Cloud Eye

Troubleshooting

Issue	01
Date	2026-11-06



HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Copyright © Huawei Cloud Computing Technologies Co., Ltd. 2026. All rights reserved.

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

Trademarks and Permissions


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 Permissions Management 1
1.1 What Should I Do If the IAM Account Permissions Are Abnormal? 1
1.2 What Can I Do If the System Displays a Message Indicating Insufficient Permissions When I Access Cloud Eye? 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? 3
2 Server Monitoring 7
2.1 Agent Installation or Upgrade Failures 7
2.1.1 What Should I Do If the Agent Installation Fails? 7
2.1.2 Why Can't I Install or Upgrade the Agent for Servers in Batches? 10
2.1.3 What Should I Do If the Agent Upgrade Fails for Some Windows Servers? 12
2.2 Agent Exceptions 12
2.2.1 What Should I Do If a Service Port Is Used by the Agent? 12
2.2.2 What Should I Do If the Agent Is in the Agency Configuration Error State? 13
2.2.3 What Should I Do If the Agent Is Faulty? 16
2.2.4 What Should I Do If the Agent Status Switches Between Running and Faulty? 17
2.3 Monitored Data Exceptions 20
2.3.1 What Should I Do If the Agent Status Is Running But Monitoring Data Is Missing? 20
2.3.2 Why Is the Agent Status Abnormal on the Cloud Eye Server Monitoring Page While OS Monitoring Metrics Are Displayed as Normal? 26
2.3.3 Why Are the Inbound Bandwidth and Outbound Bandwidth Negative? 26
2.3.4 Why Is There No Block Device Usage Metric for One of the Two Disks on a Server? 26
2.3.5 What Should I Do If the Disk I/O Usage of the Linux OS Is Incorrect? 28
2.3.6 What Should I Do If There Are No GPU Monitoring Records? 28
2.3.7 Why Are Memory Usage, Disk Usage, Inband Incoming Rate, and Inband Outgoing Rate Not Displayed for an ECS? 29
3 Cloud Service Monitoring 30
3.1 What Should I Do If I See Garbled Chinese Characters in an Exported CSV File? 30
3.2 Why Is the Monitoring Data Not Displayed on the Cloud Eye Console? 30
3.3 Why I Cannot See the Monitoring Data on the Cloud Eye Console After Purchasing Cloud Service Resources? 31
4 Alarm Management 32
4.1 When Will an Alarm Rule Trigger an Insufficient Data Alarm? 32

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

4.2 How Do I Handle an Insufficient Data Alarm Generated After a Resource Is Deleted?.....33
4.3 Why Did I Receive a Bandwidth Overflow Notification While There Is No Bandwidth Overflow Record in the Monitoring Data?.....34
4.4 Why Can't an Alarm Be Triggered After a 5-Minute Aggregated Metric Alarm Rule Is Configured?.....35
4.5 Why Is an Alarm Triggered Contrary to the Alarm Rule That Both the Disk Read and Write Metrics Must Reach the Thresholds.....35
4.6 What Can I Do If an Error Is Reported When I Configure Tags?.....35
5 Data Dump.....37
5.1 What Should I Do When There Is an Abnormal Dump Destination?.....37
6 API.....38
6.1 How Can I Query Monitoring Data of Multiple Metrics?.....38
6.2 How Can I Query Monitoring Data of a Metric?.....51
6.3 What Should I Do If I Do Not Have the Programmatic Access Permission When Calling an API?.....52

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

1 Permissions Management

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

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

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

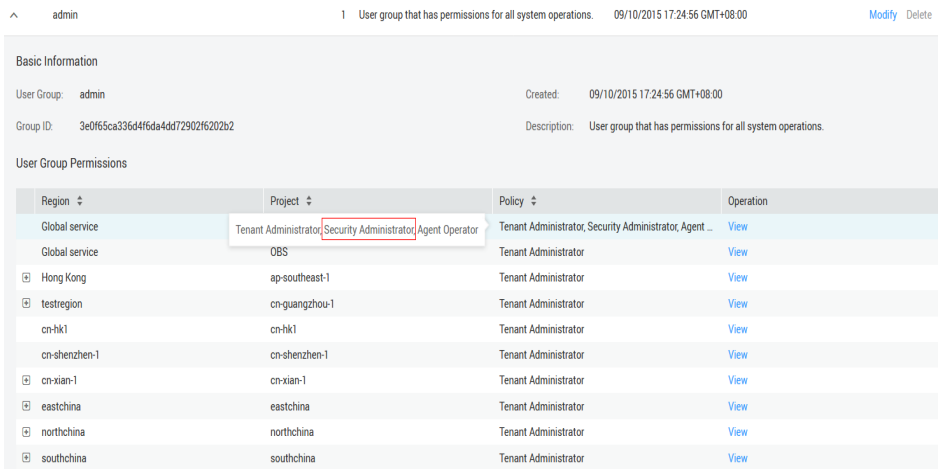
1.1 What Should I Do If the IAM Account Permissions Are Abnormal?

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**.

Figure 1-1 Checking the permissions

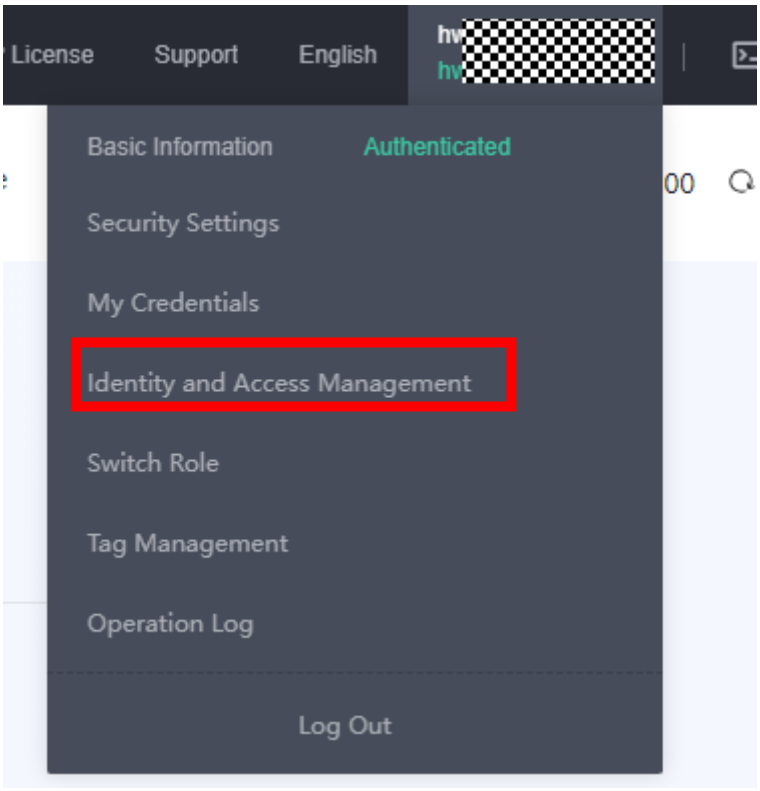


 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

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

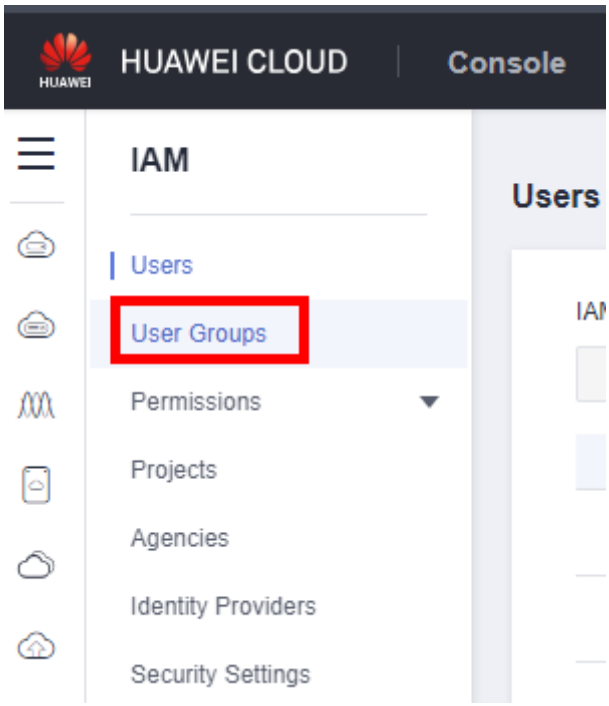
This is because that you use an IAM user account, which does not have sufficient permissions. Check your permissions configured on IAM.

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**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.



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**.

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.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

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.

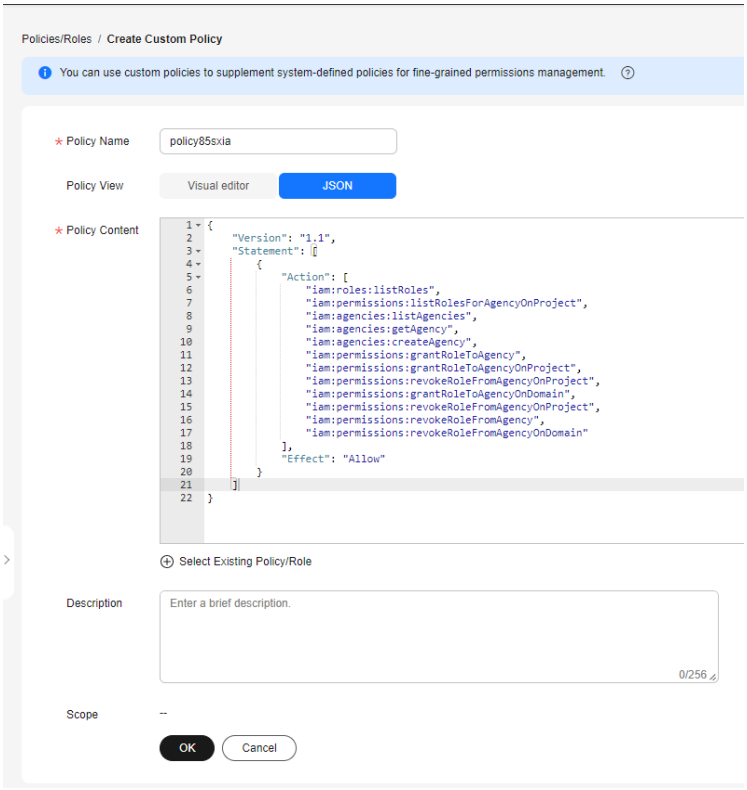
```
{
  "Version": "1.1",
  "Statement": [
    {
      "Action": [
        "iam:agencies:createAgency",
        "iam:agencies:getAgency",
        "iam:agencies:listAgencies",
        "iam:permissions:grantRoleToAgency",
        "iam:permissions:grantRoleToAgencyOnDomain",
        "iam:permissions:grantRoleToAgencyOnProject",
        "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.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

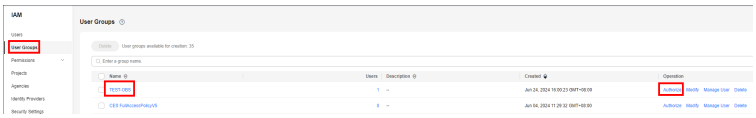
ii. Confirm the policy content(see **Figure 1-2**) and click **OK** to save the policy.

Figure 1-2 Create Custom Policy

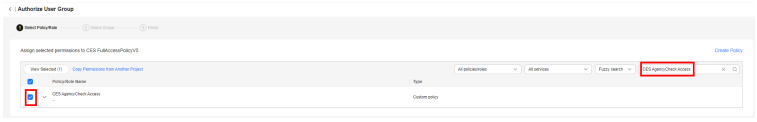


Step 2 Assign permissions to the IAM user.

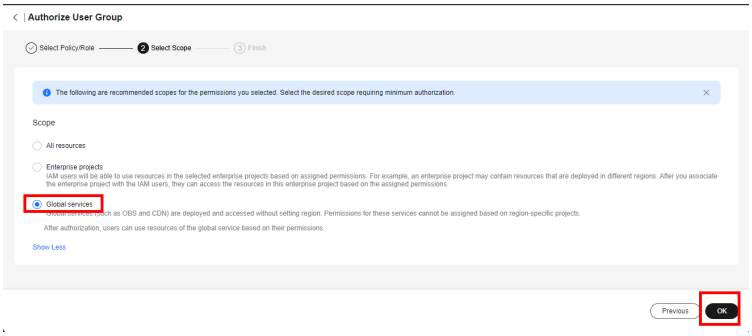
1. In the navigation pane, choose **User Groups**, locate the user group that contains the IAM user, and choose **Authorize** in the **Operation** column.



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

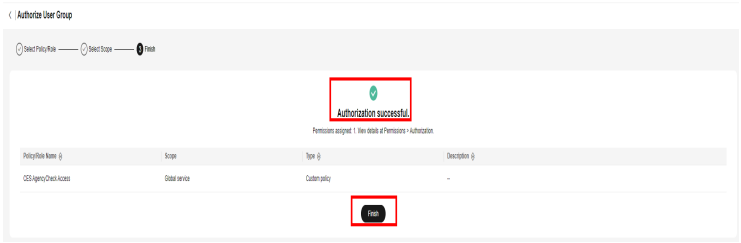


3. Select **Global services** and click **OK**.



 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

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



----End

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

2 Server Monitoring

2.1 Agent Installation or Upgrade Failures

2.2 Agent Exceptions

2.3 Monitored Data Exceptions

2.1 Agent Installation or Upgrade Failures

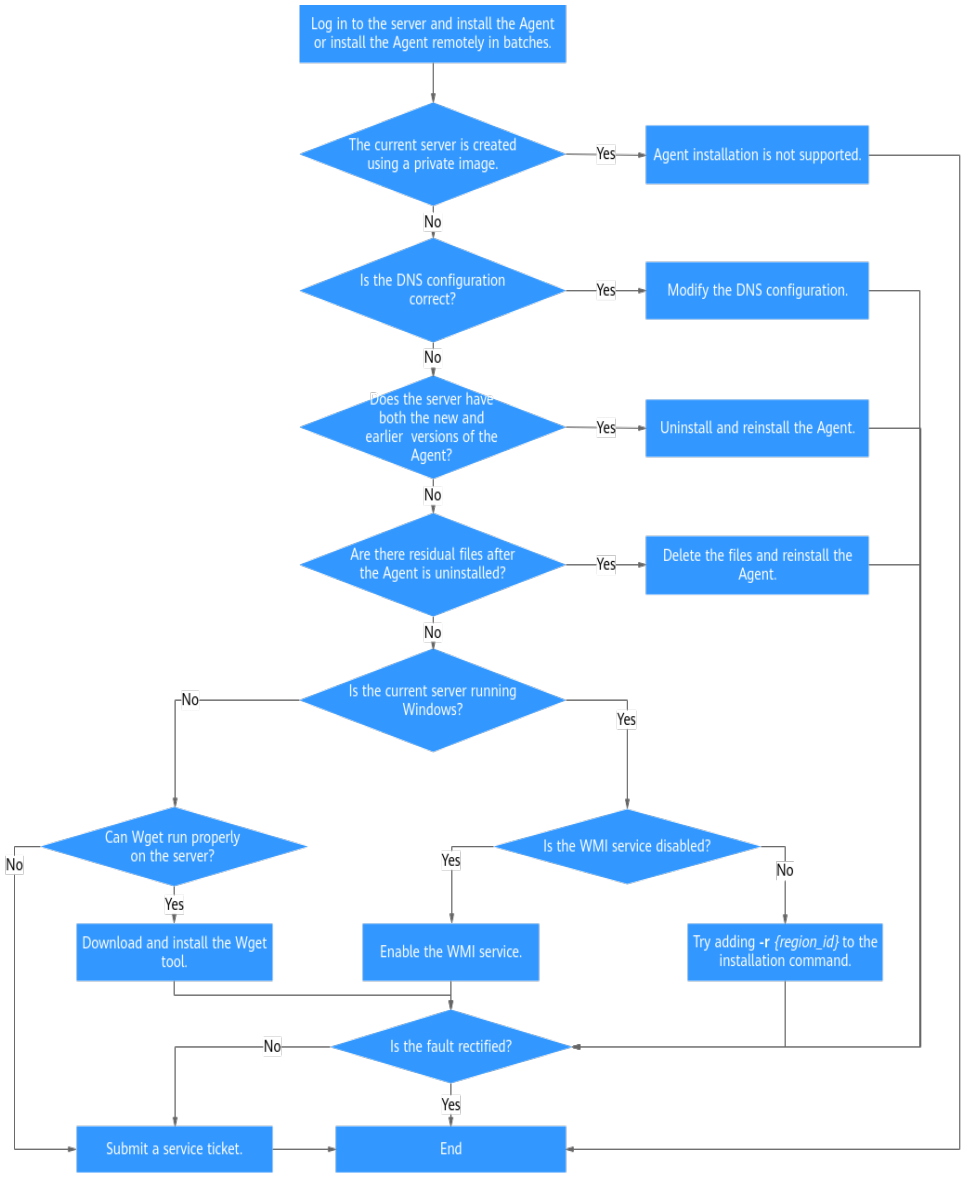
2.1.1 What Should I Do If the Agent Installation Fails?

Symptom

- If the one-click Agent installation fails, the DNS configuration may be incorrect. Check and modify the DNS configuration by referring to **Checking/Modifying the DNS and Security Group Configurations**. If the DNS configuration is correct but the installation still fails, **submit a service ticket** to contact O&M personnel.
- If you fail to log in to the server or manually install the Agent by clicking **Install Remotely**, locate the fault by referring to **Figure 2-1**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Figure 2-1 Troubleshooting an Agent installation failure



Incorrect DNS Configuration

Change the DNS server address. For details, see **Checking/Modifying the DNS and Security Group Configurations**.

Both Earlier and New Versions of the Agent Are Installed

Both earlier and new versions of the Agent are installed on the server, causing configuration file loss. Log in to the server and check whether the **manifest.json** configuration file exists. The path of the configuration file is:

- Linux:
  `/usr/local/uniagent/extension/holder/telescope/manifest.json`
- Windows:
  `C:\Program Files\uniagent\extension\holder\telescope\manifest.json`

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

If the configuration file cannot be found in the path, uninstall the Agent and install the latest Agent. For details about how to uninstall the agent, see **Uninstalling the Agent**.

Residual Files Exist After the Agent Is Uninstalled

The Agent has been installed on the current server. Before the Agent is reinstalled, the uninstalled Agent has residual files.

Check whether all files in the Agent installation directory are deleted. If there are residual files, manually delete them from the following directories:

- Windows:
  - New version: **C:\Program Files\uniagent**
  - Earlier version: **C:\Program Files\telescope**
- Linux:
  - New version:
    ```
    rm /usr/local/uniagent
    ```
  - Earlier version:
    ```
    rm /usr/local/telescope
    ```

The Wget Tool Is Missing on the Linux Server

Wget is an open-source command-line network download tool used to download files from HTTP, HTTPS, FTP, and other protocols. The installation of the Agent on a Linux server depends on Wget to pull the installation script. If Wget is not installed, the error message "command not found" is displayed, the download fails, and the installation process is interrupted.

1. Run the following command. If the message "command not found" is displayed, Wget is not installed on the server.
   ```
   wget --version
   ```
2. Download and install the wget tool. For details, see **https://ftp.gnu.org/gnu/wget/**.

The WMI Service Is Disabled in Windows

The Windows Management Instrumentation (WMI) service provides unified system management APIs for Windows. It allows you to locally and remotely query and manage system resources such as hardware, OSs, applications, services, processes, and performance counters. After this service is disabled, the Agent that depends on it cannot collect Windows metrics such as CPU, memory, disk, process, and network metrics. As a result, monitoring data is missing.

Search for **services.msc** in the search box and open it. Check the status of **Windows Management Instrumentation**. If the status is **Disabled**, perform the following steps to start the WMI service:

1. Right-click **Windows Management Instrumentation** and choose **Properties** from the shortcut menu.
2. Set the startup type to **Automatic**.
3. Click **OK**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

4. Right-click **Windows Management Instrumentation** and choose **Start** from the shortcut menu.

The Windows OS Cannot Obtain Metadata

A Windows ECS cannot obtain metadata through 169.254.169.254.

1. **Submit a service ticket** to contact customer service for ECS technical support.
2. Workaround: Add **-r** *{region_id}* to the installation command. The region ID varies depending on the region. For example, if the ECS is located in CN North-Beijing1, the region ID is **cn-north-1**. For details about the region IDs of other regions, see **Regions and Endpoints**.

Submitting a Service Ticket

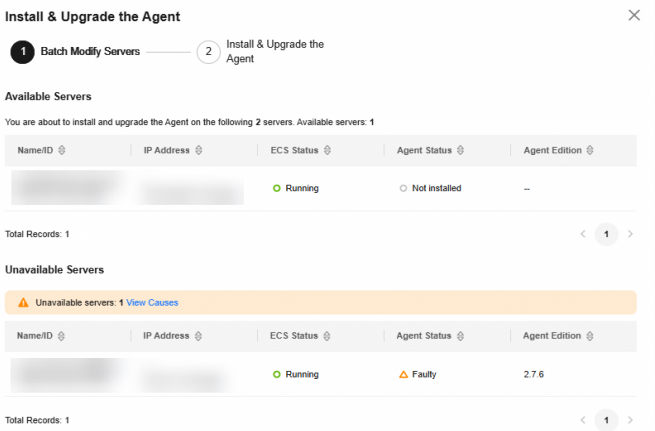
If the problem persists, **submit a service ticket**.

2.1.2 Why Can't I Install or Upgrade the Agent for Servers in Batches?

Symptom

On the **Server Monitoring** page, after you check the boxes on the left of the target servers and choose **Install & Upgrade the Agent** > **Batch Install and Upgrade Agent** above the server list, the message "Unavailable Servers" is displayed on the **Install & Upgrade the Agent** page, as shown in **Figure 2-2**.

Figure 2-2 Installing and upgrading the Agent



Possible Causes

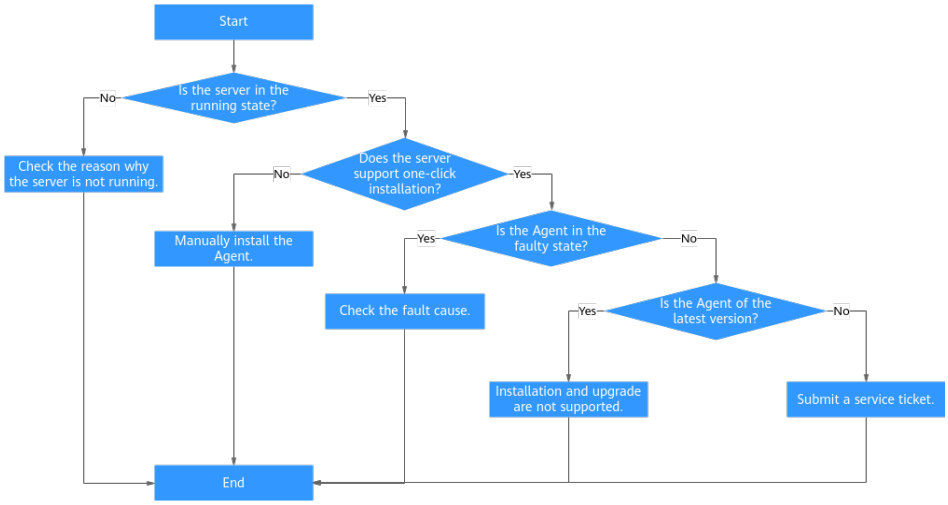
The conditions for installing and upgrading the Agent are as follows:

- The host is running, and the Agent status is **Running**.
- The server is running, the Agent status is **Not installed**, and the server OS supports one-click installation. For details about supported OSs, see **What OSs Does the Agent Support?**

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

If the system displays a message indicating that the Agent cannot be installed or upgraded, rectify the fault by referring to **Figure 2-3**.

Figure 2-3 Troubleshooting method



Cause 1: The Server Is Not in the Running State

In the server monitoring list, check the server status. If the server is not in the running state, go to the **ECS console** to locate the fault or **submit a service ticket** to contact ECS technical support.

Cause 2: The Server OS Does Not Support One-Click Installation

For details about the OSs that support one-click Agent installation, see **What OSs Does the Agent Support?**. If the server does not support one-click installation, log in to the server and manually run the installation command to install or upgrade the Agent. For details, see **Installing the Agent** or **Manually Upgrading the Agent**.

Cause 3: The Agent Status Is Faulty

If the Agent status is faulty, see **What Should I Do If the Agent Is Faulty?** for troubleshooting.

Cause 4: The Agent Version Is the Latest Supported Version

If the Agent installed on the server is already the latest version, installation or upgrade is not supported.

Submitting a Service Ticket

If the problem persists, **submit a service ticket**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

2.1.3 What Should I Do If the Agent Upgrade Fails for Some Windows Servers?

Symptom

On the **Server Monitoring** page, the Agent fails to be upgraded for some Windows servers.

Possible Causes

The internal network settings of some Windows OSs may cause the Agent package download failure.

Procedure

1. On the **Task Center** page, click the **Agent Maintenance** tab, locate the target task, and click **Retry** in the **Operation** column to upgrade the Agent again.
2. If the upgrade still fails after multiple retries, manually upgrade the Agent. For details, see **Manually Upgrading the Agent**.

2.2 Agent Exceptions

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

Cloud Eye Agent reports data using HTTP requests. During the reporting, it randomly occupies dynamic ports listed in **/proc/sys/net/ipv4/ip_local_port_range**. 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.

Prerequisites

Before restarting the Agent, check whether the Agent installed on the current server is of the new or earlier version. For details, see **Checking the Cloud Eye Agent Version**.

Linux

1. Log in to an ECS or BMS as user **root**.
2. Open the **sysctl.conf** file.
   ```
   vim /etc/sysctl.conf
   ```
3. (Permanent change) Add new ports to the **sysctl.conf** file.
   ```
   net.ipv4.ip_local_port_range=49152 65536
   ```
4. Apply the changes.
   ```
   sysctl -p /etc/sysctl.conf
   ```

   NOTE

   - The permanent change still takes effect after the ECS or BMS is restarted.
   - For temporary change (which expires after the ECS or BMS is restarted), run **# echo 49152 65536 > /proc/sys/net/ipv4/ip_local_port_range**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

5. Restart the Agent.

   Earlier version:

   ```
   /usr/local/telescope/telescoped restart
   ```

   New version:

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

Windows

1. Log in to the ECS as an administrator.
2. Open Windows PowerShell and run the following command to change the dynamic IPv4 TCP port range (that is, the temporary source port range automatically allocated when the system functions as a client to initiate a connection):

   ```
   netsh int ipv4 set dynamicportrange tcp start=49152 num=16384
   ```

3. Go to the Agent installation directory, double-click the **shutdown.bat** script to stop the Agent, and then run the **start.bat** script to start the Agent.
   - Earlier version: The Agent is installed in the directory **C:\Program Files \telescope**.
   - New version: The default Agent installation path is **C:\Program Files \uniagent\extension\install\telescope**.

2.2.2 What Should I Do If the Agent Is in the Agency Configuration Error State?

Symptom

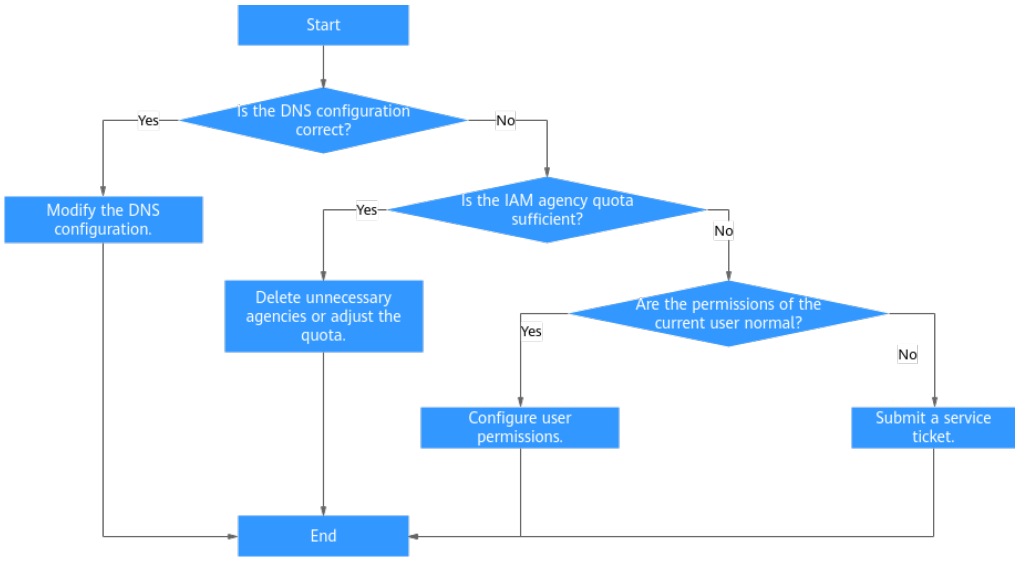
After the Agent is installed, the Agent is in the **Agency configuration error** state.

Possible Causes

If the Agent is in the **Agency configuration error** state, select the corresponding ECS and click **Restore Agent Configurations** above the host list. If the fault persists, see **Figure 2-4** for troubleshooting.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Figure 2-4 Troubleshooting method



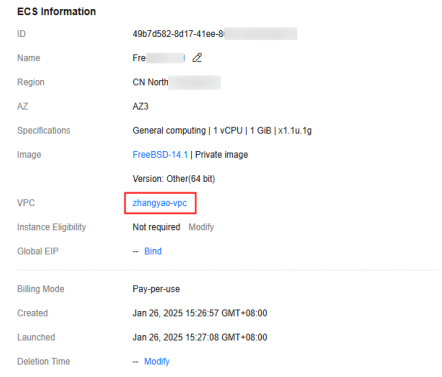
Cause 1: Incorrect DNS Configuration

To view and modify the DNS configuration, perform the following steps:

1. Log in to the **ECS console**.
2. On the ECS console, click the name of an ECS to view its details.
3. In the ECS information area, click the VPC name.

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

   Figure 2-5 ECS information

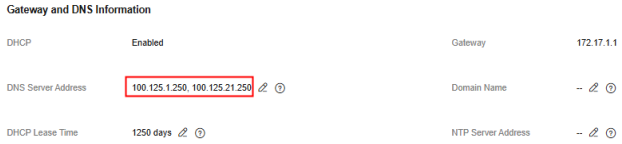
4. Locate the target VPC and click the number of subnets.
5. In the subnet list, click the name of the target subnet.
6. In the **Gateway and DNS Information** area, check whether the DNS server address is the same as the private DNS server address provided by Huawei Cloud.

   For details about how to obtain the DNS server addresses of different regions, see **What Are Huawei Cloud Private DNS Server Addresses?**

   - If they are the same, as shown in **Figure 2-6**, you do not need to change the DNS server addresses.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

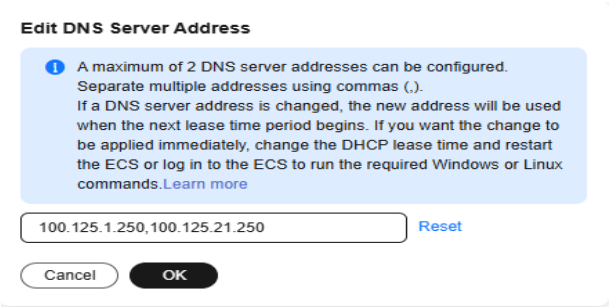
Figure 2-6 Viewing the DNS server address



- If they are different, perform steps 7 to 10 to change the DNS server address.

7. Click  next to **DNS Server Address**.
8. Enter the DNS server address. Use commas (,) to separate multiple IP addresses.

Figure 2-7 Changing DNS server addresses



9. Click **OK**.
10. Restart the ECS or BMS. For details, see **Restarting an ECS** or **Restarting a BMS**.

For more information about how to configure DNS, see **Checking/Modifying the DNS and Security Group Configurations**.

Cause 2: Insufficient IAM Agency Quota

1. Log in to the **IAM console**.
2. On the IAM console, choose **Agencies**.
3. Check the following information:
   - Whether the CESAgentAutoConfigAgency agency exists.
   - Whether the used quota of the IAM agencies has reached the upper limit. For details, see **Quotas**.
4. If the CESAgentAutoConfigAgency agency does not exist and the agency quota has been used up, delete unnecessary agencies or apply for a higher quota, and then restore the Agent configuration again.

Cause 3: Insufficient User Permissions

1. Log in to the **IAM console**.
2. In the navigation pane, click **User Groups**.
3. Click the name of the user group to which the account belongs.
4. On the **Permissions** tab page, view the permissions of the user group.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

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

Submitting a Service Ticket

If the problem persists, **submit a service ticket**.

2.2.3 What Should I Do If the Agent Is Faulty?

Network Issues

- The domain name of the Agent cannot be resolved. Check whether the DNS server address and security group rules are correct by referring to **Checking/Modifying the DNS and Security Group Configurations**. If they are, check whether the Agent configuration is correct by referring to **(Optional) Manually Configuring the Agent**.
- If the DNS server is not a Huawei Cloud DNS server, run the **dig** *domain-name* command to obtain the IP address of **agent.ces.myhuaweicloud.com** resolved by the Huawei Cloud DNS server over the intranet, and then add the IP address to the corresponding **hosts** file. For details, see **What Are Huawei Cloud Private DNS Server Addresses?**

Time Synchronization Issue

The server time is inconsistent with the local standard time. If the server time is not synchronized with the standard time, the authentication may fail. As a result, the monitoring Agent reports a fault.

Authorization and Billing Issue

The account is in arrears. If the account is in arrears, the service provider may restrict access to the service. As a result, the Agent cannot work properly.

Process and System Faults

- The Agent process is faulty. Restart it by referring to **Managing the Agent**. If the Agent process cannot be restarted, related files are deleted by mistake. In this case, reinstall the Agent.

Other Causes

When the Agent is faulty, you can view the log file to obtain more detailed error information. The log file path varies depending on the Agent version and the OS.

- 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**

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

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

2.2.4 What Should I Do If the Agent Status Switches Between Running and Faulty?

Symptom

If the Cloud Eye Agent status switches between **Running** and **Faulty**, the Agent may be overloaded and unstable.

Constraints

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

- Linux:
  a. Log in to the server as user **root**.
  b. 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 returned, the earlier version of the Agent is used. Perform operations by referring to the instructions of the earlier version.
    - If a version is returned, the new version of the Agent is in use. Perform operations by referring to the instructions of the new version.
    - If **0** is returned, the Agent is not installed.
- Windows: Determine the Agent version based on the installation path. Default installation paths:
  – New version: **C:\Program Files\uniagent\extension\install\telescope**
  – Earlier version: **C:\Program Files\telescope**

Possible Causes

To prevent the Agent from being overloaded and affecting other services on servers, Cloud Eye provides a circuit breaker mechanism when the CPU or memory usage of the Agent is too high. When the Agent is overloaded, the circuit breaker mechanism is automatically triggered. After that, the Agent stops working and does not report monitoring data.

Circuit Breaker Principles

By default, the Agent detection mechanism is as follows:

The system checks whether the Agent process exceeds the second threshold (CPU usage exceeds 30% or memory usage exceeds 700 MB) every minute. If either the CPU or memory usage exceeds the second threshold, the Agent process exits. If the second threshold is not exceeded, the system checks whether the Agent

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

process exceeds the first threshold (CPU usage exceeds 10% or memory usage exceeds 200 MB). If the first threshold is exceeded for three consecutive times, the Agent process exits and the event is 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 **Solution** to trigger the circuit-breaker pattern according to the actual resource usages.

Solution

1. Log in to the ECS or BMS where the Agent does not report data.
2. **Optional:** 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 2-1 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 (%).	

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Parameter	Description	How to Query Parameter Values
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. In the **manifest.json** file, modify **mem** and **cpuUsage** in **resourceLimit**. There are three groups of parameters. 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
    }
  }
]
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 2-2 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
```

2.3 Monitored Data Exceptions

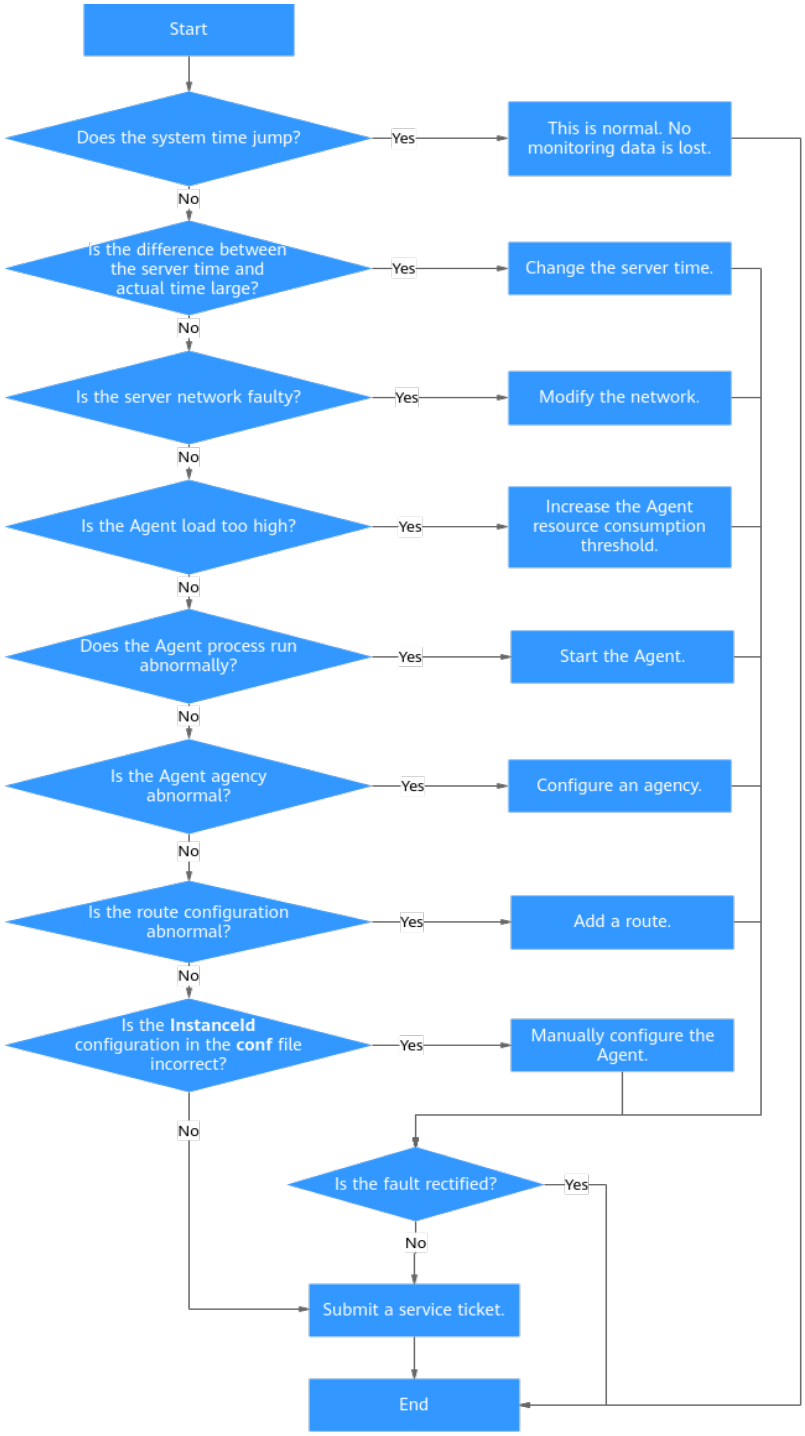
2.3.1 What Should I Do If the Agent Status Is Running But Monitoring Data Is Missing?

Symptom

After the Agent is installed and configured, no OS monitoring data is displayed after 3 to 5 minutes, or the OS monitoring data generated in some time periods is missing. For details, see **Figure 2-8**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Figure 2-8 Troubleshooting method



System Time Jump

The collection time of the Cloud Eye Agent is subject to the OS time of the ECS. If the system clock jumps discontinuously and sharply (forward or backward) within a short period of time, instead of changing smoothly, it may appear that data points are lost (time changes due to time synchronization). However, the collection points are not lost.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Large Difference Between the Server Time and Actual Time

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. For details about how to rectify the fault, see **Does Huawei Cloud Provide the NTP Server and How Can I Configure It?**

Server Network Exception

Check whether the current **Server Monitoring** page is of the earlier or new version.

- If the **Restore Agent Configurations** button is displayed above the server list on the **Server Monitoring** page, the page is of the earlier version. The earlier version page supports only the installation of the earlier version Agent. For details, see **Agent of the Earlier Version**.
- If the **Restore Agent Configurations** button is not displayed, the page is of the new version. Check the current Agent version by referring to **Checking the Cloud Eye Agent Version**. If the Agent is of the earlier version, upgrade it to the new version by referring to **Upgrading the Agent**. If the fault persists, see **Agent of the New Version** for troubleshooting.

Agent of the Earlier Version

1. Log in to the server and obtain the endpoint from the Agent configuration file.
   - For Linux, run the following command:
     ```
     cat /usr/local/telescope/bin/conf_ces.json
     ```
   - For Windows, open the **bin/conf_ces.json** configuration file in the directory where the Agent installation package is stored.
2. Check whether the endpoint in the Agent configuration file is the same as that of the current region. For details about Cloud Eye endpoints for each region, see **Regions and Endpoints**.

   The following uses CN North-Beijing4 as an example to describe the endpoint in the **conf_ces.json** configuration file.

   {"Endpoint":"https://ces.cn-north-4.myhuaweicloud.com"}
   - If yes, go to the next step.
   - If no, modify the endpoint in the configuration file.
3. Run the following command to check whether the DNS resolution is normal:
   ```
   ping {Endpoint}
   ```
   Take CN North-Beijing4 as an example. The command is as follows:
   ```
   ping ces.cn-north-4.myhuaweicloud.com
   ```
4. If a message is displayed indicating that the network is abnormal, check and modify the DNS configuration by referring to **Checking/Modifying the DNS and Security Group Configurations**.

Agent of the New Version

1. Run the following command to check whether the DNS resolution is normal:
   ```
   ping agent.ces.myhuaweicloud.com
   ```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

2. If a message is displayed indicating that the network is abnormal, check and modify the DNS configuration by referring to **Checking/Modifying the DNS and Security Group Configurations**.

High Agent Load

For the Agent of the new version, when the Agent load is too high, the circuit breaker mechanism may be triggered. After the circuit breaker is triggered, the system stops collecting server metrics and attempts to restart the Agent within 5 minutes. As a result, monitoring data may be missing. For more information, see **What Is the Circuit Breaker Mechanism of the Agent?** To locate and rectify the fault, perform the following steps:

1. Log in to the server.
2. Check whether the **ces.log** file contains information about high Agent load. If no, go to step **3**. If yes, go to step **4**.
   - For Linux, run the following command:
     ```
     grep "Agent will exit due to fuse protection" /usr/local/uniagent/extension/install/telescope/log/ces.log
     ```
   - For Windows, open the **ces.log** file and search for "Agent will exit due to fuse protection". The log path is as follows:
     ```
     "C:\Program Files\uniagent\extension\install\telescope\log"
     ```
3. Check whether the **uniagent.log** file contains information about high Agent load. If no, the Agent load is normal. If yes, go to step **4**.
   - For Linux, run the following command:
     ```
     grep "telescope has occurred for 3 times" /usr/local/uniagent/log/uniagent.log
     ```
   - For Windows, open the **ces.log** file and search for "telescope has occurred for 3 times". The log path is as follows:
     ```
     "C:\Program Files\uniagent\log"
     ```
4. Increase the Agent resource usage threshold by referring to **How Do I Change the Agent Resource Usage Threshold by Modifying the Configuration File?**

Abnormal Agent Process

1. Check the Agent version installed on the server. For details, see **Checking the Cloud Eye Agent Version**.
2. Log in to the server and check whether the Agent process is running properly. For details, see **Checking the Agent Status**.
   ```
   ps -ef |grep telescope
   ```
3. If the Agent is abnormal, start the Agent by referring to **Starting the Agent**.

Abnormal Agent Agency

Check whether the current **Server Monitoring** page is of the earlier or new version.

- If the **Restore Agent Configurations** button is displayed above the server list on the **Server Monitoring** page, the page is of the earlier version. The earlier version page supports only the installation of the earlier version Agent. For details, see **Agent of the Earlier Version**.
- If the **Restore Agent Configurations** button is not displayed, the page is of the new version. Check the Agent version of the server by referring to **Checking the Cloud Eye Agent Version**. If the Agent is of the earlier version,

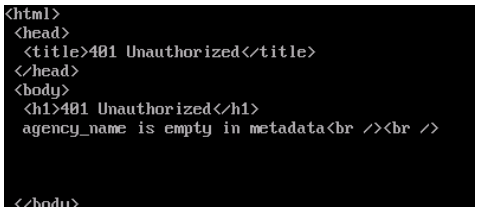
 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

upgrade it to the new version. If the fault persists, see **Agent of the New Version** for troubleshooting.

Server Monitoring (Earlier Version)

1. Check whether the cloud server agency has been created.
   - Linux: Log in to the server and run the following command. If the command fails to be executed or the command output shown in **Figure 2-9** is displayed, the agency is abnormal.
     ```
     curl http://169.254.169.254/openstack/latest/securitykey
     ```

     Figure 2-9 AK/SK acquisition failure

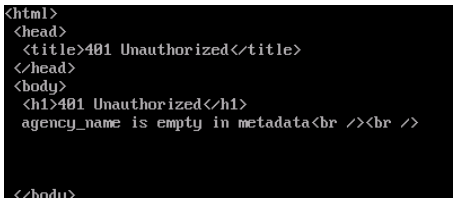
     

   - Windows: Access the following address. If the access fails, the agency is abnormal.
     ```
     http://169.254.169.254/openstack/latest/meta_data.json
     ```
2. Go to the **Server Monitoring** page, select the target server, and click **Restore Agent Configurations** above the list.

Server Monitoring (New Version)

1. Check whether the cloud server agency has been created.
   - Linux: Log in to the server and run the following command. If the command fails to be executed or the command output shown in **Figure 2-10** is displayed, the agency is abnormal.
     ```
     curl -ivk https://agent.ces.myhuaweicloud.com/v1.0/agencies/cesagency/securitykey
     ```

     Figure 2-10 AK/SK acquisition failure

   - Windows

     Log in to the **IAM console**, choose **Agencies**, and search for **cesagency**. Click the agency name. In the **Permissions** area, check whether the value of **Project [Region]** of the CES AgentAccess permission contains the current region. If the current region is not contained, the agency is abnormal.
2. Log in to the **IAM console**, choose **Agencies**, and search for the **cesagency** agency.
3. Locate the row that contains **cesagency** and click **Authorize** in the **Operation** column.
4. On the **Authorize Agency** page, search for and select **CES Administrator**, and click **Next**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

5. Configure the authorization scope and click **OK**.

Abnormal Route Configuration

1. Run the following command to check the route:
   - Linux
     ```
     route -n
     ```
     If the following information is displayed, the route is normal.

     Figure 2-11 Normal route configuration (Linux)

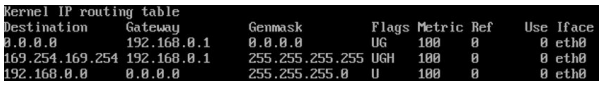
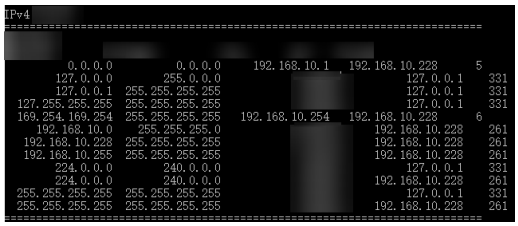
     
     ```
     Kernel IP routing table
     Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
     0.0.0.0         192.168.0.1     0.0.0.0         UG    100    0        0 eth0
     169.254.169.254 192.168.0.1     255.255.255.255 UGH   100    0        0 eth0
     192.168.0.0     0.0.0.0         255.255.255.0   U     100    0        0 eth0
     ```
   - Windows
     ```
     route print
     ```
     If the following information is displayed, the route is normal:

     Figure 2-12 Normal route configuration (Windows)

     
     ```
     IPv4
     ===========================================================================
     [redacted]
     ===========================================================================
     Persistent Routes:
       Network Address          Netmask  Gateway Address  Metric
     ===========================================================================
     ```
2. If the route does not exist, run the following command to add a route:
   - Linux
     ```
     route add -host 169.254.169.254 gw 192.168.0.1
     ```
   - Windows
     ```
     route add 169.254.169.254 mask 255.255.255.255 192.168.0.1
     ```

   NOTE

   Replace *192.168.0.1* in the example command with the gateway of the server.

Incorrect InstanceId Configuration in the conf File

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

Check whether the configuration is correct by referring to **(Optional) Manually Configuring the Agent** in the *Cloud Eye User Guide*.

Submitting a Service Ticket

If the problem persists, **submit a service ticket**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

2.3.2 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

2.3.3 Why Are the Inbound Bandwidth and Outbound Bandwidth Negative?

If Docker is installed, the earlier 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 for the difference between the last and current monitoring periods.

To update the Agent, see **Managing the Agent**.

2.3.4 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**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.



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
```

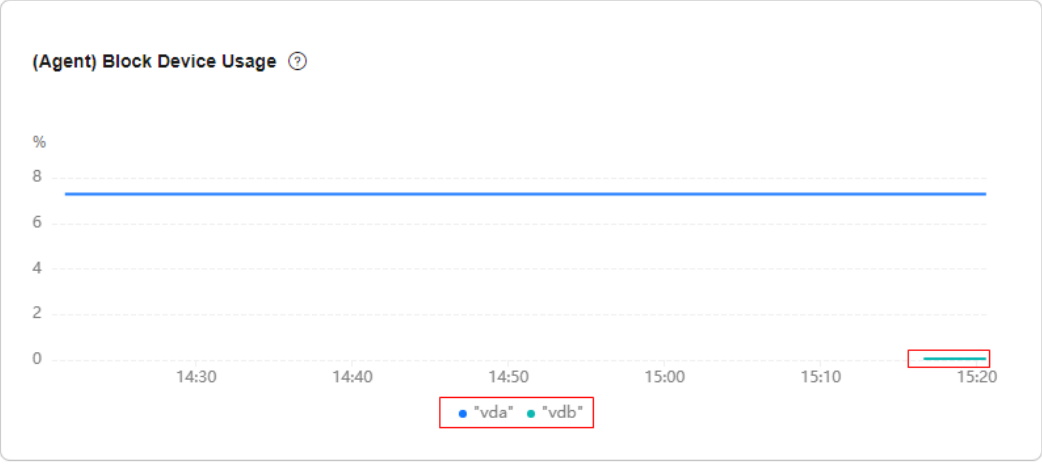
Procedure

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.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.



2.3.5 What Should I Do If the Disk I/O Usage of the Linux OS Is Incorrect?

Symptom

After the kernel of the Linux OS is upgraded from 3.10.0 to 4.19.12, the value of the **(Agent) Disk I/O Usage** metric is inaccurate and increases abnormally.

Possible Causes

The Linux 4.19 kernel updated the **/proc/diskstats** statistical method. This change caused errors in calculating disk I/O usage with the old method and also affected system commands such as **iostat** and **sar**. For details about the calculation method, see **What Metrics Are Supported by the Agent?**

This issue specifically affects Linux 4.19 and 4.20. Disk I/O calculations remain accurate for other versions. The new method aligns with industry standards and matches the results produced by the **iostat** command.

Procedure

Upgrade or roll back the OS kernel.

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

In some regions, the basic and enhanced editions of the Agent have been merged. If both the basic and enhanced editions of the Agent are available in your region, the following situation may occur:

If no data is displayed for GPU, NPU, DAVP, or RoCE monitoring when you view server monitoring metrics, check whether your server supports these types of metrics by referring to **What Are Environment Constraints for GPU Monitoring?** If your server supports them and the driver is running properly, upgrade the Agent to the enhanced edition.

Step 1 Uninstall the Agent of the basic edition.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

- Linux: Log in to the server and run the following command:
  ```
  bash /usr/local/uniagent/script/uninstall.sh
  ```
- 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 2-3 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.
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.

2.3.7 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**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

3 Cloud Service Monitoring

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

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

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

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**.

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

Possible causes are as follows:

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

- 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 3 hours, the cloud service will not be displayed in the cloud service monitoring list. However, for services like APIG, OBS, FunctionGraph, DIS, DataArts Studio, Live, and SFS, their monitoring data will be retained for seven days.

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.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

4 Alarm Management

4.1 When Will an Alarm Rule Trigger an Insufficient Data Alarm?

4.2 How Do I Handle an Insufficient Data Alarm Generated After a Resource Is Deleted?

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

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

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

4.6 What Can I Do If an Error Is Reported When I Configure Tags?

4.1 When Will an Alarm Rule Trigger an Insufficient Data Alarm?

Prerequisites

- You have created an alarm rule with **No-Data Processing** set to **Generate no-data alarms** in **Advanced Settings**.
- An alarm triggered by the alarm rule already exists in the alarm records and is not in the **Expired** state.

Triggering Mechanism

1. Triggering condition

   If a metric configured in the alarm rule does not report data for three consecutive hours, the system determines whether to generate an alarm indicating insufficient data.

2. Resource and metric matching verification

   The system checks whether the resource and metric whose monitoring data is not reported match the existing alarm records (with the same abnormal

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

resource and alarm policy metric). The following status transition logic is executed only when they are matched.

3. Status transition logic

   The system performs the following operations based on the current status of the matched existing alarm record:

   - If the status is **Resolved** or **Resolved (forcible clear)**, the system considers the fault as a new one and adds an **Insufficient data** alarm.
   - If the status is **Alarm**, the system considers that the fault persists and updates the status of the existing alarm record to **Insufficient data**.
   - If the status is **Insufficient data**, the system considers that the status remains unchanged and does not perform any operation. This prevents the same alarm from being generated repeatedly and reduces interference caused by invalid alarms.

NOTE

Generally, if a cloud service metric does not report data for three consecutive hours, the data is considered insufficient. If the reporting period of a metric is longer than three hours and no monitoring data is reported for three consecutive periods, the data is also considered insufficient.

4.2 How Do I Handle an Insufficient Data Alarm Generated After a Resource Is Deleted?

Symptom

After you delete a cloud service resource, the status of an alarm generated for the resource remains **Insufficient data** in the alarm records.

Possible Causes

An **Insufficient data** alarm is triggered when the monitoring data is interrupted for a period longer than the specified one. This alarm is used to notify you of data collection exceptions.

After you delete a cloud service resource, the alarm rules configured for the resource in Cloud Eye remain effective. Because the resource has been deleted, no monitoring data is reported. Generally, an **Insufficient data** alarm is generated when no monitoring data is reported for the metric configured in an alarm rule for three consecutive hours. For details, see **When Will an Alarm Rule Trigger an Insufficient Data Alarm?**

Data reporting cannot be restored for deleted resources, and the system lacks a signal for data restoration. Therefore, the alarm cannot be automatically cleared.

Impact

If an alarm remains in the **Insufficient data** state for a long time, it keeps drawing O&M attention and may be mistakenly considered a real fault, interfering with routine O&M.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Solution

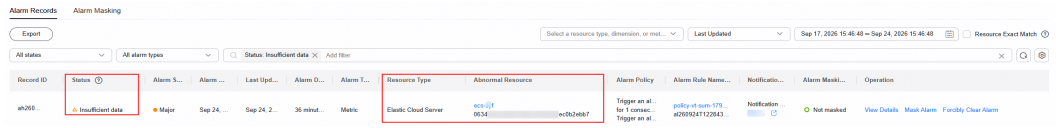
1. Log in to the **Cloud Eye console**.
2. In the navigation pane, choose **Alarm Management** > **Alarm Handling**. The **Alarm Records** page is displayed.

   NOTE

   In some regions, the path is **Alarm Management** > **Alarm Records**.
3. In the alarm list, locate the target alarm whose status is **Insufficient data**.

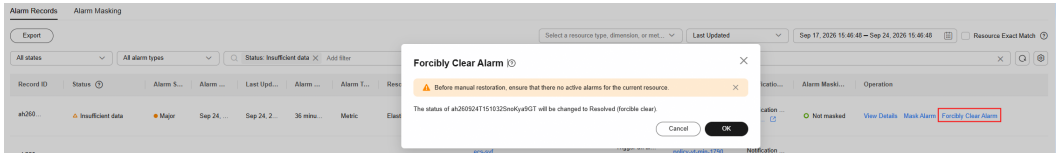
   You can check whether the alarm is generated for a deleted resource based on the **Resource Type** and **Abnormal Resource** information in the alarm list.

   Figure 4-1 Insufficient data alarm

4. Click **Forcibly Clear Alarm** in the **Operation** column of the alarm record. The **Forcibly Clear the Alarm** dialog box is displayed.

   Figure 4-2 Forcibly clearing an alarm

5. Click **OK**.

   In the alarm record list, the status of the alarm record will be updated to **Resolved (forcible clear)**. Subsequent O&M will not be affected.

Preventive Measures

1. Before deleting a resource, if you do not need to pay attention to its alarms, you can delete or disable the alarm rules associated with the resource. For details about how to delete an alarm rule, see **Deleting Alarm Rules**. For details about how to disable an alarm rule, see **Disabling Alarm Rules**.
2. After releasing resources in batches, check whether there are associated alarm rules and clear them in a timely manner.

4.3 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.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

4.4 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.

4.5 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**.

4.6 What Can I Do If an Error Is Reported When I Configure Tags?

Symptom

- When you create or modify an alarm rule, the system displays a message indicating that the API for verifying tag compliance fails to be called or the tenant does not have sufficient permissions.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

- When you add a tag to an alarm rule, the system displays a message indicating that the API for verifying tag compliance fails to be called or the tenant does not have sufficient permissions.
- When you search for resources by resource tag or manage resource tags on the Tag Management Service (TMS) console, the system displays a message indicating that the API for verifying tag compliance fails to be called or the tenant does not have sufficient permissions.

Procedure

1. Log in to the **new IAM console**.
2. In the navigation pane, choose **Users**.
3. In the user list, locate your username and click **Authorize** in the **Operation** column.
4. On the **Authorize User** page, select an assignment mode and identity policy.
   - Set **Assign By** to **Identity policy**.
   - For **Identity Policy**, select **CESServiceFullAccessPolicy** or customize one.
5. (Optional) Customize an identity policy. If you have selected **CESServiceFullAccessPolicy** for **Identity Policy**, skip this step.
   a. Click **Create** next to **Identity Policy**.
   b. On the **Create Identity Policy** page, enter a policy name.
   c. Set **Policy View** to **JSON**.
   d. Enter the policy content as follows:

```
{
 "Version": "5.0",
 "Statement": [
  {
   "Effect": "Allow",
   "Action": [
    "ces:tags:create",
    "ces:tags:listResources"
   ]
  }
 ]
}
```

   e. Click **OK**.
   f. On the **Authorize User** page, search for and select the created custom identity policy.
6. Click **OK**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

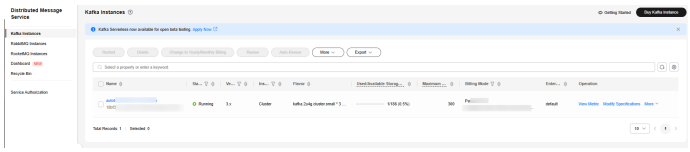
5 Data Dump

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

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. **Insufficient agency permissions**: If the destination is **Other account**, and the agency does not have sufficient permissions, data dump will fail on Cloud Eye. In this case, you need to confirm that the agency has **all necessary permissions**. If not, add them again.
3. **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.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

6 API

6.1 How Can I Query Monitoring Data of Multiple Metrics?

6.2 How Can I Query Monitoring Data of a Metric?

6.3 What Should I Do If I Do Not Have the Programmatic Access Permission When Calling an API?

6.1 How Can I Query Monitoring Data of Multiple Metrics?

FAQ Before API Calling

1. Issue 1

   Description

   How can I call the POST /V1.0/{*project_id*}/batch-query-metric-data API?

   Solution

   Rectify the fault by following the instructions provided in **Querying Monitoring Data of Multiple Metrics**.

2. Issue 2

   Description

   What is the maximum query time range supported when I call the POST /V1.0/{project_id}/batch-query-metric-data API?

   Solution

   The maximum query range is 155 days.

3. Issue 3

   Description

   What are the domain names for calling this API in different regions?

   Solution

   For details, see **Regions and Endpoints**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

FAQ During API Calling

1. Issue 1

   Description

   The response status code is 200 and no metric data is returned. Example response:

```
{
   "metrics": [{
      "namespace": "SYS.RDS",
      "metric_name": "rds039_disk_util",
      "dimensions": [{
         "name": "instance_id",
         "value": "5e319882ffa04c968e469035a116b2d1in04"
      }],
      "datapoints": [],##No metric data is displayed in the data points.
      "unit": "unknown"
   }]
}
```

   Possible causes

   - Cause 1: The namespace of the cloud service is incorrect. For details, see Case 1.
   - Cause 2: The requested resource cannot be found. For details, see Case 2.
   - Cause 2: The dimension is not applicable to the cloud service. For details, see Case 3.
   - Cause 3: The metric ID is not applicable to the cloud service. For details, see Case 4.

   Solution

   For details about the namespaces, dimensions, and metrics, see **Services Interconnected with Cloud Eye**.

   Case 1 : **The namespace of the cloud service is incorrect.**

   The namespace corresponding to the metric **mem_usedPercent** is **AGT.ECS**.

   Request parameters

```
{
   "from": 1724311893283,
   "to": 1724315493283,
   "period": "1",
   "filter": "average",
   "metrics": [{
      "dimensions": [{
         "name": "instance_id",
         "value": "129718f5-833d-4f78-b685-6b1c3091ea6"
      }],
      "metric_name": "mem_usedPercent",
      "namespace": "SYS.ECS"  ##Incorrect namespace
   }]
}
```

   Response parameters

```
{
   "metrics": [{
      "namespace": "SYS.ECS",
      "metric_name": "mem_usedPercent",
      "dimensions": [{
         "name": "instance_id",
         "value": "129718f5-833d-4f78-b685-6b1c3091ea6"
      }],
      "datapoints": [],
      "unit": "unknown"
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
    }]
}
```

Case 2 : The requested resource cannot be found.

The instance **129718f5-833d-4f78-b685-6b1c3091ea7** is not in the ECS list.

Request parameters

```
{
    "from": 1724311893283,
    "to": 1724315493283,
    "period": "1",
    "filter": "average",
    "metrics": [{
        "dimensions": [{
            "name": "instance_id",
            "value": "129718f5-833d-4f78-b685-6b1c3091ea7"  ##129718f5-833d-4f78-b685-6b1c3091ea7 is not in the ECS list.
        }],
        "metric_name": "mem_usedPercent",
        "namespace": "AGT.ECS"
    }]
}
```

Response parameters

```
{
    "metrics": [{
        "namespace": "AGT.ECS",
        "metric_name": "mem_usedPercent",
        "dimensions": [{
            "name": "instance_id",
            "value": "129718f5-833d-4f78-b685-6b1c3091ea6"
        }],
        "datapoints": [],
        "unit": "unknown"
    }]
}
```

Case 3: The dimension is not applicable to the cloud service.

instance_id is not a dimension of RDS.

Request parameters

```
{
    "metrics": [{
        "dimensions": [{
            "name": "instance_id", ##instance_id is not a dimension of RDS.
            "value": "5e319882ffa04c968e469035a116b2d1in04"
        }],
        "metric_name": "rds039_disk_util",
        "namespace": "SYS.RDS"
    }],
    "filter": "average",
    "period": "1",
    "from": 1724312777938,
    "to": 1724316377938
}
```

Response parameters

```
{
    "metrics": [{
        "namespace": "SYS.RDS",
        "metric_name": "rds039_disk_util",
        "dimensions": [{
            "name": "instance_id",
            "value": "5e319882ffa04c968e469035a116b2d1in04"
        }],
        "datapoints": [],
        "unit": "unknown"
    }]
}
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Case 4: The metric ID is not applicable to the cloud service.

The **rds958_disk_util** metric ID is not applicable to RDS.

Request parameters

```
{
   "metrics": [{
      "dimensions": [{
         "name": "rds_cluster_sqlserver_id",
         "value": "5e319882ffa04c968e469035a116b2d1in04"
      }],
      "metric_name": "rds958_disk_util",   ##The rds958_disk_util metric ID is not applicable to RDS.
      "namespace": "SYS.RDS"
   }],
   "filter": "average",
   "period": "1",
   "from": 1724312777938,
   "to": 1724316377938
}
```

Response parameters

```
{
   "metrics": [{
      "namespace": "SYS.RDS",
      "metric_name": "rds958_disk_util",
      "dimensions": [{
         "name": "rds_cluster_sqlserver_id",
         "value": "5e319882ffa04c968e469035a116b2d1in04"
      }],
      "datapoints": [],
      "unit": "unknown"
   }]
}
```

2. Issue 2

Description

The response status code is 200, and no data of the ECS disk usage is returned.

Example response:

```
{
   "metrics": [{
      "namespace": "AGT.ECS",
      "metric_name": "disk_usedPercent",
      "dimensions": [{
         "name": "disk",
         "value": "012bec14bc176310c19f40e384fd629b"
      }, {
         "name": "instance_id",
         "value": "07d878a9-2243-4e84-aeef-c47747d18024"
      }],
      "datapoints": [],  ##No metric data is displayed in the metric data list.
      "unit": "unknown"
   }]
}
```

Possible causes

Cause 1: The namespace is incorrect. For details, see Case 1.

Cause 2: The metric dimension is incorrect. For details, see Case 2.

Cause 3: The Agent is not installed on the ECS. For details, see Case 3.

Cause 4: The Agent installed on the ECS does not report the disk usage. For details, see Case 4.

Case 1: incorrect namespace

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

If the OS monitoring metrics of an ECS are queried, the namespace must be **AGT.ECS**.

Request parameters

```
{
   "from": 1724118017498,
   "to": 1724121617498,
   "period": "1",
   "filter": "average",
   "metrics": [{
      "dimensions": [{
         "name": "instance_id",
         "value": "07d878a9-2243-4e84-aeef-c47747d18024"
      }, {
         "name": "mount_point",
         "value": "012bec14bc176310c19f40e384fd629b"
      }],
      "metric_name": "disk_usedPercent",
      "namespace": "SYS.ECS"  ##Incorrect namespace
   }]
}
```

Response parameters

```
{
   "metrics": [{
      "namespace": "SYS.ECS",
      "metric_name": "disk_usedPercent",
      "dimensions": [{
         "name": "mount_point",
         "value": "012bec14bc176310c19f40e384fd629b"
      }, {
         "name": "instance_id",
         "value": "07d878a9-2243-4e84-aeef-c47747d18024"
      }],
      "datapoints": [],
      "unit": "unknown"
   }]
}
```

Case 2: incorrect metric dimension

The disk usage is queried by mount point. Two dimensions: **instance_id** and **mount_point** are required in the request parameters for querying the disk usage.

Request parameters

```
{
   "from": 1724118017498,
   "to": 1724121617498,
   "period": "1",
   "filter": "average",
   "metrics": [{
      "dimensions": [{
         "name": "instance_id",
         "value": "07d878a9-2243-4e84-aeef-c47747d18024"
      }, {
         "name": "disk," ## Incorrect metric dimension
         "value": "012bec14bc176310c19f40e384fd629b"
      }],
      "metric_name": "disk_usedPercent",
      "namespace": "AGT.ECS"
   }]
}
```

Response parameters

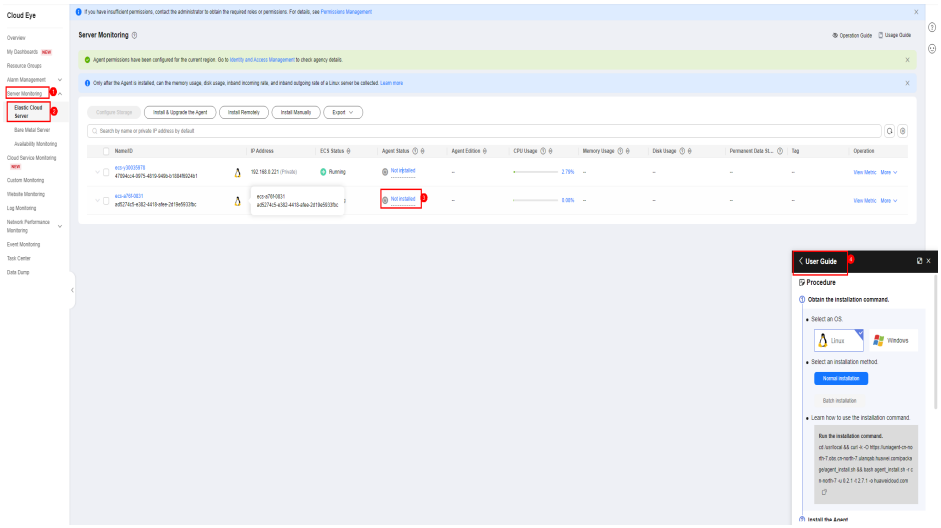
```
{
   "metrics": [{
      "namespace": "AGT.ECS",
      "metric_name": "disk_usedPercent",
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
        "dimensions": [{
            "name": "disk",
            "value": "012bec14bc176310c19f40e384fd629b"
        }, {
            "name": "instance_id",
            "value": "07d878a9-2243-4e84-aeef-c47747d18024"
        }],
        "datapoints": [],
        "unit": "unknown"
    }]
}
```


Case 3: The Agent is not installed on an ECS.

On the Cloud Eye console, choose **Server Monitoring** > **Elastic Cloud Server** in the navigation pane. Locate the ECS and click **Not installed** in the **Agent Status** column. Then install the Agent as instructed.



Case 4: The Agent installed on the ECS does not report the disk usage.

The Agent is faulty, so there is no metric data reported. For details, see **Troubleshooting Common Agent Issues**.

3. Issue 3

Description

The number of metric data records reported within a specified time range is greater than 3,000. However, the number of returned metric data records is less than 3,000 when the current API is called.

Possible causes

The default maximum query interval (**to**–**from**) varies depending on **period** and the number of metrics to be queried. The rule is as follows: The number of metrics × (**to** - **from**)/Monitoring interval ≤ 3000.

NOTE

- The number of metrics: the number of elements in the **metrics** attribute, a request parameter
- Monitoring period: value of the **period** attribute in the request. The unit is minute by default and needs to be converted into milliseconds.
- **3000**: the total number of all data points (the metric data list) in the response body

Cause 1: If the metric reporting period is shorter than the monitoring period for querying monitoring data of multiple metrics, multiple metrics reported

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

during the monitoring period are aggregated into a point based on the aggregation rule. As a result, the queried metric data volume is less than the reported data volume.

Cause 2: If the metric reporting period is the same as the monitoring period for querying monitoring data of multiple metrics, a maximum of 3,000 metric data records can be returned according to the preceding calculation rule.

Solution

a. Set the monitoring period in the request parameters to a smaller value based on the enumerated values provided in the API reference.
b. Use the API for querying monitoring data of a single metric. This API has no limit on the number of returned metric data records.

4. Issue 4

Description

When the API for querying monitoring data of multiple metrics is called, the time taken for returning the metric data points is much greater than the value of the **from** parameter in the request.

Possible causes

The default maximum query interval (**to**–**from**) varies depending on **period** and the number of metrics to be queried. The rule is as follows: The number of metrics × (**to** - **from**)/Monitoring interval ≤ 3000.

NOTE

- The number of metrics: the number of elements in the **metrics** attribute, a request parameter
- Monitoring period: value of the **period** attribute in the request. The unit is minute by default and needs to be converted into milliseconds.
- **3000**: the total number of all data points (the metric data list) in the response body

For example, if 300 metrics are queried in batches and the monitoring interval is 60,000 ms, the maximum value of (**to**-**from**) is **600000**. If (**to-from**) exceeds 600,000, **from** is automatically changed to **to-600000**.

Cause 1: According to the preceding formula, the number of metrics is too large. For details, see Case 1.

Cause 2: According to the preceding formula, the monitoring period is too short. For details, see Case 1.

Solution

Cause 1: There are too many metrics.

Solution: Reduce the number of metrics.

Use the API for querying monitoring data to query a single metric.

Cause 2: A small enumerated value for the monitoring period is selected.

Solution: Set the monitoring period in the request parameter to a large enumerated value provided in the API reference.

Case 1: too many metrics and short monitoring period

If the number of requested metrics is 300 and the monitoring period is 1 minute, the maximum value of (**to** - **from**) is 600000. If the value of the request parameter (**to** – **from**) is 3600000 (1724742027556 – 1724738427556), which exceeds the value of 600000, the value of **from** is

automatically changed to "**to** – 600000", that is, 1724742027556 – 600000 = 1724741427556.

The earliest metric data point returned by the API within the specified time range is **2024-08-27 14:51:27**, but the query start time is **2024-08-27 14:00:27**.

Request parameters

```
{
 "metrics": [
  {
   "dimensions": [
    {
     "name": "disk_name",
     "value": "6a2bf14a-e3be-4fc9-8522-ba6fe7f0b503-vda"
    }
   ],
   "metric_name": "disk_device_read_bytes_rate",
   "namespace": "SYS.EVS"
  },
  {
   "dimensions": [
    {
     "name": "disk_name",
     "value": "6a2bf14a-e3be-4fc9-8522-ba6fe7f0b503-vdc"
    }
   ],
   "metric_name": "disk_device_read_bytes_rate",
   "namespace": "SYS.EVS"
  },
  {
   "dimensions": [
    {
     "name": "disk_name",
     "value": "6a2bf14a-e3be-4fc9-8522-ba6fe7f0b503-vda"
    }
   ],
   "metric_name": "disk_device_write_bytes_rate",
   "namespace": "SYS.EVS"
  },
  {
   "dimensions": [
    {
     "name": "disk_name",
     "value": "6a2bf14a-e3be-4fc9-8522-ba6fe7f0b503-vdc"
    }
   ],
   "metric_name": "disk_device_write_bytes_rate",
   "namespace": "SYS.EVS"
  },
  ......
  {
   "dimensions": [
    {
     "name": "nat_gateway_id",
     "value": "3c55363f-6416-45ca-8512-cf1f6f2533e7"
    }
   ],
   "metric_name": "inbound_pps",
   "namespace": "SYS.NAT"
  }
 ],
 "filter": "max",
 "period": "1",
 "from": 1724738427556, ##2024-08-27 14:00:27
 "to": 1724742027556 ##2024-08-27 15:00:27
}
```

Response parameters

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
{
   "metrics": [
      {
         "namespace": "SYS.EVS",
         "metric_name": "disk_device_read_bytes_rate",
         "dimensions": [
            {
               "name": "disk_name",
               "value": "6a2bf14a-e3be-4fc9-8522-ba6fe7f0b503-vda"
            }
         ],
         "datapoints": [
            {
               "max": 0,
               "timestamp": 1724741487000  ##2024-08-27 14:51:27
            },
            {
               "max": 0,
               "timestamp": 1724741547000  ##2024-08-27 14:52:27
            },
            {
               "max": 0,
               "timestamp": 1724741607000
            },
            {
               "max": 0,
               "timestamp": 1724741667000
            },
            {
               "max": 0,
               "timestamp": 1724741727000
            },
            ......
         ],
         "unit": "B/s"
      },
      {
         "namespace": "SYS.EVS",
         "metric_name": "disk_device_read_bytes_rate",
         "dimensions": [
            {
               "name": "disk_name",
               "value": "6a2bf14a-e3be-4fc9-8522-ba6fe7f0b503-vdc"
            }
         ],
         "datapoints": [
            {
               "max": 0,
               "timestamp": 1724741487000
            },
            {
               "max": 0,
               "timestamp": 1724741547000
            },
            {
               "max": 0,
               "timestamp": 1724741607000
            },
            {
               "max": 0,
               "timestamp": 1724741667000
            },
            {
               "max": 0,
               "timestamp": 1724741727000
            },
             ......
         ],
         "unit": "B/s"
```

```
    },
    {
        "namespace": "SYS.EVS",
        "metric_name": "disk_device_write_bytes_rate",
        "dimensions": [
            {
                "name": "disk_name",
                "value": "6a2bf14a-e3be-4fc9-8522-ba6fe7f0b503-vda"
            }
        ],
        "datapoints": [
            {
                "max": 3055.1,
                "timestamp": 1724741487000
            },
            {
                "max": 3195.78,
                "timestamp": 1724741547000
            },
            {
                "max": 2973.39,
                "timestamp": 1724741607000
            },
            {
                "max": 3533.52,
                "timestamp": 1724741667000
            },
            {
                "max": 2636.8,
                "timestamp": 1724741727000
            },
             .......
        ],
        "unit": "B/s"
    },
    ......
  ]
}
```

Troubleshooting Common 4*XX* Issues

1. **HTTP status code**

   400

   Error code

   ces.0014

   Possible causes

   Cause 1: The request parameter format is incorrect. For details, see Case 1.

   Cause 2: Mandatory fields are not transferred. For details, see Case 2.

   Case 1: incorrect request parameter format

   a. The values of the **from** and **to** attributes must be converted into millisecond.

   b. The **period** attribute supports the following enumerated values: **1300**, **1200**, **3600**, **14400**, and **86400**.

   c. The **filter** attribute supports the following enumerated values: **average**, **max**, **min**, **sum**, and **variance**.

      Request parameters

      ```
      {
         "from": 1724331974,   ## The input parameter is in seconds instead of milliseconds.
         "to": 1724315493,     ##The input parameter is in seconds instead of milliseconds.
      ```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
    "period": "10086",    ##Invalid period value
    "filter": "standard", ##Invalid filter value
    "metrics": [{
        "dimensions": [{
            "name": "instance_id",
            "value": "129718f5-833d-4f78-b685-6b1c3091ea69"
        }],
        "metric_name": "mem_usedPercent",
        "namespace": "AGT.ECS"
    }]
}
```

Response parameters

```
{
    "http_code": 400,
    "message": {
        "details": "Some content in message body is not correct, error message: [from,
to]",##from and to issues
        "code": "ces.0014"
    },
    "encoded_authorization_message": null
}
```

Case 2: Mandatory fields are not transferred.

The mandatory field **filter** is not transferred. For more mandatory fields, see the API reference.

Request parameters

```
{
    "from": 1724119607020,
    "to": 1724123207020,
    "period": "1",
    "metrics": [{
        "dimensions": [{
            "name": "instance_id",
            "value": "238764d4-c4e1-4274-88a1-5956b057766b"
        }],
        "metric_name": "mem_usedPercent",
        "namespace": "AGT.ECS"
    }]
}
```

Response parameters

```
{
    "http_code": 400,
    "message": {
        "details": "Some content in message body is not correct, error message: [filter]",  ##filter
issues
        "code": "ces.0014"
    },
    "encoded_authorization_message": null
}
```

2. **HTTP status code**

   404

   Error code

   APIGW.0101

   Possible causes

   Cause 1: The path URI is inconsistent with that in the API reference. For details, see Case 1.

   Case 1: The URI of the path is inconsistent with that in the API reference.

   The version in the URI in the request path is incorrect. The correct version is V1.0 instead of V1. The correct URI is /V1.0/{project_id}/batch-query-metric-data.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Request path

```
POST  /V1/04f9aca88c00d3202fd4c01ed679daf0/batch-query-metric-data
```

Response parameters

```
{
   "error_code": "APIGW.0101",
   "error_msg": "The API does not exist or has not been published in the environment",
   "request_id": "7d7a8258354300ac158c7b14a158d6ec"
}
```

3. **HTTP status code**

   401

   Error code

   ces.0015

   Possible causes

   Cause 1: The project ID in the request for obtaining the token from IAM is different from the project ID used for calling the API for querying monitoring data of multiple metrics.

   Cause 2: The token has expired.

   Cause 3: The token content is copied less or more.

   Cause 4: The AK and SK do not match.

   Troubleshooting

   Rectify the fault based on the possible causes.

   Solution

   Cause 1: The project ID in the request for obtaining the token from IAM is different from the project ID used for calling the API for querying monitoring data of multiple metrics.

   Solution: Ensure that the two project IDs are the same.

   Cause 2: The token has expired.

   Solution: Generate a new token.

   Cause 3: The token content is copied less or more.

   Solution: Obtain the correct token.

   Cause 4: The AK and SK do not match.

   Solution: Obtain the AK and SK of the tenant.

   Case

   The authentication fails due to a token exception.

   Request header

   ```
   X-Auth-Token: MIIqDgYJKoZIhvcNAQcCoIIp-zCC.....+6CIyAFrbHVxQZJ2Jq    ##Token is abnormal.
   ```

   Request parameters

   ```
   {
      "from": 1724311893283,
      "to": 1724315493283,
      "period": "1",
      "filter": "average",
      "metrics": [{
         "dimensions": [{
            "name": "instance_id",
            "value": "129718f5-833d-4f78-b685-6b1c3091ea69"
         }],
         "metric_name": "mem_usedPercent",
         "namespace": "AGT.ECS"
   ```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
    }]
}
```

Response parameters

```
{
    "http_code": 401,
    "message": {
        "details": "Authenticate failed.",
        "code": "ces.0015"
    },
    "encoded_authorization_message": null
}
```

4. **HTTP status code**

   403

   Error code

   ces.0050

   Possible causes

   Possible cause 1: The user policy does not contain the **ces:metricData:list** permissions. For details, see Case 1.

   Case 1: The user policy does not contain the ces:metricData:list fine-grained permissions.

   Add the **ces:metricData:list** action to the policy to which the user belongs.

   Request header

   ```
   X-Auth-Token:  MIIqDgYJKoZIhvcNAQcCoIIp-zCC.....+6CIyAFrbHVxQZJ2Jq
   ```

   Request parameters

   ```
   {
       "from": 1724311893283,
       "to": 1724315493283,
       "period": "1",
       "filter": "average",
       "metrics": [{
           "dimensions": [{
               "name": "instance_id",
               "value": "129718f5-833d-4f78-b685-6b1c3091ea69"
           }],
           "metric_name": "mem_usedPercent",
           "namespace": "AGT.ECS"
       }]
   }
   ```

   Response parameters

   ```
   {
       "http_code": 403,
       "message": {
           "details": "Policy doesn't allow [ces:metricData:list] to be performed.",    ## The user policy does not contain the ces:metricData:list fine-grained permissions.
           "code": "ces.0050"
       },
       "encoded_authorization_message": null
   }
   ```

5. **HTTP status code**

   429

   Error code

   ces.0429

   Possible causes

   Cause 1: The API is throttled. For details, see Case 1.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Case 1: The API is throttled.

The request API is throttled. If the API is throttled, contact O&M personnel to configure a new process policy immediately.

Request parameters

```
{
   "from": 1724311893283,
   "to": 1724315493283,
   "period": "1",
   "filter": "average",
   "metrics": [{
      "dimensions": [{
         "name": "instance_id",
         "value": "129718f5-833d-4f78-b685-6b1c3091ea69"
      }],
      "metric_name": "mem_usedPercent",
      "namespace": "AGT.ECS"
   }]
}
```

Response parameters

```
{
   "http_code": 429,
   "message": {
      "details": "Too Many Requests.",
      "code": "ces.0429"
   },
   "encoded_authorization_message": null
}
```

6.2 How Can I Query Monitoring Data of a Metric?

FAQ Before API Calling

1. Issue 1

   Description

   How can I call the GET /V1.0/{*project_id*}/metric-data API?

   Solution

   For details, see **Querying Monitoring Data of a Metric**.

2. Issue 2

   Description

   What are the domain names for calling this API in different regions?

   Solution

   For details, see **Regions and Endpoints**.

Troubleshooting Common 4*XX* Issues

1. **HTTP status code**

   429

   Error code

   ces.0429

   Possible causes

   Cause 1: The API is throttled. For details, see Case 1.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Solution

If the API is throttled, contact O&M personnel to configure a new process policy immediately.

Case 1: The API is throttled.

View the CPU usage of the ECS whose ID is **6f3c6f91-4b24-4e1b-b7d1-a94ac1cb011d** from 20:00:00 to 22:00:00 on April 30, 2019. The monitoring interval is 20 minutes.

```
GET https://{Cloud Eye endpoint}/V1.0/{project_id}/metric-data?
namespace=SYS.ECS&metric_name=cpu_util&dim.0=instance_id,6f3c6f91-4b24-4e1b-b7d1-
a94ac1cb011d&from=1556625600000&to=1556632800000&period=1200&filter=min
```

Response parameters

```
{
    "http_code": 429,
    "message": {
        "details": "Too Many Requests.",
        "code": "ces.0429"
    },
    "encoded_authorization_message": null
}
```

6.3 What Should I Do If I Do Not Have the Programmatic Access Permission When Calling an API?

Symptom

When you call an API, the message **"code":403,"message":"This user only supports console access, not programmatic access."** is displayed.

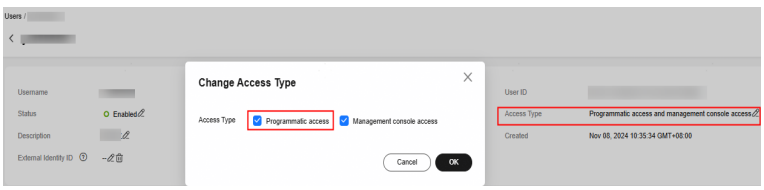
Possible Causes

The user does not have the programmatic access permission.

Procedure

1. Log in to **IAM console** as an administrator.
2. In the user list, click the name of the user to be modified, or click **Security Settings** in the **Operation** column of the user.
3. Click on the right of **Access Type**.
4. In the **Change Access Type** dialog box, select **Programmatic access**.

Figure 6-1 Changing the access type



5. Click **OK**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.