ALIBABA CLOUD

Alibaba Cloud

CloudMonitor

FAQ

Document Version: 20200925

Alibaba Cloud

Legal disclaimer

Alibaba Cloud reminds you to carefully read and fully understand the terms and conditions of this legal disclaimer before you read or use this document. If you have read or used this document, it shall be deemed as your total acceptance of this legal disclaimer.

1. You shall download and obtain this document from the Alibaba Cloud website or other Alibaba Cloud-authorized channels, and use this document for your own legal business activities only. The content of this document is considered confidential information of Alibaba Cloud. You shall strictly abide by the confidentiality obligations. No part of this document shall be disclosed or provided to any third party for use without the prior written consent of Alibaba Cloud.

2. No part of this document shall be excerpted, translated, reproduced, transmitted, or disseminated by any organization, company or individual in any form or by any means without the prior written consent of Alibaba Cloud.

3. The content of this document may be changed because of product version upgrade, adjustment, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and an updated version of this document will be released through Alibaba Cloud-authorized channels from time to time. You should pay attention to the version changes of this document as they occur and download and obtain the most up-to-date version of this document from Alibaba Cloud-authorized channels.

4. This document serves only as a reference guide for your use of Alibaba Cloud products and services. Alibaba Cloud provides this document based on the "status quo", "being defective", and "existing functions" of its products and services. Alibaba Cloud makes every effort to provide relevant operational guidance based on existing technologies. However, Alibaba Cloud hereby makes a clear statement that it in no way guarantees the accuracy, integrity, applicability, and reliability of the content of this document, either explicitly or implicitly. Alibaba Cloud shall not take legal responsibility for any errors or lost profits incurred by any organization, company, or individual arising from download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, take responsibility for any indirect, consequential, punitive, contingent, special, or punitive damages, including lost profits arising from the use or trust in this document (even if Alibaba Cloud has been notified of the possibility of such a loss).

5. By law, all the contents in Alibaba Cloud documents, including but not limited to pictures, architecture design, page layout, and text description, are intellectual property of Alibaba Cloud and/or its affiliates. This intellectual property includes, but is not limited to, trademark rights, patent rights, copyrights, and trade secrets. No part of this document shall be used, modified, reproduced, publicly transmitted, changed, disseminated, distributed, or published without the prior written consent of Alibaba Cloud and/or its affiliates. The names owned by Alibaba Cloud shall not be used, published, or reproduced for marketing, advertising, promotion, or other purposes without the prior written consent of Alibaba Cloud. The names owned by Alibaba Cloud include, but are not limited to, "Alibaba Cloud", "Aliyun", "HiChina", and other brands of Alibaba Cloud and/or its affiliates, which appear separately or in combination, as well as the auxiliary signs and patterns of the preceding brands, or anything similar to the company names, trade names, trademarks, product or service names, domain names, patterns, logos, marks, signs, or special descriptions that third parties identify as Alibaba Cloud and/or its affiliates.

6. Please directly contact Alibaba Cloud for any errors of this document.

Document conventions

Style	Description	Example
Danger	A danger notice indicates a situation that will cause major system changes, faults, physical injuries, and other adverse results.	Danger: Resetting will result in the loss of user configuration data.
Warning	A warning notice indicates a situation that may cause major system changes, faults, physical injuries, and other adverse results.	Warning: Restarting will cause business interruption. About 10 minutes are required to restart an instance.
Notice	A caution notice indicates warning information, supplementary instructions, and other content that the user must understand.	Notice: If the weight is set to 0, the server no longer receives new requests.
Note	A note indicates supplemental instructions, best practices, tips, and other content.	Note: You can use Ctrl + A to select all files.
>	Closing angle brackets are used to indicate a multi-level menu cascade.	Click **Settings**> **Network**> **Set network type**.
Bold	Bold formatting is used for buttons , menus, page names, and other UI elements.	Click **OK**.
`Courier font`	Courier font is used for commands	Run the `cd /d C:/window` command to enter the Windows system folder.
Italic	Italic formatting is used for parameters and variables.	`bae log list --instanceid` *Instance_ID*
[] or [a|b]	This format is used for an optional value, where only one item can be selected.	`ipconfig [-all|-t]`
{} or {a|b}	This format is used for a required value, where only one item can be selected.	`switch {active|stand}`

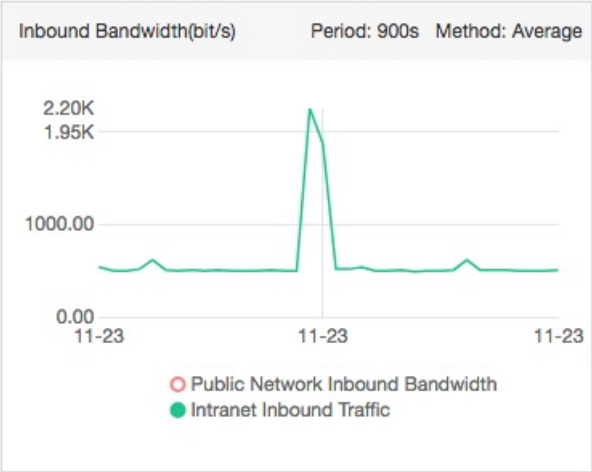
Table of Contents

1.Monitoring

1.1. What are the cause and solution for unexpectedly high traffic over the internal network?

Unexpectedly high traffic over the internal network can be caused by normal data transmission or viruses. You can install the nethogs tool on an Elastic Compute Service (ECS) instance that runs Linux to troubleshoot issues.

The following figure shows that the inbound traffic over the internal network is unexpectedly high for an ECS instance in the CloudMontor console.



Typically, an ECS instance uses a public NIC to provide services and only uses the internal network in a few cases, for example, to communicate with other ECS instances or Server Load Balancer (SLB). Generally, the traffic over the internal network is high when other ECS instances transmits large amounts of data to the ECS instance.

If no ECS instances transmit data to the ECS instance but the traffic over the internal network is high, the ECS instance may be infected with viruses, which cause the ECS instance to forward a large number of packets. If the ECS instance runs Linux, you can use the **nethogs** tool to view the internal bandwidth usage of processes.

```
#yum install nethogs // Install the nethogs tool.
```

```
#nethogs eth0 // View the traffic on the internal NIC.
```

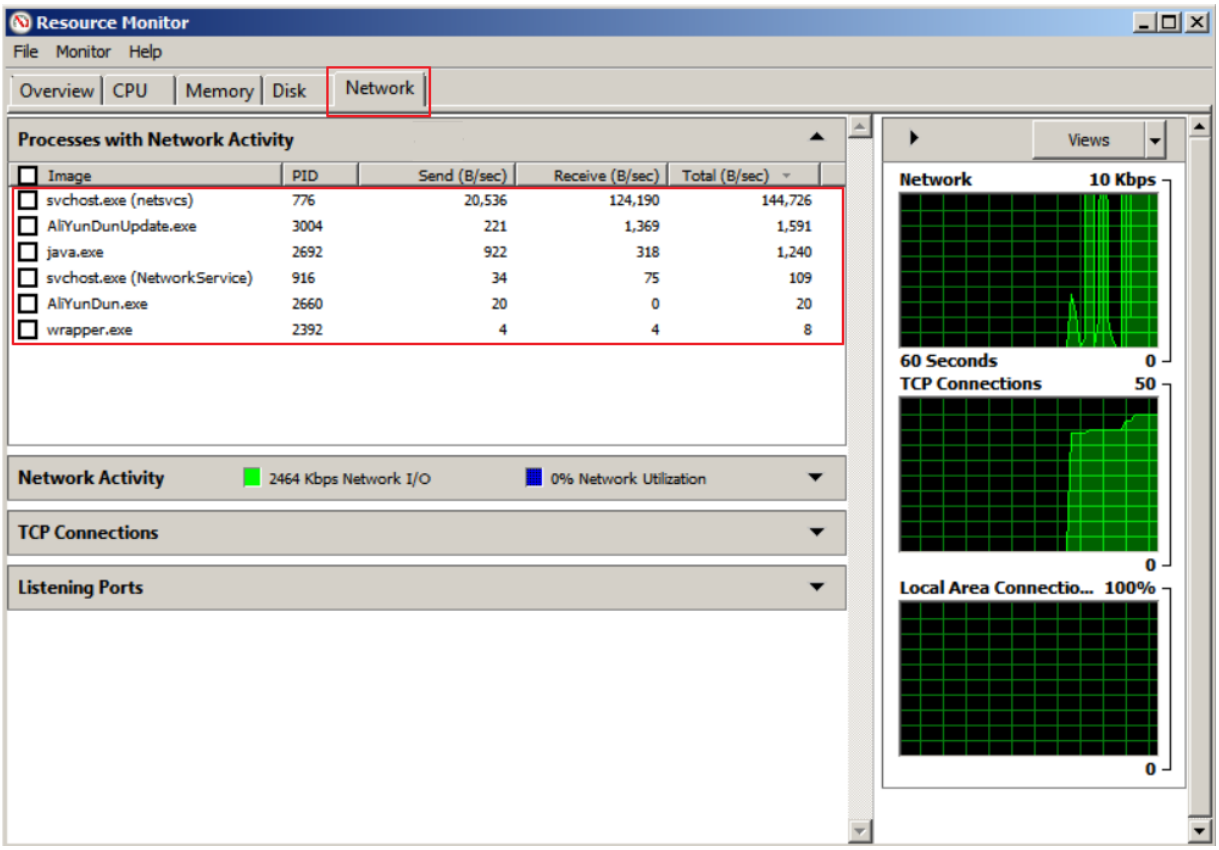
```
NetHogs version 0.8.0

  PID USER     PROGRAM                                                DEV        SENT      RECEIVED
23701 root     /usr/sbin/sshd                                         eth0       0.667     26.321 KB/sec
23696 sshd     sshd: [net]                                            eth0       0.000      0.000 KB/sec
?     root     unknown TCP                                                       0.000      0.000 KB/sec
```

The **nethogs** tool displays the internal bandwidth usage of each process. You can check whether the bandwidth usage is normal.

If the ECS instance runs Windows Server 2008 or later, you can view the internal bandwidth usage of processes in Resource Monitor.

To open Resource Monitor, right-click the taskbar and select **Task Manager**. In the Task Manager dialog box, click the Performance tab and click Open Resource Monitor on the Performance tab. In the **Resource Monitor** dialog box, click the **Networking** tab. On the Networking tab, you can view the internal bandwidth usage of processes.



1.2. What are the custom monitoring SDKs?

Currently, two versions of the custom monitoring SDK are available.

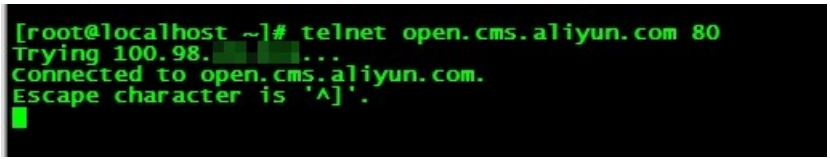
- Custom monitoring SDK (Python): cms_post.py
- Custom monitoring SDK (Bash): cms_post.sh

1.3. What does status code 610 mean in CloudMonitor?

Status code 610 indicates an HTTP connection timeout. These connection timeouts occur when no response packet is returned within five seconds after CloudMonitor sends an HTTP request. If connection timeouts are frequent, we recommend that you increase the value of retry times and enable combined alarms for your corresponding alarm rules.

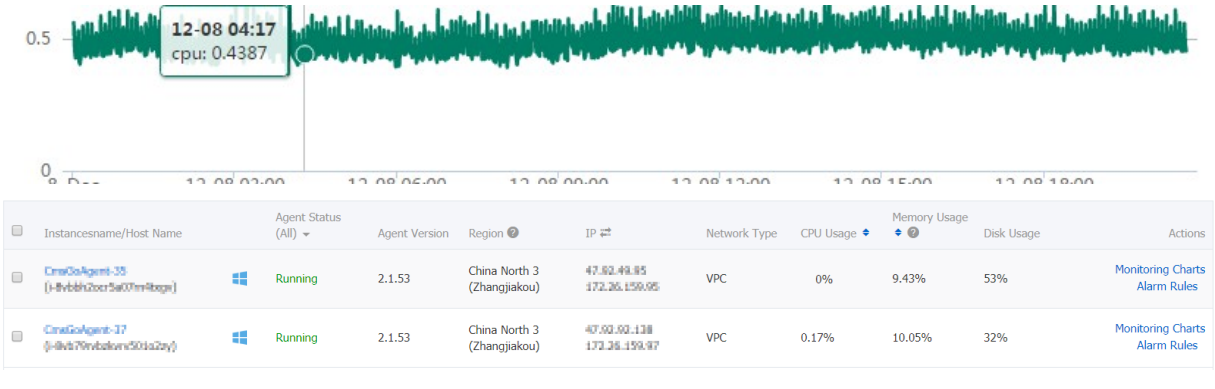
1.4. Why is CloudMonitor unavailable after the ECS intranet is disabled?

When the ECS intranet is disabled, the CloudMonitor service becomes unavailable because CloudMonitor resolves the communication address (open.cms.aliyun.com) on the intranet, and obtains data through the intranet. To use CloudMonitor properly, make sure that ECS can telnet port 80 of open.cms.aliyun.com, as shown in the following figure.



1.5. Why is my CPU usage in the CloudMonitor console displayed as 0%?

The reason that your CPU usage in the CloudMonitor console is displayed as 0% relates to how CPU usage is calculated in the CloudMonitor console. While ECS reports data to CloudMonitor once a minute, data shown in the console is the average of the previous five minutes of reported data. Therefore, if the average of every minute in the five minutes is less than 0.5%, then 0% will be displayed in the CloudMonitor console. As such, even if your CPU usage may be displayed as 0% in the CloudMonitor console, this does not necessarily mean that your actual CPU usage is at 0%, as it is more likely the case that your CPU usage is relatively low. As shown in the following monitoring chart, actual CPU usage for this user is around 0.5%, despite 0% being displayed on the console.



1.6. How to install a CloudMonitor agent on multiple instances using PSSH?

PSSH is a Python-based application that allows you to execute SSH commands on up to 30 instances all at once. As such, you will be able to install software, kill a process, or download a file on multiple instances at the same time.

Install CloudMonitor Agent on a single instance

```
bash -c "$(curl http://cloudmonitor-agent.oss-cn-hangzhou.aliyuncs.com/release/install.sh)"
```

Install CloudMonitor Agent on multiple instances using PSSH

- Install PSSH.
  i. Install Python v2.4 or later.
  ii. Install PSSH.

```
wget https://pypi.python.org/packages/source/p/pssh/pssh-2.3.1.tar.gz
tar zxf pssh-2.3.1.tar.gz
cd pssh-2.3.1
python setup.py install
```

- Configure the IP list and prepare the instances on which CloudMonitor will be installed.
  i. Configure the ip.txt file.
  ii. The format is user@ip:port, one per line. By default, Port 22 is used if you do not specify a different port.
  iii. The sudo permission is required for running commands.
  iv. The password used for multiple instances must be the same for each instance. Alternatively, you can establish password-less SSH trust between instances.
- Execute parallel commands on multiple instances.

```
pssh -h ip.txt -A -i bash -c "$(curl http://cloudmonitor-agent.oss-cn-hangzhou.aliyuncs.com/release/install.sh)"
```

  -H: Enter the host list file.

  -A: Enter the password you have set for the corresponding instances. If you established password-less SSH trust between instances, you do not need to enter this parameter.

  -I: Enter your command.

- Check whether CloudMonitor is installed.

```
pssh -h ip.txt -A -i"/usr/local/cloudmonitor/wrapper/bin/cloudmonitor.sh status"
```

1.7. Why is an error reported when I add a process for monitoring in CloudMonitor?

If the message **Add Task Error: add error** is shown when you add a process for monitoring, this means that Server Guard, which is the Alibaba Cloud Security client, is not installed on the server.

1.8. How is memory usage calculated in CloudMonitor?

Memory usage is calculated using the following formula in CloudMonitor:

(mem_total - (mem_free + mem_buffer + mem_cache))/mem_total

You can run the `cat /proc/meminfo` command to check mem_free, mem_buffer, and mem_cache. Consider the following example:

```
[root@localhost ~]# cat /proc/meminfo MemTotal: 8011936 kBMemFree: 227336 kBBuffers: 277872 kBCa
ched: 1451828 kB
```

For this example, memory is calculated with the following formula:

(8011936 - (227336 + 277872 + 1451828))/8011936

The result of this calculation is that memory usage is about 75%.

1.9. What are the cause and solution if the CPU-related metrics of an ECS instance running Windows have abnormal values?

If only the CPU-related metrics of an ECS instance running Windows have abnormal values, such as 0 or a negative value, the performance counter in Windows may have been damaged.

You can run the **typeperf "\Processor(_Total)\% Processor Time"** command to check whether the performance counter is normal. If an error message is returned, indicating that no performance counter is available, the performance counter is damaged. You can run the **lodctr /r** command to fix the performance counter.

1.10. What should I do if a CloudMonitor agent is stopped?

A CloudMonitor agent is registered as stopped if the agent does not respond to a heartbeat for five times consecutively (or for 15 minutes, with each internal of its heartbeat mechanism lasting three minutes). The agent may have stopped due to one of the following reasons:

1. The agent fails to communicate with the CloudMonitor instance.
2. The CloudMonitor process has ended.

The agent fails to communicate with the CloudMonitor instance

If the agent ran normally before the exception occurred, you can reinstall it. To do so, follow these steps:

1. Log on to the CloudMonitor Console.
2. In the left-side navigation pane, select **Host Monitoring**.
3. Select the target host and click **Install**, or install the agent manually. For more information, see Install the CloudMonitor GoLang agent.

The CloudMonitor process has ended

You can check CloudMonitor logs to verify whether the CloudMonitor process has ended, which is a problem that may be due to a bug. If you suspect a bug is the cause, we recommend that you open a ticket for consultation, but you should do so only after verifying that the CloudMonitor process has ended. Do so by following these steps:

1. **Check CloudMonitor logs.**

- Linux: */usr/local/cloudmonitor/logs*
- Windows: *C:/Program Files/Alibaba/cloudmonitor/logs*

2. **Check the agent running status.**
   - Linux:

     ```
     sudo /usr/local/cloudmonitor/wrapper/bin/cloudmonitor.sh status
     ```

   - Windows:

     ```
     C:\"Program Files (x86)"\Alibaba\cloudmonitor\wrapper\bin\AppCommand.bat status
     ```

   In Linux, you can run the command `/usr/local/cloudmonitor/wrapper/bin/cloudmonitor.sh` to view more details.

2.Operation

2.1. Does CloudMonitor support the HMAC-SHA1 signature algorithm and how do I use it?

Yes, CloudMonitor supports the HMAC-SHA1 signature algorithm. It is the only signature algorithm that CloudMonitor supports. To use the HMAC-SHA1 signature algorithm, perform the steps described in this topic.

Procedure

1. Prepare an Alibaba Cloud AccessKey pair.

   A pair of AccessKey ID and AccessKey secret is required to generate a signature for an HTTP request.

   > **Note** You can use an existing AccessKey pair or create one. The AccessKey pair must be active.

2. Generate a signature string for an HTTP request.

   The signature string of an HTTP request is generated based on the *Method*, *Header*, and *Body* fields of the HTTP request.

   ```
   SignString = VERB + "\n"
           + CONTENT-MD5 + "\n"
           + CONTENT-TYPE + "\n"
           + DATE + "\n"
           + CanonicalizedHeaders + "\n"
           + CanonicalizedResource
   ```

   In the preceding formula, `\n` indicates the escaped newline character and the plus sign (`+`) indicates the string concatenation operator. The following table describes the definitions of other fields.

Field	Description	Example
VERB	The HTTP method used to make the request.	PUT, GET, or POST

Field	Description	Example
CONTENT-MD5	The MD5 value of the Body field in the HTTP request. Note The MD5 value must be a string consisting of uppercase letters and digits.	875264590688CA6171F6228AF5BBB3D2
CONTENT-TYPE	The type of the Body field in the HTTP request.	application/json
DATE	The standard timestamp header of the HTTP request. Note This timestamp header follows the RFC 1123 time format and uses the GMT standard time.	Mon, 3 Jan 2010 08:33:47 GMT
CanonicalizedHeaders	The string constructed from the custom headers that are prefixed with `x-cms` and `x-acs` in the HTTP request.	x-cms-api-version:0.1.0\nx-cms-signature
CanonicalizedResource	The string constructed from the resources requested by the HTTP request.	/event/custom/upload

The CanonicalizedHeaders and CanonicalizedResource strings in the preceding table are constructed as the following rules:

- CanonicalizedHeaders
  a. Convert the names of all headers that are prefixed with `x-cms` and `x-acs` to lowercase letters.
  b. Sort the case-converted headers generated in the preceding step in lexicographic order.
  c. Delete all spaces on each side of a delimiter between each header and its content.
  d. Separate all the preceding headers with delimiters (`\n`) to form the final CanonicalizedHeaders string.
- CanonicalizedResource
  a. Set the CanonicalizedResource string to an empty string ("").
  b. Place the URI that you want to access, such as `/event/custom/upload` , between the quotation marks.

c. If the request contains a query string, add a question mark (?) and the query string to the end of the CanonicalizedResource string.

The sort string is the lexicographically sorted string of the request parameters included in the URI. Equal signs (=) are used between the names and values of parameters to form a string. The parameter name-parameter value pairs are then sorted in lexicographic order and connected with ampersands (&) to form a string. The formula for constructing the query string:

```
QUERY_STRING = "KEY1=VALUE1" + "&" + "KEY2=VALUE2"
```

3. Generate a digital signature for the HTTP request.

The formula for generating a digital signature:

```
Signature = base16(hmac-sha1(UTF8-Encoding-Of(SignString), AccessKeySecret))
```

The sample signature string of an HTTP request:

```
SignString="POST" + \n
+"875264590688CA6171F6228AF5BBB3D2" + \n
+"application/json" + \n
+"Tue, 11 Dec 2018 21:05:51 +0800" + \n
+"x-cms-api-version:1.0" + \n
+"x-cms-ip:127.0.0.1" + \n
+"x-cms-signature:hmac-sha1" + \n
+"/metric/custom/upload"

accesskey="testkey"
accessSecret="testsecret" // The AccessKey secret used to sign the HTTP request.
```

The signature generated based on the preceding signature string:

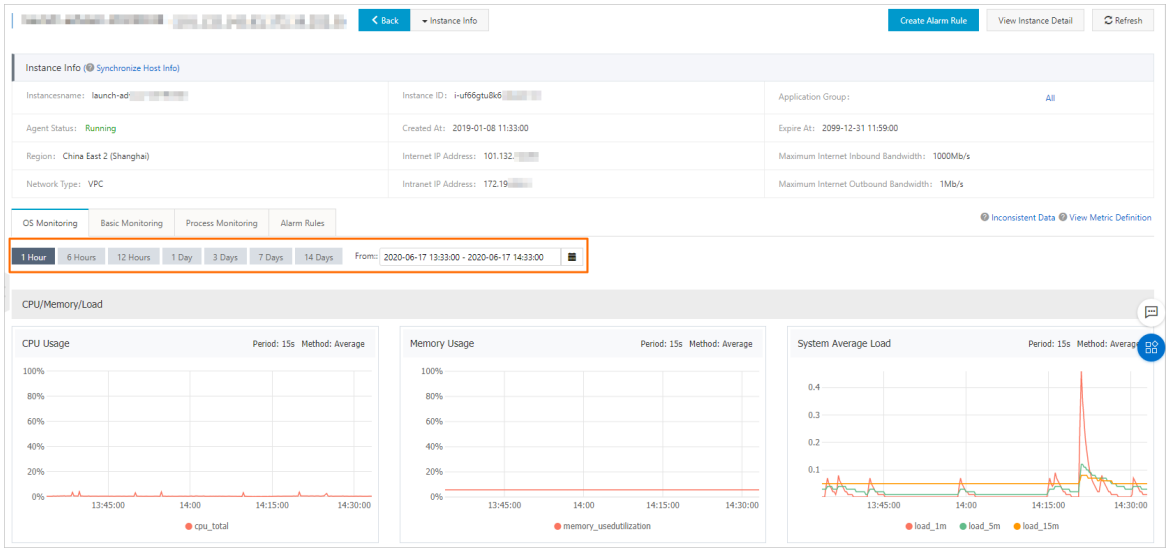
```
1DC19ED63F755ACDE203614C8A1157EB1097E922
```

2.2. How do I view the monitoring data for a specified date or data range in the CloudMonitor console?

To view the monitoring data of a specified date in the CloudMonitor console, follow these steps:

1. Log on to the CloudMonitor Console.
2. In the left-side navigation pane, click the type of monitoring data you want to view, for example, **Host Monitoring**.
3. Click **Monitoring Charts**.

4. Choose a duration and select a date to view monitoring data for the period you select.



Note CloudMonitor only supports querying the monitoring data of the last 30 days.

2.3. What is the inode usage metric in CloudMonitor for?

Linux and Unix systems use inode numbers, instead of file names, to identify files. In other words, files names are simply aliases of inode numbers used for the convenience of identification. When you open a file, the process involved in the system is as follows:

1. The system locates the inode number that corresponds to the file name.
2. The system retrieves inode information using this inode number.
3. The system locates the block where the file data is stored based on the inode information, and then reads the data.

Because every file must have an inode, a potential issue is that all of the inodes of a hard disk may be already used even before this disk is not completely full. In such case, it is not possible to create a new file on the hard disk. Therefore, the purpose of the inode usage metric is to monitor inode usage to manage and avoid issues like the preceding one.

To learn more about inode usage, you can use the following commands:

- To view the total number of inodes for each hard disk partition and the number already used, you can use `df -i` .
- To view the size of each inode node, you can use `sudo dumpe2fs -h /dev/hda | grep "Inode size"` .

2.4. How has event monitoring been upgraded?

Upgrades

Event monitoring has been upgraded to be fully integrated with event alarms, which were originally separate from event monitoring. This change allows for a unified area for both event queries and event alarms.

Upgrade details

1. Event alarms have now migrated to the Event Monitoring page of the console. Originally, event alarms were set on the Create Alarm Rule page. This change has the effect that you can no longer create the following event alarms by using alarm templates: CloudMonitor agent no heartbeat alarms; RDS, Redis, and Memcache faults; RDS, Redis, and Memcache master/slave switchover alarms; MongoDB and Container Service status and node exception alarms; RDS and Redis synchronization exception alarms for disaster recovery.
2. Application groups support event alarm subscription notifications. When you create an application group, you can enable this function. After you enable this feature, you will receive notifications for critical-level and warning-level events for the resources in your application group.
3. This upgrade does not affect any existing event alarm rules. However, you cannot modify these rules after upgrading. To make modifications, you need to create new alarm rules in the event monitoring console.

The preceding upgrade does not affect your online services and existing alarm configurations.

For more information about the event monitoring feature of CloudMonitor, see Cloud product system event monitoring and Use system event alarms.

2.5. How do I restart the Cloud Monitor agent?

After you install or configure the Cloud Monitor agent, you must restart it to apply the configuration. This topic describes how to restart the Cloud Monitor agent in Windows and Linux.

Windows

1. Log on to the server where the Cloud Monitor agent resides as the administrator.
2. Go to the *C:\Program Files\Alibaba\cloudmonitor* directory where the Cloud Monitor agent resides.
3. Double-click *stop.bat* to stop the Cloud Monitor agent.
4. Double-click *start.bat* to start the Cloud Monitor agent.

Linux

1. Log on to the server where the Cloud Monitor agent resides as the root user.
2. Run the following command to go to the directory of the Cloud Monitor agent:**cd /usr/local/cloudmonitor**
3. Run the following command to restart the Cloud Monitor agent:**./cloudmonitorCtl.sh restart**