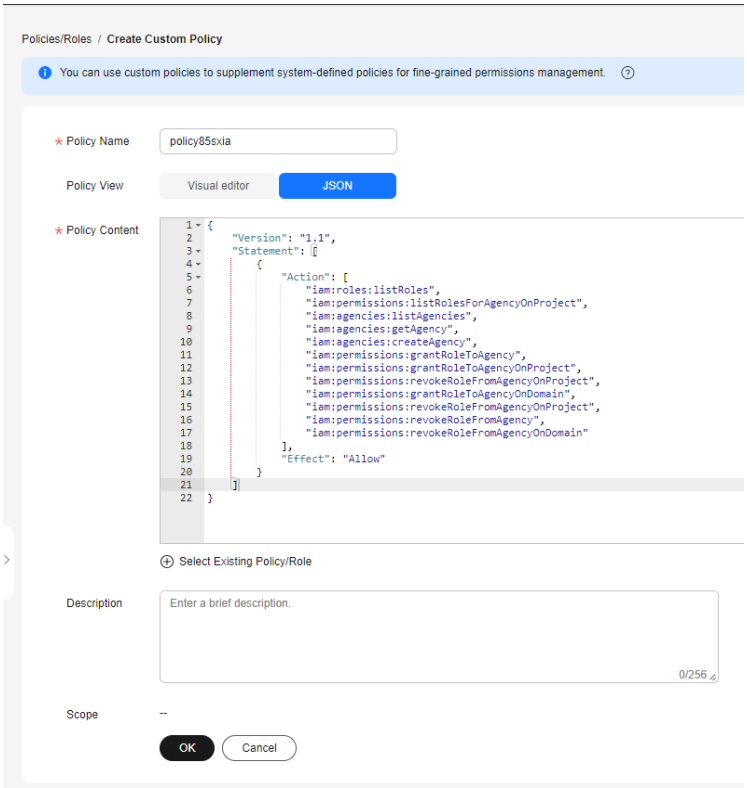
Step 1 Add a policy for querying the agencies.

1. Log in to the Huawei Cloud management console using an account or IAM user that has the permissions to create custom policies and grant permissions to other IAM users.
2. Ensure that the account has been granted the Agent permissions for the region by performing the following operations: On the Cloud Eye console, choose **Server Monitoring** > **Elastic Cloud Server**. Check whether **Configure** is displayed above the ECS list.
   - If no, the Agent permissions have been granted for the region.
   - If yes, click **Configure** to enable the Agent permissions for the region.
3. 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, choose **Permissions** > **Policies/Roles**. Search for the CES agency policy **CES AgencyCheck Access**. If the policy can be found, grant permissions by referring to **Step 2**. If the policy does not exist, perform the following steps to create a custom policy:
   a. Click **Create Custom Policy** in the upper right corner.
      i. Configure the following parameters:
         - **Policy Name**: Specify a custom policy name.
         - **Policy View**: Select **JSON**.
         - **Policy Content**: Copy the following code and paste it to the text box.

```
{
   "Version": "1.1",
   "Statement": [
      {
         "Action": [
            "iam:agencies:createAgency",
            "iam:agencies:getAgency",
            "iam:agencies:listAgencies",
            "iam:permissions:grantRoleToAgency",
            "iam:permissions:grantRoleToAgencyOnDomain",
            "iam:permissions:grantRoleToAgencyOnProject",
            "iam:permissions:listRolesForAgency",
            "iam:permissions:listRolesForAgencyOnDomain",
            "iam:permissions:listRolesForAgencyOnProject",
            "iam:permissions:revokeRoleFromAgency",
            "iam:permissions:revokeRoleFromAgencyOnDomain",
            "iam:permissions:revokeRoleFromAgencyOnProject",
            "iam:roles:createRole",
            "iam:roles:listRoles",
            "iam:roles:updateRole"
         ],
         "Effect": "Allow"
      }
   ]
}
```

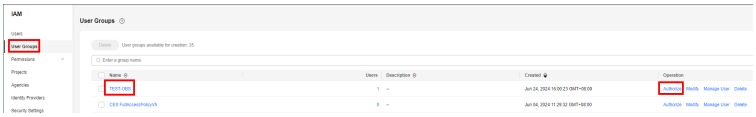
         - **Description**: (Optional) Provide supplementary information about the policy.
      ii. Confirm the policy content(see **Figure 2-1**) and click **OK** to save the policy.

Figure 2-1 Create Custom Policy

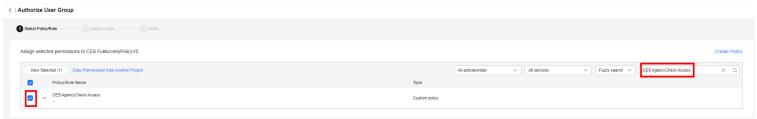


Step 2 Assign permissions to the IAM user.

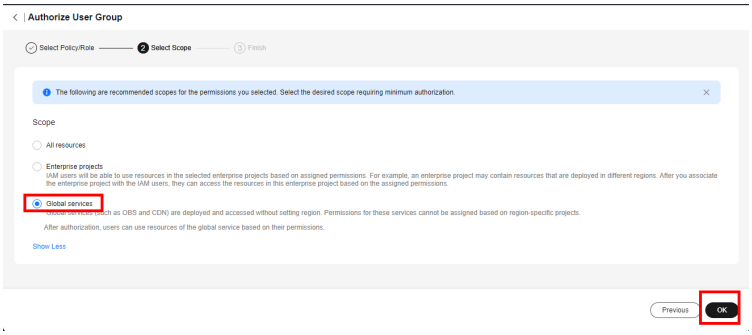
1. In the navigation pane, choose **User Groups**, locate the user group that contains the IAM user, and choose **Authorize** in the **Operation** column.



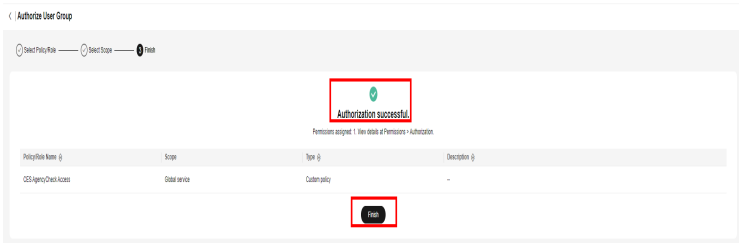
2. Search for the added custom policy name or **CES AgencyCheck Access**, select the policy, and click **Next**.



3. Select **Global services** and click **OK**.



4. If **Authorization successful** is displayed, click **Finish**.



----End

2.2 Server Monitoring

2.2.1 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, 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 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.

Possible Causes

The circuit patter 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 system is as follows:

The system checks the CPU usage and memory usage of the Agent process every minute. If the CPU usage exceeds 30% or the memory usage exceeds 700 MB, that

is, the second threshold, the Agent process will exit. If both the CPU usage and memory usage do not exceed the second threshold, the system checks whether they exceed the first threshold (10% of CPU usage or 200 MB of memory usage). If any of them exceeds the first threshold for three consecutive times, the Agent process will exit and the information will be recorded.

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\bin**.

   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 2-1**.

Table 2-1 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.
[a] To query the CPU usage and memory usage of the Agent, use the following method: • Linux: **top -p** *telescope PID* • Windows: View the details about the Agent process in **Task Manager**.	


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

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

:wq

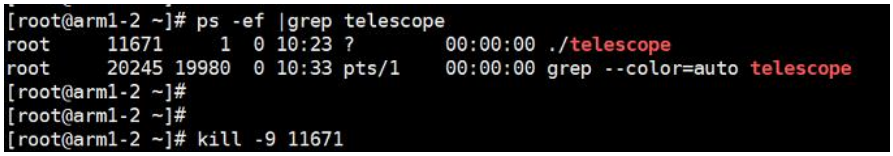
4. Restart the Agent.
   - Windows:
     - In the directory where the Agent installation package is stored, double-click the **shutdown.bat** script to stop the Agent, and then execute the **start.bat** script to start the Agent.
   - Linux:
     - Check the Agent process ID.

       ps -ef |grep telescope

     - Run **kill -9** *PID* to stop the process and then wait for 3 to 5 minutes for the Agent to automatically restart.

       kill -9 *PID*

       Figure 2-2 Restarting the Agent

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

Cloud Eye Agent uses a port from path **/proc/sys/net/ipv4/ip_local_port_range** to send HTTP requests. Any port in the range obtained may be occupied. If the port used by the Agent is the same as the service port, 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 ID 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. 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. Apply the changes.
   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**
     - Run the following command to stop the process and then wait for 3 to 5 minutes for the Agent to restart.
     - **kill -9** *PID*

     Figure 2-3 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
     ```

2.2.3 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 ID is returned, the new version of the Agent is used.
- If **0** is returned, the Agent is not installed.

Possible Causes

The following may cause this issue:

1. DNS configurations
2. IAM agency quota
3. 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** page, check whether the DNS server addresses of the ECS are correct.

   For details about how to configure DNS server addresses 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)**.

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, 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 CommonOperations, or BMS CommonOperations and CES Administrator, or CES FullAccess

----End

2.2.4 Why Is No Monitoring Data Displayed After Performing a One-Click Restoration 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 ID 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.

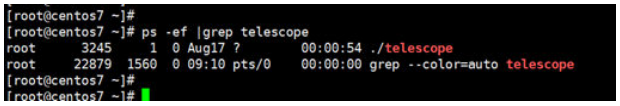
Procedure (Linux)

1. Log in to the ECS or BMS as user **root**.
2. Check whether the **telescope** process is running.

   ps -ef |grep telescope

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

   Figure 2-4 Viewing the telescope processes



- If the telescope process is normal, go to **4**.
- If the telescope process is abnormal, go to **3**.

3. Start the Agent.

   service uniagent restart

4. Check whether an agency has been created for the server.

   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 2-5 Failing to obtain the AK/SK

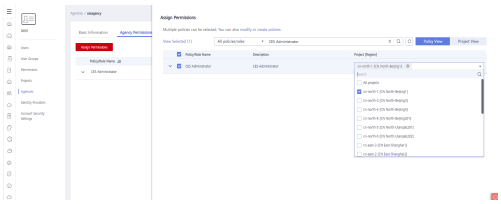
   ```
   <html>
    <head>
     <title>401 Unauthorized</title>
   </head>
   <body>
    <h1>401 Unauthorized</h1>
    agency_name is empty in metadata<br /><br />
   
   
   </body>
   ```

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 2-6 Searching for **cesagency**

   Figure 2-7 Assigning permissions

   - If the problem is resolved, no further action is required.
   - Otherwise, go to **6**.

6. Check whether the DNS settings are normal.

   ping *agent.ces.myhuaweicloud.com*

   - If yes, no further action is required.
   - If no, 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 2-8** and **Figure 2-9**, the telescope process is running.

   Figure 2-8 agent process (Windows)

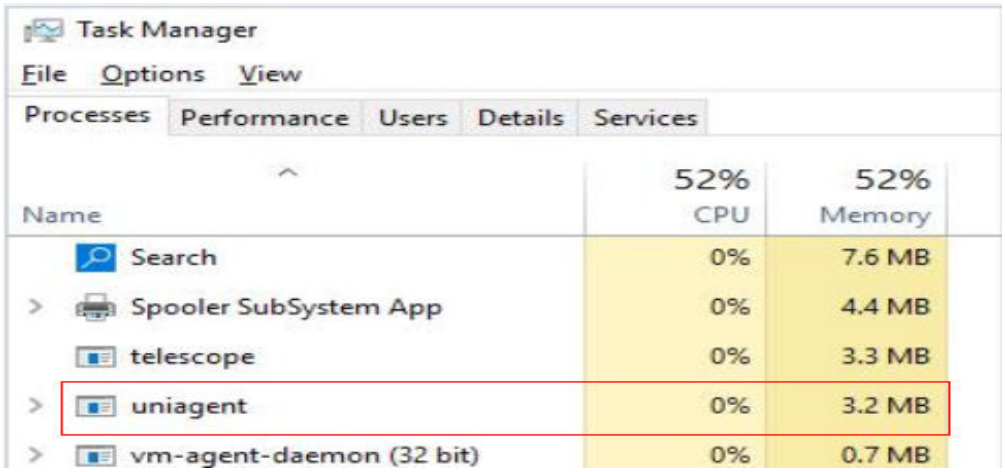
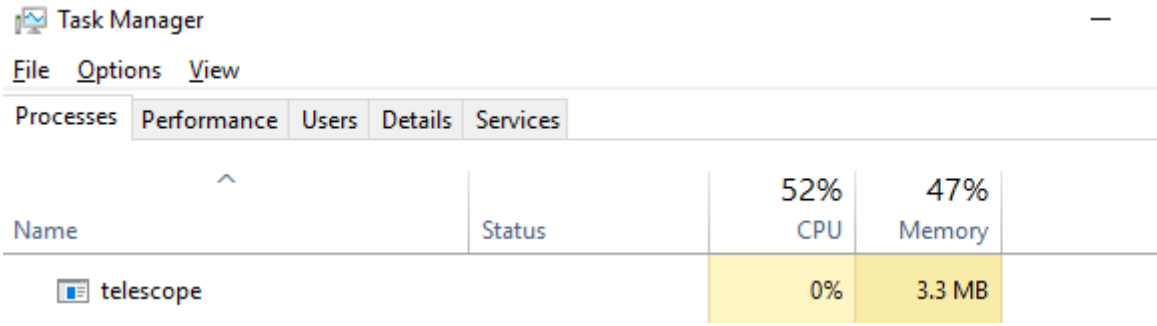
   

   Figure 2-9 telescope process (Windows)

   - 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 2-10 Searching for **cesagency**

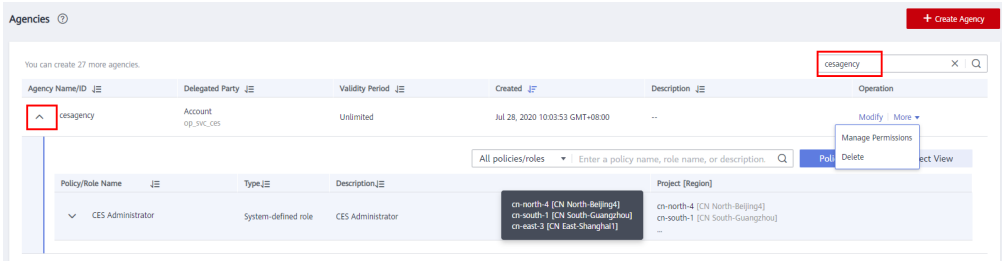
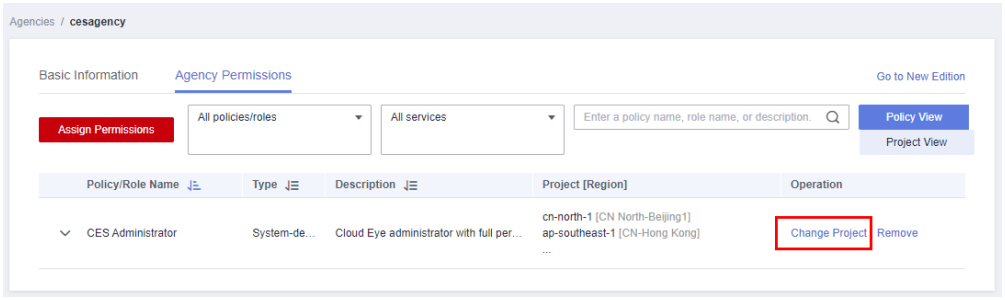


Figure 2-11 Assigning permissions



- If the problem is resolved, no further action is required.
- Otherwise, go to **6**.

5. Check whether the DNS settings are normal.

   ping *agent.ces.myhuaweicloud.com*

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

   NOTE

   For details about Cloud Eye endpoints for each region, see **Regions and Endpoints**.

2.2.5 How Can I Troubleshoot the Issue 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:

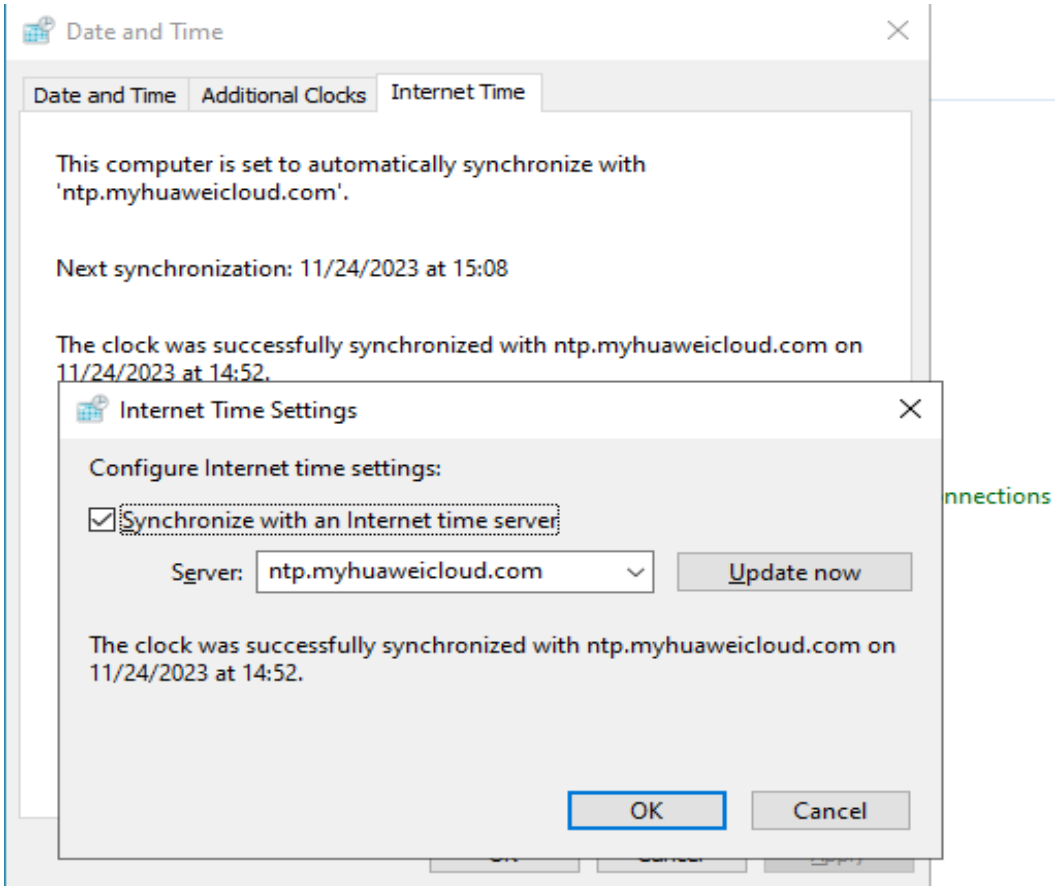
```
ntpdate -u ntp.myhuaweicloud.com
```

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** > **Internal Time** > **Change Settings**.

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



2.2.6 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 has not receive any heartbeat messages for 3 minutes, **Agent Status** becomes **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**. If it is, check that the Agent is correctly configured by referring to **(Optional) Manually Configuring the Agent**.

- The account is in arrears.
- The Agent process is faulty. In this case, restart the Agent by referring to **Managing the Agent**. If the Agent cannot be restarted, related files may have been deleted by mistake and you need to reinstall the Agent.
- The server time is inconsistent with the local standard time.
- The log path varies depending on 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**

2.2.7 What Should I Do If the Agent 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.

Starting the Agent (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.

Starting the Agent (Early Version)

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.

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

If there is no monitoring data 10 minutes after the Agent is installed, **InstanceId** in the **conf** file may be incorrectly configured.

Correct the configurations by performing operations described in **(Optional) Manually Configuring the Agent (Linux)**.

2.2.9 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. 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.

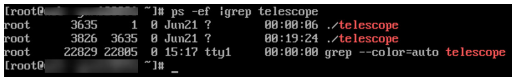
Procedure (Linux)

1. Log in to the ECS or BMS as user **root**.
2. Check whether the Agent process is running.

   ps -ef |grep telescope

   The following information indicates that the Agent process is normal.

   Figure 2-12 Viewing the telescope processes



- If the telescope process is normal, go to **4**.
- If the telescope process is abnormal, go to **3**.

3. Start the Agent.

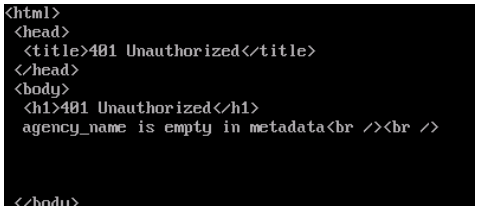
   /usr/local/telescope/telescoped start

4. 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 2-13 Failing to obtain the AK/SK

5. On the Cloud Eye console, choose **Server Monitoring** > **Elastic Cloud Server**, select the target ECS, and click **Restore Agent Configurations**.

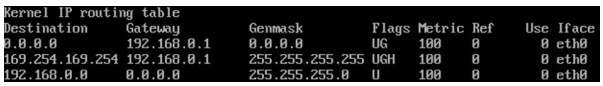
   - If the problem is resolved, no further action is required.
   - Otherwise, go to **6**.

6. Check the route.

   route -n

   The following information indicates that the route is normal.

   Figure 2-14 Normal route configuration-Linux

   - 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.

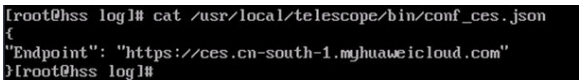
   - If yes, no further action is required.
   - If no, go to **8**.

8. Open the Agent configuration file.

   cat /usr/local/telescope/bin/conf_ces.json

9. Obtain the endpoint from the Agent configuration file.

Figure 2-15 Querying the Agent endpoint



10. Check whether the DNS settings are normal.

    ping *ces.cn-south-1.myhuaweicloud.com*

    - If yes, no further action is required.
    - If no, 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 or as an administrator.
2. Open the **Task Manager** and check whether the Agent process is running.

   If there are **Figure 2-16** and **Figure 2-17**, the Agent process is running.

   Figure 2-16 agent process (Windows)

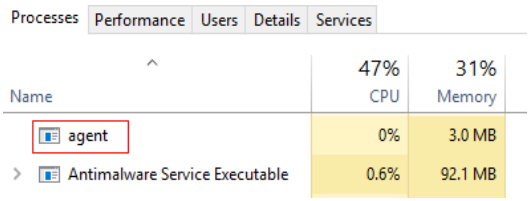
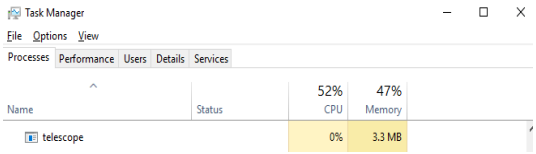
   

   Figure 2-17 telescope process (Windows)

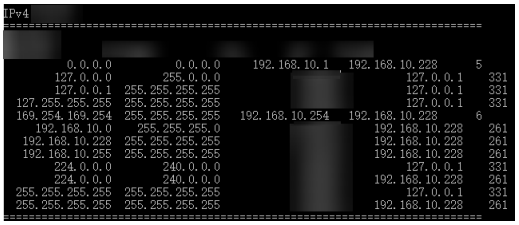
   

   - If the telescope process is normal, go to **4**.
   - If the telescope process is abnormal, go to **3**.
3. Double-click **start.bat** to start the Agent.
4. Access **http://169.254.169.254/openstack/latest/meta_data.json** and check whether the agency has been created.
   - If the website is accessible, the agency is normal. No further action is required.
   - Otherwise, go to **6**.
5. Check the route.

   route print

   The following information indicates that the route is normal.

Figure 2-18 Normal route configuration-Windows



- 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 Agent installation package is stored.
8. Obtain the endpoint from the Agent configuration file.

   {"Endpoint":"https://ces.cn-north-4.myhuaweicloud.com"}

9. Check whether the DNS settings are normal.

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

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

     NOTE

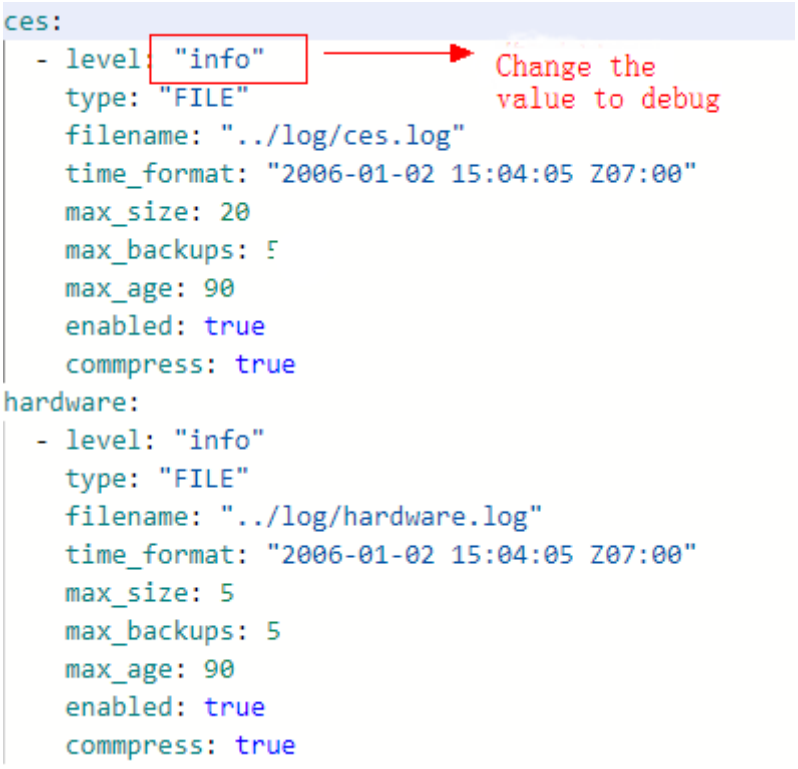
     For details about Cloud Eye endpoints for each region, see **Regions and Endpoints**.

2.2.10 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

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



3. Restart the Agent by referring to **Managing the Agent**.
4. After obtaining the debug logs, restore the modified configurations and restart the Agent by referring to **Managing the Agent**.

2.2.11 Why Is OS Monitoring Data Not Displayed Immediately After the Agent Is Installed and Configured or Not Displayed at All?

After you install the Agent, choose **Server Monitoring**, wait for 2 minutes before you can see the monitoring data 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 uses the ECS or BMS local time. When the console delivers requests, it uses the browser time of the user client. If the two times are different, no OS monitoring data will be displayed on the Cloud Eye console.

2.2.12 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 when no data was collected.

2.2.13 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**.

2.2.14 Why Is There No Block Device Usage Metric for One of the Two Disks on a Server?

Symptom

When you view the disk I/O metrics on the Cloud Eye console, two disks **vda** and **vdb** are displayed. The block device usage metric is available for **vda** but not for **vdb**.

Possible Causes

If a disk is not attached to a mount point, the block device usage of the disk will not be collected. In the following figure, the **vdb** disk is not attached.

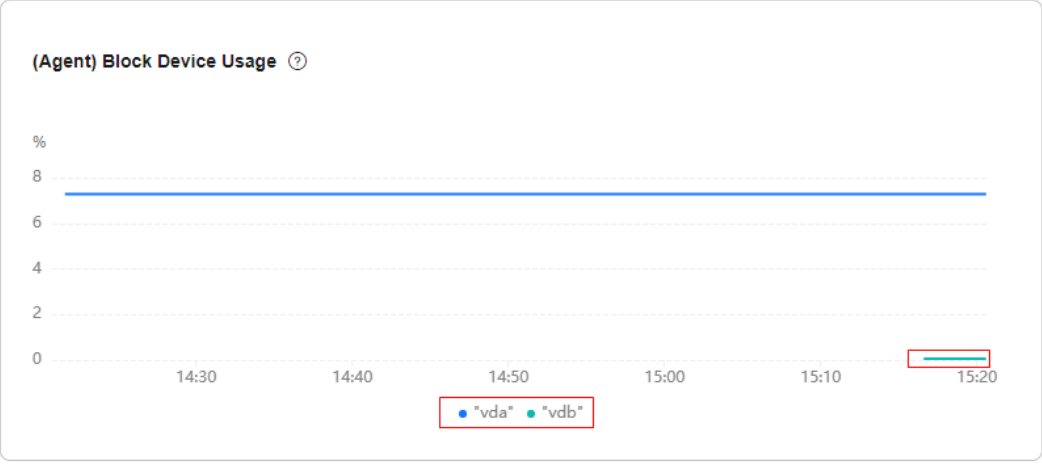
```
[root@ecs-block-0001 conf]# lsblk
NAME   MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
vda    253:0    0  40G  0 disk
└─vda1 253:1    0  40G  0 part /
vdb    253:16   0  10G  0 disk
```

Procedure

1. Attach the disk to a mount point.

```
[root@ecs-block-0001 mnt]# lsblk
NAME   MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
vda    253:0    0  40G  0 disk
└─vda1 253:1    0  40G  0 part /
vdb    253:16   0  10G  0 disk
└─vdb1 253:17   0   2G  0 part /mnt/sdc
```

2. Verify that the block device usage can be collected.



2.2.15 Why Is the Agent Status Abnormal on the Cloud Eye Server Monitoring Page While OS Monitoring Metrics Are Displayed as Normal?

Symptom

On the Cloud Eye server monitoring page, the Agent status was abnormal, but the OS monitoring metrics were displayed as normal.

Possible Causes

The Agent of an earlier version had a problem with status management. As a result, the Agent was displayed as abnormal on the console, but the Agent was functioning properly and OS monitoring metrics cloud be collected and reported.

Procedure

Step 1 Uninstall the Agent. For details, see **Managing the Agent**.

Step 2 Install an Agent of the latest version. For details, see **Installing the Agent**.

----End

2.3 Cloud Service Monitoring

2.3.1 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**.

2.3.2 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 collection and monitoring frequency for each service that has been interconnected with Cloud Eye is not the same. The data may have just not been collected yet.
- The ECS or BMS has been stopped for more than one 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 stopped.
- It has been less than 10 minutes since the resource was purchased.
- No data is reported. If no monitoring data is reported for all instances of a cloud service for more than three hours, the cloud service will not be displayed in the cloud service monitoring list. However, for services like API Gateway, OBS, FunctionGraph, DIS, DataArts Studio, SFS, and Live, their monitoring data will be retained for seven days.

2.3.3 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 complete, 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.

2.4 Alarm Management

2.4.1 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 the monitoring data reporting interval is longer than three hours and no monitoring data is reported for three consecutive intervals, the alarm rule status also changes to **Insufficient data**.

2.4.2 Why Did I Receive a Bandwidth Overflow Notification While There Is 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 bandwidth for the last 5 minutes falls under the preset threshold, no alarm will be recorded in the system.

2.4.3 Why Can't an Alarm Be Triggered After a 5-Minute Aggregated Metric Alarm Rule Is Configured?

Symptom

A 5-minute aggregated metric alarm rule has been configured for services such as CBR. No alarms were reported even if the triggering conditions had been met three times in a row.

Possible Causes

A metric data record is reported for the CBR service every 15 minutes. After the region of the CloudSense engine is switched, such metrics cannot reach the threshold in two consecutive 5-minute time windows. As a result, the alarm cannot be triggered.

2.4.4 Why Is an Alarm Triggered Contrary to the Alarm Rule That Both the Disk Read and Write Metrics Must Reach the Thresholds

Symptom

The alarm rule is that both the disk read and write metrics must reach the thresholds, but an alarm was triggered when only one of them reached the threshold.

Possible Causes

The ECS reporting the alarm has more than one disk. The read metric of one disk and the write metric of another disk reached the thresholds.

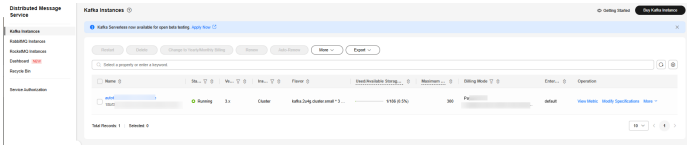
Currently, cloud product alarms are determined by instance. An alarm can be triggered for an instance as long as the metric of any resource of this instance reaches the threshold, instead of the metric of a specific resource. To configure an alarm rule for a specific resource, you are advised to select **Specific dimension** for **Resource Level**.

2.5 Data Dump

2.5.1 What Should I Do When There Is an Abnormal Dump Destination?

On the **Data Dump** page, if **The resource is abnormal** is displayed in the **Destination** column, the possible causes are as follows:

1. **Resource not found**: If no dump destination is found, data dump will fail on Cloud Eye. You can log in to the Distributed Message Service console and check if the destination Kafka cluster has been deleted from the resource list. If it is, you cannot configure it as a dump destination. You need to modify the dump task or delete it and then create a new one.



2. **Other**: Click **Modify** in the **Operation** column to reconfigure a dump destination. Then, restart the task, and check if the dump task can be restored.

