Alibaba Cloud
Cloud Monitor

User Guide

Issue: 20180909

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 due to product version upgrades, adjustments, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and the updated versions of this document will be occasionally released through Alibaba Cloud-authorized channels. You shall 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 the document in the context that Alibaba Cloud products and services are provided on an "as is", "with all faults" and "as available" basis. 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 bear any liability for any errors or financial losses incurred by any organizations, companies, or individuals arising from their download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, bear responsibility for any indirect, consequential, exemplary, incidental, 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 content of the Alibaba Cloud website, including but not limited to works, products, images, archives, information, materials, website architecture, website graphic layout, and webpage design, 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 the Alibaba Cloud website, product programs, or content 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 contact Alibaba Cloud directly if you discover any errors in this document.

Generic conventions

Table -1: Style conventions

Style	Description	Example
	This warning information 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.
	This warning information 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 restore business.
	This indicates warning information, supplementary instructions, and other content that the user must understand.	 **Note:** Take the necessary precautions to save exported data containing sensitive information.
	This indicates supplemental instructions, best practices, tips, and other content that is good to know for the user.	 **Note:** You can use **Ctrl** + **A** to select all files.
>	Multi-level menu cascade.	**Settings** > **Network** > **Set network type**
Bold	It is used for buttons, menus, page names, and other UI elements.	Click **OK**.
`Courier font`	It is used for commands.	Run the `cd /d C:/windows` command to enter the Windows system folder.
Italics	It is used for parameters and variables.	`bae log list --instanceid` *Instance_ID*
[] or [a|b]	It indicates that it is a optional value, and only one item can be selected.	`ipconfig` *[-all|-t]*
{} or {a|b}	It indicates that it is a required value, and only one item can be selected.	`swich` *{stand | slave}*

Contents

1 Host monitoring

1.1 Introduction to Host monitoring

The host monitoring service of CloudMonitor allows you to install an agent on your servers to monitor the server system. Currently, host monitoring supports Linux and Windows operating systems.

Scenarios

Host monitoring can provide support to the Alibaba Cloud ECS servers, as well as the servers or physical machines of other vendors. Host monitoring collects statistics using a diverse range of OS-related metrics, allowing you to request for the server resource usage and obtain metric data for troubleshooting.

Hybrid cloud monitoring solution

CloudMonitor agent collects server metric data. You can install the agent on a non-ECS server for basic monitoring, on and off the cloud.

Enterprise-level monitoring solution

Host monitoring also provides the application groups function. This function allows you to allocate servers to the different regions of Alibaba Cloud (to the same group) for server management from the business perspective. Host monitoring supports group-based alarm management. You need to configure only one alarm rule for the entire group. This will greatly improve O&M efficiency and overall management experience.

Note:

- Host monitoring supports Linux and Windows, but does not support Unix.
- Server resource consumption of the agent: The CloudMonitor agent installation package is 75 MB. After installation, the size of the package becomes 200 MB with 64-MB memory usage, which is smaller than 1% CPU usage.
- Root permission is required for Agent installation.
- The TCP status statistics function is similar to the Linux netstat -anp command. When many TCP connections exist, a large amount of CPU time is consumed. Therefore, this function is disabled by default.

a. To enable this function in Linux, set “netstat.tcp.disable” in the “cloudmonitor/config/conf.properties” configuration file to “false”. Restart the agent once you modify the configuration.

To enable this function in Windows, set “netstat.tcp.disable” in the “C:\Program Files\Alibaba\cloudmonitor\config” configuration file to “false”. Restart the agent once you modify the configuration.

Monitoring capability

CloudMonitor allows more than 30 metrics covering CPU, memory, disk, and network to meet the basic monitoring and O&M requirements of the servers. Click *here* to view the full list of metrics.

Alarm capability

CloudMonitor provides alarm service for all metrics, allowing you to set alarm rules for individual servers, application groups, and all the other resources. You can use the alarm service as per your business requirements.

You can use the alarm service directly in the host monitoring list, or use it in your application group once you add servers to the group.

1.2 Process Monitoring

Process monitoring by default, allows you to collect information regarding CPU and memory usage and the number of files opened by the active processes over a period of time. If you include a process keyword, the number of processes containing that keyword are displayed.

View the consumption status of an active process

- Every minute the agent singles out the top 5 processes with maximum CPU consumption that happens during the last minute. It displays information like CPU usage, memory usage and the number of opened files.
- For the CPU and memory usage process, see the Linux top command. Here, CPU means a multi-core CPU. CPU means a multi-core CPU.
- For the number of files opened by an active process, see the Linux lsof command.

Note:

- If your process occupies multiple CPUs, there will be more than 100% CPU usage. Here the result of the acquisition is the total utilization of multi-core.

- If the top 5 processes are changing over the time span specified for your query, the process list shows all the processes that are ranked in the top 5 list during the specified time period. The time displayed in the bar chart indicates the processes that were ranked last among the top 5.Top5 time.
- Information regarding the CPU and memory usage and the number of files the processes open is collected only for the top 5 processes. If a process is not ranked among the top 5 continually for a longer time specified for any query, its data points appear randomly in the monitoring charts. The density of the data points for the process shows its degree of activity on the server.
  - The following charts display the HTTP process, which is not ranked continuously among the top 5 processes with maximum server CPU consumption, the data points in the metric charts appear sparse and not continuous. The data points here indicate that the process has ranked amongst the top 5 at exactly the points of time for the data points.
  - The following charts display the mysql process. The data points in the metric charts are dense and appear to be consistent. This indicates that the process is ranked continuously among the top 5 with the maximum CPU consumption.

Manage the number of specified processes

You can get the number of key processes and the viability status, through the process count metric.

- Add a specified process to the monitor

  Example

  For example, the server is currently running the following processes. `/usr/bin/java -Xmx2300m -Xms2300m org.apache.catalina.startup.Bootstrap` `/usr/bin/ruby nginx -c /ect/nginx/nginx.conf`Assume that the user configures 6 keywords, following is the output shown respectively: Keyword: ruby, number of processes returned: 1, hitting a process name. Keyword: nginx, number of processes returned: 1, hitting a process name and a parameter. Keyword: /usr/bin, number of processes returned: 2, hitting 2 paths (two processes under the paths respectively). Keyword: apache.catalina, number of processes returned: 1, hitting part of a parameter. Keyword: nginx.conf, number of processes returned: 1, hitting part of a parameter. Keyword: -c, number of processes returned: 1, hitting part of a parameter.

Procedure

1. Log on to the *CloudMonitor console*.
2. Click **Host Monitoring**in the navigation pane.
3. Click the name of the instance you want to monitor. Or click **Monitoring Chart** from the Actions column to access the instance monitoring details page.
4. Click Process Monitoring at the top of the page to access process monitoring page.
5. To add the process you want to monitor, click Add Process button, and enter the Process Name in the search box.

- Delete a monitored process

  1. Log on to the *CloudMonitor console*.
  2. Click **Host Monitoring**in the navigation pane.
  3. Click the name of the instance you want to monitor. Or click **Monitoring Chart** from the Actions column to access the instance monitoring details page.
  4. Click **Process Monitoring** at the top of the page to access process monitoring page.
  5. When hovering over the process count monitoring chart, click **Add Process to Monitor** button to access the list of processes added to the page.
  6. If you want to delete any process, select the process and click Delete.

- Set alarm rules

  After you have configured monitoring for the specified process, you can configure the alarm rules for the process, you receive an alarm notification when the number of processes changes .

  1. Log on to the *CloudMonitor console*.
  2. Click **Host Monitoring**in the navigation pane.
  3. Select the machine that needs to add the alarm that the process monitors, and click the alarm rule in action, enter the alarm Rules Page.
  4. Click new alarm rule at the top of the page to enter the alarm rule creation page.
  5. Select the number of processes in the rule description, and then configure the appropriat e alarm threshold. If multiple processes are configured on the machine, the number of processes varies, you can click Add alarm rule to configure alerts for multiple processes at once.

1.3 Host monitoring metrics

Host monitoring metrics are divided into agent-collected metrics and ECS native metrics. Agent-collected metrics are collected every 15 seconds, and ECS basic metrics are collected every minute.

Note:

The ECS basic metric data may be inconsistent with the operating system (OS) metric data mainly because of:

- Different statistical frequencies Metric chart data has the average values collected during measurement periods. The statistical frequency of basic monitoring is one minute, whereas that of OS monitoring is 15 seconds. In case of large metric data fluctuations, basic metric data is smaller than OS metric data because the former data is de-peaked.
- Different statistical perspectives The network traffic billing data in basic monitoring does not include the unbilled network traffic between ECS and Server Load Balancer. Whereas, the network traffic statistics in OS monitoring records the actual network traffic of each network adapter. Therefore, the network data in OS monitoring is greater than that in basic monitoring (that is, the agent-collected data is greater than the actual purchased bandwidth or traffic quota).

Agent-collected metrics

- CPU metrics

  You can refer to the Linux top command to understand the meaning of the metrics.

Metric	Definition	Unit	remark
Host.cpu.idle	Percentage of currently idle CPUs	%	Percentage of the current CPU is idle
Host.cpu.system	Percentage of the current kernel space used as CPU	%	This metric measures the consumption resulting from system context switchover. A great value indicates that many processes or threads are running on the server.

Metric	Definition	Unit	remark
Host.cpu.user	This metric measures the CPU consumption of user processes.	%	CPU consumption by user processes
Host. CPU. iowaiit	Percentage of CPUs currently waiting for Io operation	%	This is a relatively high value, which means that there are frequent Io operations .
Host.cpu.other	Other CPU usage percentage	%	Other consumption, calculated in the form of (Nice + sofpratt q + IRQ + stolen) Consumption
Host.cpu.totalUsed	Percentage of total CPU currently consumed	%	The sum of the CPU consumption above, usually used for alarm purposes.

- Memory related monitors

  You can refer to the free command to understand the meaning of the indicators.

Metrics	Definition	Unit	Description
Host.mem.total	Total memory	Bytes	Total Server Memory
Host.mem.used	Amount of used memory	Bytes	Memory Used by the user program + buffers + Cache, the amount of memory used for the buffer , and the amount of memory used for the system cache used by the cache
Host.mem.actualused	Memory actually used by the user	Bytes	calculation formula :(used - buffers - cached)
Host.mem.free	Amount of memory remaining	Bytes	Calculated as (total memory-amount of memory used)

Metrics	Definition	Unit	Description
Host.mem.freeutilization	Percentage of memory remaining	%	Calculated as (amount of remaining memory/total amount of memory * 100)
Host.mem.usedutilization	Memory usage	%	Calculated as (actual used/total * 100)

- Metrics of average system load

  You can refer to the Linux TOP command to understand what the metrics mean. The higher the value of the monitoring item indicates that the more busy the system is.

Metrics	Definition	Unit
Host.load1	Average system load over the past 1 minute, Windows operating system does not have this metric	None
Host. load5	Average system load over the past 5 minutes, Windows operating system does not have this metric	None
Host. load15	Average system load over the past 15 minutes, Windows operating system does not have this metric	None

- Disk related metrics

  — Disk usage and inode usage refer to the Linux DF command.

  — Disk read/write metrics can refer to the Linux iostat command.

  —

Metric	Definition	Unit
Host.diskusage.used	Used storage space on disk	Bytes
Host.disk.utilization	Disk usage	%
Host.diskusage.free	Remaining storage space on disk	Bytes
Host.diskussage.total	Total disk storage	Bytes
Host.disk.readbytes	The number of bytes read per second by the disk.	Bytes/s

Metric	Definition	Unit
Host.disk.writebytes	Number of bytes written per second on disk	Bytes/s
Host.disk.readiops	Number of read requests per second on disk	Times/second
Host.disk.writeiops	Number of write requests per second on disk	Times/second

- File System Monitor

Metrics	Definition	Unit	Description:
Host.fs.inode	Inode usage, the Unix /Linux system uses inode numbers to identify files, and the disks are not fully stocked, however, when inode has been assigned, it will not be able to create a new file on disk, windows operating system does not have this metric.	%	Inode number represents the number of file system files, and a large number of small files can cause too high inode usage.

- Network related metrics

  — You can refer to the Linux iftop command For a collection of TCP connections, refer to the Linux SS Command.

  — The number of TCP connections is collected by default By default, statistics are collected on the number of TCP connections by TCP_TOTAL (total connections), ESTABLISHED (normally established connections), and NON_ESTABLISHED (connections not in the established state). If you want to obtain the number of connections in each state, follow the subsequent procedure:

  ■ Linux

  Set `netstat.tcp.disable` in the *`cloudmonitor/config/conf.properties`* configuration file to `false` to enable data collection. Restart the Agent once you modify the configuration. Restart the Agent once you modify the configuration.

  ■ Windows

Set `netstat.tcp.disable` in the *`C:\"Program\Alibaba\cloudmonitor\config`*configuration file to `false`to enable data collection. Restart the Agent once you modify the configuration.

Metric	Definition	Unit
Host.netin.rate	Number of bits received by the network adapter per second, that is, the uplink bandwidth of the network adapter.	bits/s
Host.netout.rate	Number of bits sent by the network adapter per second, that is, the downlink bandwidth of the network adapter.	bits/s
Host.netin.packages	Number of packets received by the network adapter per second.	packets/s
Host.netout.packages	Number of incoming error packets detected by the drive .	packets/s
Host.netin.errorpackage	Number of outgoing error packets detected by the drive .	packets/s
Host.netout.errorpackages	Number of outgoing error packets detected by the drive .	packets/s
Host.tcpconnection	Number of TCP connection s in various states, including LISTEN, SYN_SENT, ESTABLISHED, SYN_RECV , FIN_WAIT1, CLOSE_WAIT , FIN_WAIT2, LAST_ACK, TIME_WAIT, CLOSING, and CLOSED.	

- Process metrics

  — For details regarding process-specific CPU usage and memory usage, refer to the Linux top command. CPU usage indicates the CPU consumption of multiple kernels.

- For details about Host.process.openfile, refer to the Linux lsof command.
- For details about Host.process.number, refer to the Linux ps aux |grep 'keyword' command.

Metric	Definition	Unit
Host.process.cpu	CPU usage of a process.	%
Host.process.memory	Memory usage of a process.	%
Host.process.openfile	Number of files opened by a process.	Files
Host.process.number	Number of processes that match the specified keyword.	Processes

ECS metrics

If your host is an ECS server, the following metrics are provided without agent installation once you purchase an ECS instance. The collection granularity is one minute.

Metric	Definition	Unit
ECS.CPUUtilization	CPU usage	%
ECS.InternetInRate	Average rate of Internet inbound traffic.	bits/s
ECS.IntranetInRate	Average rate of intranet inbound traffic.	bits/s
ECS.InternetOutRate	Average rate of Internet outbound traffic.	bits/s
ECS.IntranetOutRate	Average rate of intranet outbound traffic.	bits/s
ECS.SystemDiskReadbps	Number of bytes read from the system disk per second.	Bytes/s
ECS.SystemDiskWritebps	Number of bytes written to the system disk per second.	Bytes/s
ECS.SystemDiskReadOps	Number of times data is read from the system disk per second.	times/s
ECS.SystemDiskWriteOps	Number of times data is written to the system disk per second.	times/s
ECS. internetin	Internet inbound traffic.	bytes
ECS.InternetOut	Internet outbound traffic.	bytes

Metric	Definition	Unit
ECS.IntranetIn	Intranet inbound traffic.	bytes
ECS.IntranetOut	Intranet outbound traffic.	bytes

1.4 Agent introduction

Installation path

- Linux : `/usr/local/cloudmonitor`
- Windows 64-bit: `C:\Program Files (x86)\Alibaba\cloudmonitor`
- Windows 32-bit: `C:\Program Files\Alibaba\cloudmonitor`

Process Information

After the host monitor plug-in is installed, you will run the following two processes on your server:

- `/usr/local/cloudmonitor/jre/bin/java`
- `/usr/local/cloudmonitor/wrapper/bin/wrapper`

Port description

- Listen on the TCP localhost 32000 port for the process daemon.
- Access the TCP localhost 32000 port for the process daemon.
- Access TCP remote port 3128, 8080, 443. Used for heartbeat and monitoring data reporting, non-Ali cloud machines use 443 ports, the Ali cloud machine uses either port 3128 or port 8080 .
- Access the HTTP remote 80 port for cloud monitoring plug-in upgrades.

Plug-in log

- The monitoring data acquisition log is located at`/usr/local/cloudmonitor/logs`
- Startup, shutdown, process daemon and other logs are located at `/usr/local/cloudmonitor/wrapper/logs` 。
- You can modify`/usr/local/cloudmonitor/config/log4j.properties` to adjust the log level.

Resource footprint

- /usr/local/cloudmonitor/wrapper/bin/wrapper process occupies about 1 m of memory, basically does not consume the CPU.

- /usr/local/cloudmonitor/Barre/bin/Java Process occupies about 70 m of memory and single-core 1-2% CPU.
- Installation Package 70 m, approximately 200 m disk space after installation is completed.
- The log takes up to 40 m space and more than 40 m is cleared.
- Monitor data is sent every 15 seconds, and the bandwidth of the internal network is approximat ely 10kb.
- Send heartbeat data every 3 minutes, which occupies approximately 2kb of network bandwidth.

External dependencies

- The cloud monitoring agent is written in the Java language and is built in With Barre 1.8.
- Java service wrapper is used for process daemon, boot startup, Windows Service Registration , and so on.
- The `iproute ss` command is used to capture a TCP connection, and if the current system does not, the user needs to install it himself

Installation instructions

See *Install CloudMonitor agent*.

Non-Ali cloud host Installation Method

1. Log in to the cloud monitoring *host monitoring* page.
2. After clicking on the upper right corner of the page, **how to add hosts** and open the document, after you copy the plug-in installation command for a non-Ali cloud server, you can just execute it on the machine.

1.5 Agent release notes

1.2.11

When using the local health check function, upgrade the agent to this version.

New features

- Protocol-dependent local and remote detection, with support for Telnet and HTTP detection

Rectification and optimization of known issues

- The privilege escalation loophole that may occur when the tmp directory is used as the temporary download directory of the installation script is fixed.

- The problem of submitting identical device data when the same disk is attached multiple times is fixed.
- The problem that some processes cannot obtain the path and name is fixed.
- The file download method is optimized to prevent monitoring process blocking that may result from the downloading process.

1.1.64

Known issues are fixed and optimized. If you use a version later than CentOS 7.2, we recommend that you upgrade the agent to this version.

- The memory usage collection logic is adjusted. For versions later than CentOS 7.2, MemAvailable field is used for available memory estimation to improve the accuracy of memory usage calculation.

1.1.63

Rectification and optimization of known issues

- The default wrapper log is changed to the info level.
- Log information of the error level is added for ease of problem locating.
- The risk of memory leakage that may result from logs at the debug level is eliminated.

1.1.62

Rectification and optimization of known issues

- The HTTP Proxy selection logic is optimized to improve the agent installation success rate.
- Key logs are added for ease of problem locating.

1.1.61

Rectification and optimization of known issues

- The problem of incorrect collection of topN processes that results from abnormal collection of process user names by some systems is fixed.

1.1.59

Rectification and optimization of known issues

- The process count collection method is optimized to improve performance.
- Two CloudMonitor agent processes are excluded from process count collection during process monitoring.

1.6 Alarm rules service

Host monitoring provides the alarm rules service option. With the help of this alarm service, you can set an alarm rule for a single server in host monitoring, or set an alarm policy in group granularity once you add servers to the specified group. For more information, see*Managing Alarm Rules*.

Create an alarm rule

1. Log on to the *CloudMonitor console*.
2. Switch to the alarm rules on the host monitoring page, page.
3. Click **Create Alarm Rule** in the upper-right corner.
4. Set alarm parameters on the Create Alarm Rule page. Fill all the fields with the required information. For more information, see *Manage alarm rules*.
5. Click Confirm to save your alarm rules settings.

Delete an alarm rule

1. Go to the *Host Monitoring* page of CloudMonitor.
2. Click Alarm Rules tab.
3. Click the delete action corresponding to the alarm rule to delete the single alarm rule. Or when multiple rules are checked, click the delete button below the list to delete multiple rules.

Modify an alarm rule

1. Go to the *>Host Monitoring* page of CloudMonitor.
2. Click Alarm Rules tab.
3. Click Modify to make changes to the alarm rules.

View alarm rules

1. Go to the *>Host Monitoring* page of CloudMonitor.
2. Click Alarm Rules from the Actions tab to view the alarm rule of a single server.
3. Go to the Alarm Rules page to view all the alarm rules.

1.7 Install CloudMonitor agent

Install CloudMonitor agent on Linux

Frequently used commands

```
# Running status
/usr/local/cloudmonitor/wrapper/bin/cloudmonitor.sh status
```

```
# Start
/usr/local/cloudmonitor/wrapper/bin/cloudmonitor.sh start

# Stop
/usr/local/cloudmonitor/wrapper/bin/cloudmonitor.sh stop

# Restart
/usr/local/cloudmonitor/wrapper/bin/cloudmonitor.sh restart

# Uninstall
/usr/local/cloudmonitor/wrapper/bin/cloudmonitor.sh remove && \
rm -rf /usr/local/cloudmonitor
```

Installation command

Copy the following command and then run it on the server as the root user:

North China 1 Qingdao cn-qingdao

```
REGION_ID=cn-qingdao VERSION=1.3.2 \
bash -c "$(curl https://cms-agent-cn-qingdao.oss-cn-qingdao-internal.
aliyuncs.com/release/cms_install_for_linux.sh)"
```

North China 2 Beijing cn-beijing

```
REGION_ID=cn-beijing VERSION=1.3.2 \
bash -c "$(curl https://cms-agent-cn-beijing.oss-cn-beijing-internal.
aliyuncs.com/release/cms_install_for_linux.sh)"
```

North China 3 Zhangjiakou cn-zhangjiakou

```
REGION_ID=cn-zhangjiakou VERSION=1.3.2 \
bash -c "$(curl https://cms-agent-cn-zhangjiakou.oss-cn-zhangjiakou-
internal.aliyuncs.com/release/cms_install_for_linux.sh)"
```

North China 5 Hohhot cn-huhehaote

```
REGION_ID=cn-huhehaote VERSION=1.3.2 \
bash -c "$(curl https://cms-agent-cn-huhehaote.oss-cn-huhehaote-
internal.aliyuncs.com/release/cms_install_for_linux.sh)"
```

East China 1 Hangzhou cn-hangzhou

```
REGION_ID=cn-hangzhou VERSION=1.3.2 \
bash -c "$(curl https://cms-agent-cn-hangzhou.oss-cn-hangzhou-internal
.aliyuncs.com/release/cms_install_for_linux.sh)"
```

East China 2 Shanghai cn-shanghai

```
REGION_ID=cn-shanghai VERSION=1.3.2 \
bash -c "$(curl https://cms-agent-cn-shanghai.oss-cn-shanghai-internal
.aliyuncs.com/release/cms_install_for_linux.sh)"
```

South China 1 Shenzhen cn-shenzhen

```
REGION_ID=cn-shenzhen VERSION=1.3.2 \
bash -c "$(curl https://cms-agent-cn-shenzhen.oss-cn-shenzhen-internal
.aliyuncs.com/release/cms_install_for_linux.sh)"
```

Hong Kong Hong Kong cn-hongkong

```
REGION_ID=cn-hongkong VERSION=1.3.2 \
bash -c "$(curl https://cms-agent-cn-hongkong.oss-cn-hongkong-internal
.aliyuncs.com/release/cms_install_for_linux.sh)"
```

West US 1 Silicon Valley us-west-1

```
REGION_ID=us-west-1 VERSION=1.3.2 \
bash -c "$(curl https://cms-agent-us-west-1.oss-us-west-1-internal.
aliyuncs.com/release/cms_install_for_linux.sh)"
```

East US 1 Virginia us-east-1

```
REGION_ID=us-east-1 VERSION=1.3.2 \
bash -c "$(curl https://cms-agent-us-east-1.oss-us-east-1-internal.
aliyuncs.com/release/cms_install_for_linux.sh)"
```

Asia Pacific Southeast 1 Singapore ap-southeast-1

```
REGION_ID=ap-southeast-1 VERSION=1.3.2 \
bash -c "$(curl https://cms-agent-ap-southeast-1.oss-ap-southeast-1-
internal.aliyuncs.com/release/cms_install_for_linux.sh)"
```

Asia Pacific Southeast 2 Sydney ap-southeast-2

```
REGION_ID=ap-southeast-2 VERSION=1.3.2 \
bash -c "$(curl https://cms-agent-ap-southeast-2.oss-ap-southeast-2-
internal.aliyuncs.com/release/cms_install_for_linux.sh)"
```

Asia Pacific Southeast 3 Kuala Lumpur ap-southeast-3

```
REGION_ID=ap-southeast-3 VERSION=1.3.2 \
```

```
bash -c "$(curl https://cms-agent-ap-southeast-3.oss-ap-southeast-3-
internal.aliyuncs.com/release/cms_install_for_linux.sh)"
```

Asia Pacific Southeast 5 Jakarta ap-southeast-5

```
REGION_ID=ap-southeast-5 VERSION=1.3.2 \
bash -c "$(curl https://cms-agent-ap-southeast-5.oss-ap-southeast-5-
internal.aliyuncs.com/release/cms_install_for_linux.sh)"
```

Asia Pacific Northeast 1 Tokyo ap-northeast-1

```
REGION_ID=ap-northeast-1 VERSION=1.3.2 \
bash -c "$(curl https://cms-agent-ap-northeast-1.oss-ap-northeast-1-
internal.aliyuncs.com/release/cms_install_for_linux.sh)"
```

Asia Pacific South 1 Mumbai ap-south-1

```
REGION_ID=ap-south-1 VERSION=1.3.2 \
bash -c "$(curl https://cms-agent-ap-south-1.oss-ap-south-1-internal.
aliyuncs.com/release/cms_install_for_linux.sh)"
```

Central Europe 1 Frankfurt eu-central-1

```
REGION_ID=eu-central-1 VERSION=1.3.2 \
bash -c "$(curl https://cms-agent-eu-central-1.oss-eu-central-1-
internal.aliyuncs.com/release/cms_install_for_linux.sh)""
```

Eastern Middle East Dubai me-east-1

```
REGION_ID=me-east-1 VERSION=1.3.2 \
bash -c "$(curl https://cms-agent-me-east-1.oss-me-east-1-internal.
aliyuncs.com/release/cms_install_for_linux.sh)"
```

East China 1 Finance Cloud Hangzhou cn-hangzhou

```
REGION_ID=cn-hangzhou VERSION=1.3.2 \
bash -c "$(curl https://cms-agent-cn-hangzhou.oss-cn-hangzhou-internal
.aliyuncs.com/release/cms_install_for_linux.sh)"
```

East China 2 Finance Cloud Shanghai cn-shanghai-finance-1

```
REGION_ID=cn-shanghai-finance-1 VERSION=1.3.2 \
```

```
bash -c "$(curl https://cms-agent-cn-shanghai-finance-1.oss-cn-
shanghai-finance-1-pub-internal.aliyuncs.com/release/cms_instal
l_for_linux.sh)"
```

South China 1 Finance Cloud Shenzhen cn-shenzen-finance-1

```
REGION_ID=cn-shenzhen-finance-1 VERSION=1.3.2 \
bash -c "$(curl http://cms-agent-cn-shenzhen-finance-1.oss-cn-shenzhen
-finance-1-internal.aliyuncs.com/release/cms_install_for_linux.sh)"
```

Install CloudMonitor agent on Windows

Installation procedure

1. Download *64-bit version Agent* or *32-bit version Agent*.
2. Create a folder and name it `cloudmonitor` in the path `C:/Program Files/Alibaba`.
3. Decompress the package to `C:/Program Files/Alibaba/cloudmonitor`.
4. Double-click `C:/Program Files/Alibaba/cloudmonitor/wrapper/bin/InstallApp-NT.bat` to install CloudMonitor as the administrator.
5. Double-click `C:/Program Files/Alibaba/cloudmonitor/wrapper/bin/StartApp-NT.bat` to start CloudMonitor as the administrator.
6. After the installation is complete, you can view, start, and stop the CloudMonitor application from the service panel of Windows.

Uninstall procedure

1. Stop the CloudMonitor application from the service panel of Windows.
2. Run `C:/Program Files/Alibaba/cloudmonitor/wrapper/bin/UninstallApp-NT.bat` to delete the CloudMonitor application as the administrator.
3. In the installation directory, delete the entire directory `C:/Program Files/Alibaba/cloudmonitor`.

Download with no public network

If there is no public network, you can download the package from the Intranet. For example, the download address of Qingdao 64-bit installation package is: *http://cms-agent-cn-qingdao.oss-cn-qingdao.aliyuncs.com/release/1.3.2/windows64/agent-windows64-1.3.2-package.zip*

- For the download address of another region, change "cn-qingdao" both in the preceding example.
- For the download address of Windows 32-bit version, change "windows64" both to "windows32" in the preceding example.

- For the download address of another version, change "1.3.2" both in the preceding example.

Region list

Region name	Region description	City
North China 1	cn-qingdao	Qingdao
North China 2	cn-beijing	Beijing
North China 3	cn-zhangjiakou	Zhangjiakou
North China 5	cn-huhehaote	Hohhot
East China 1	cn-hangzhou	Hangzhou
East China 2	cn-shanghai	Shanghai
South China 1	cn-shenzhen	Shenzhen
China (Hong Kong)	cn-hongkong	China (Hong Kong)
West US 1	us-west-1	Silicon Valley
East US 1	us-east-1	Virginia
Asia Pacific Southeast 1	ap-southeast-1	Singapore
Asia Pacific Southeast 2	ap-southeast-2	Sydney
Asia Pacific Southeast 3	ap-southeast-3	Kuala Lumpur
Asia Pacific Southeast 5	ap-southeast-5	Jakarta
Asia Pacific Northeast 1	ap-northeast-1	Japan
Asia Pacific South 1	ap-south-1	Mumbai
Central Europe 1	eu-central-1	Frankfurt
Eastern Middle East 1	me-east-1	Dubai
East China 1 Finance Cloud	cn-hangzhou	Hangzhou
East China 2 Finance Cloud	cn-shanghai-finance-1	Shanghai
South China 1 Finance Cloud	cn-shenzhen-finance-1	Shenzhen

Security configuration instructions

The following table lists the ports that the CloudMonitor agent uses to interact with the server. If these ports are disabled by the security software, monitoring data may fail to be collected. If your ECS server requires a higher level of security, you can add the following IP addresses to the white list.

Note:

Future updates and maintenance of the CloudMonitor version may add more IP addresses or change the IP addresses. To simplify the configuration of the firewall rules, you can directly allow the outbound direction of the 100.100 network segment, which is reserved for the intranet of Alibaba Cloud and used to provide official Alibaba Cloud services, with no security issues in general.

Port	IP address	Direction	Description
32000	127.0.0.1	Inbound, outbound	Bound to 127.0.0.1, used for CloudMonit or agent process Daemon
3128, 8080	100.100.19.43 cn-hangzhou100.100.18.22 cn-beijing100.100.36.102 cn-qingdao100.100.0.13 cn-shenzhen100.100.35.4 cn-hongkong100.100.38.1 us-west-1100.100.38.1 us-east-1100.100.30.20 ap-southeast-1100.100.36.11 cn-shanghai100.100.80.184 ap-northeast-1100.100.80.241 eu-central-1100.100.80.142 me-east-1100.100.80.92 ap-southeast-2100.100.80.92 cn-zhangjiakou100.100.80.153 ap-southeast-3100.100.80.135 cn-huhehaote100.100.80.152 ap-south-1100.100.80.160 ap-southeast-5100.100.80.229 cn-chengdu	Outbound	Used for agent upgrade, monitoring configuration management, and other management and control operations

80	100.100.0.19 cn-zhangjiakou100.100.36.6 cn-shanghai100.100.38.3 us-east-1100.100.29.7 us-west-1100.100.35.11 cn-hongkong100.100.80.137 ap-northeast-1100.100.80.72 eu-central-1100.100.0.31 cn-shenzhen100.100.18.50 cn-beijing100.100.45.73 cn-hangzhou100.100.15.23 cn-qingdao100.100.80.151 me-east-1100.100.80.13 ap-southeast-2100.100.103.7 ap-southeast-1100.100.80.140 ap-southeast-3100.100.80.12 cn-huhehaote100.100.80.66 ap-south-1100.100.80.180 ap-southeast-5100.100.80.14 cn-chengdu	Outbound	Used to collect monitoring data to the CloudMonitor server

Resource consumption

- Installation package size: 75 M
- Space occupied after installation: 200 M
- Memory: 64 M
- CPU: less than 1%
- Network: Intranet, with no public network bandwidth consumption

FAQs

- CloudMonitor log location
- — Linux: `/usr/local/cloudmonitor/logs`

  — Windows: `C:/Program Files/Alibaba/cloudmonitor/logs`

- What should I do if there is a conflict between the port occupied by the agent and the port used by my service?

  1. Change the port range by modifying the CloudMonitor configuration, with the file location: `/usr/local/cloudmonitor/wrapper/conf/wrapper.conf`
  2. Restart CloudMonitor

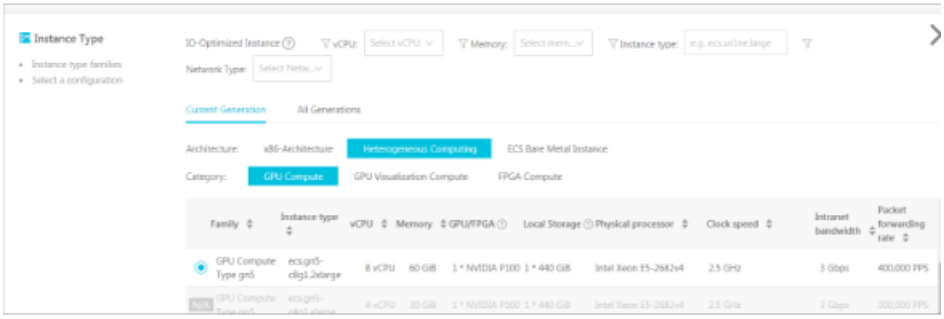
```
wrapper.port.min=40000
wrapper.port.max=41000
wrapper.jvm.port.min=41001
wrapper.jvm.port.max=42000
```

1.8 Query GPU monitoring data

You can query GPU monitoring data in two ways: CloudMonitor console and API

Query GPU monitoring data through the CloudMonitor console

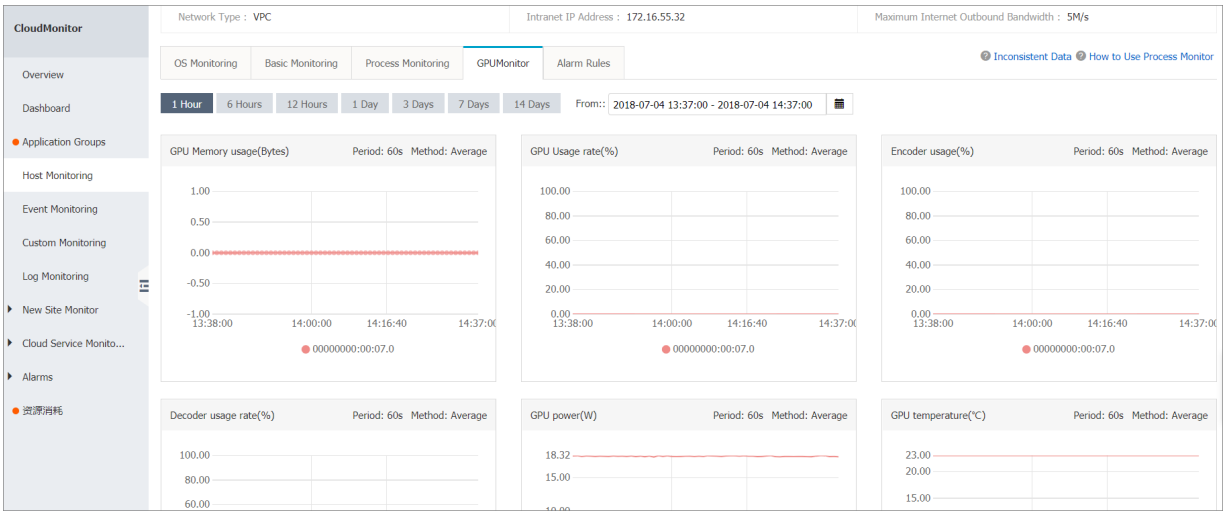
After purchasing an instance of the GPU Compute type for ECS, you only need to install the *GPU driver* and the 1.2.28 version of the CloudMonitor plug-in before you can view and configure GPU-related metric charts, or set alarm rules.



View metric charts

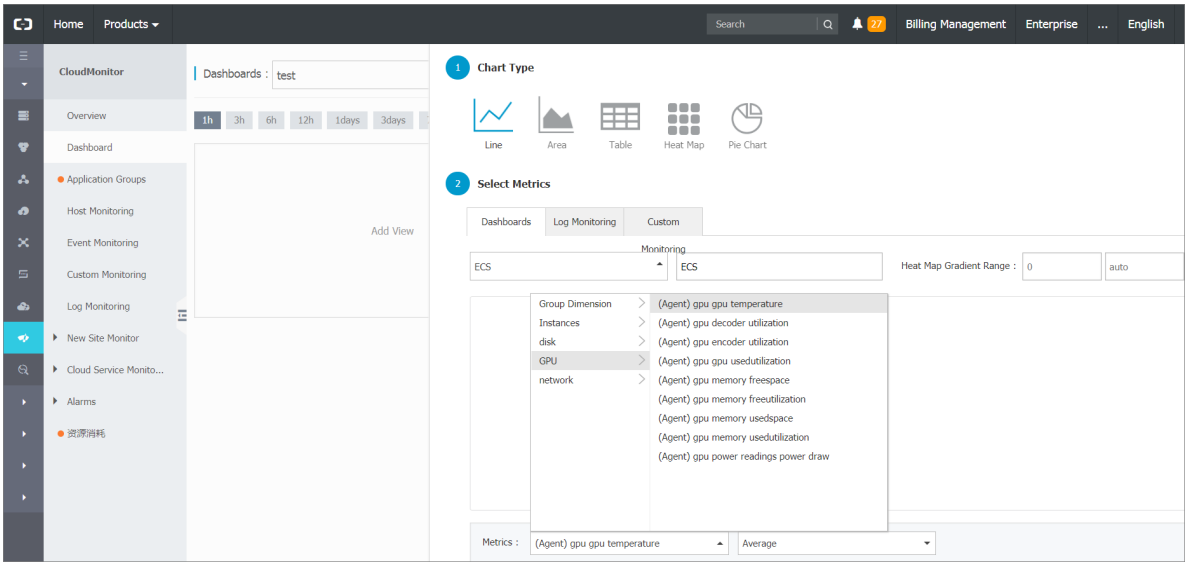
To view GPU-related metric charts, follow these steps:

1. Log on to the *CloudMonitor console*.
2. Click **Host Monitoring** in the navigation bar.
3. Query GPU-related metric charts on the **GPUMonitor** page, as shown in the following figure.

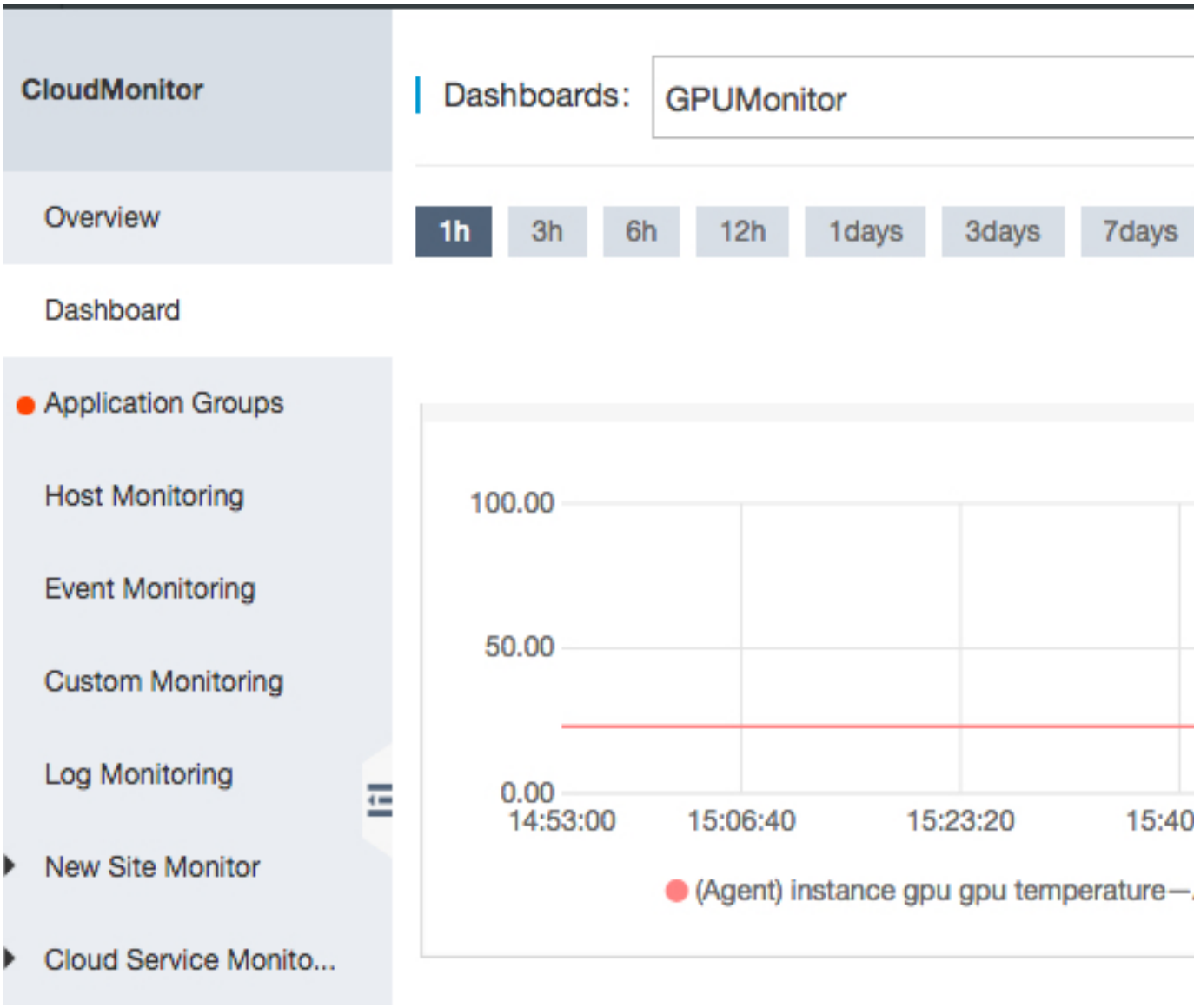


Configure metric charts

1. Log on to the *CloudMonitor console*.
2. Click **Dashboard** in the navigation bar.
3. Click **Create Dashboard** on the **Dashboard** page.
4. In the pop-up dialog box, enter the name of the new dashboard and click **Create**.
5. On the refreshed page, click **Add View**.
6. On the **Add View** page, select the chart type you want, and then select **Metrics**, as shown in the following figure.



7. Select the metrics you want from the drop-down menu. The following figure uses the instance-dimension GPU temperature as an example.



Set alarm rules

The method of adding alarm rules for new GPU metrics is the same as that for other ECS metrics. It is recommended that you add GPU alarm rules in batches by applying the template to groups after creating the template. For details, see *Alarm template*.

Metrics description

GPU-related metrics are classified into three dimensions: GPU, instance, and group.

GPU-dimension metrics

GPU-dimension metrics measure monitoring data on a per GPU basis. The following table lists GPU-dimension metrics.

Metric Name	Unit	Description	Dimensions
gpu_memory _freespace	Bytes	GPU-dimension memory free space	instanceId,gpuId
gpu_memory _totalspace	Bytes	GPU-dimension memory total space	instanceId,gpuId
gpu_memory _usedspace	Bytes	GPU-dimension memory used space	instanceId,gpuId
gpu_gpu_usedutilization	%	GPU-dimension GPU utilization	instanceId,gpuId
gpu_encoder_utilization	%	GPU-dimension encoder utilization	instanceId,gpuId
gpu_decoder_utilization	%	GPU-dimension decoder utilization	instanceId,gpuId
gpu_gpu_temperature	℃	GPU-dimension GPU temperature	instanceId,gpuId
gpu_power_ readings_power_draw	W	GPU-dimension GPU power	instanceId,gpuId
gpu_memory_freeutilization	%	GPU-dimension memory idle rate	instanceId,gpuId
gpu_memory_useutilization	%	GPU-dimension memory utilization	instanceId,gpuId

Instance-dimension metrics

Instance-dimension metrics measure the maximum, minimum, or average value of multiple GPUs on a per instance basis, so that you can query the overall resource usage at the instance level.

Metric Name	Unit	Description	Dimensions
instance_gpu_decoder _utilization	%	Instance-dimension GPU decoder utilization	instanceId
instance_gpu_encoder _utilization	%	Instance-dimension GPU encoder utilization	instanceId
instance_g pu_gpu_temperature	℃	Instance-dimension GPU temperature	instanceId

Metric Name	Unit	Description	Dimensions
instance_gpu_gpu_usedutilization	%	Instance-dimension GPU utilization	instanceId
instance_gpu_memory_freespace	Bytes	Instance-dimension GPU memory free space	instanceId
instance_gpu_memory_freeutilization	%	Instance-dimension GPU memory idle rate	instanceId
instance_gpu_memory_totalspace	Bytes	Instance-dimension GPU memory total space	instanceId
instance_gpu_memory_usedspace	Bytes	Instance-dimension GPU memory used space	instanceId
instance_gpu_memory_usedutilization	%	Instance-dimension GPU memory utilization	instanceId
instance_gpu_power_readings_power_draw	W	Instance-dimension GPU power	instanceId

Group-dimension metrics

Group-dimension metrics measure the maximum, minimum, or average value of multiple instances on a per group basis, so that you can query the overall resource usage at the group level.

Metric Name	Unit	Description	Dimensions
group_gpu_decoder_utilization	%	Group-dimension GPU decoder utilization	groupId
group_gpu_encoder_utilization	%	Group-dimension GPU encoder utilization	groupId
group_gpu_gpu_temperature	℃	Group-dimension GPU temperature	groupId
group_gpu_gpu_usedutilization	%	Group-dimension GPU utilization	groupId

Metric Name	Unit	Description	Dimensions
group_gpu_ memory_freespace	Bytes	Group-dimension GPU memory free space	groupId
group_gpu_ memory_freeutilization	%	Group-dimension GPU memory idle rate	groupId
group_gpu_ memory_totalspace	Bytes	Group-dimension GPU memory total space	groupId
group_gpu_ memory_usedspace	Bytes	Group-dimension GPU memory used space	groupId
group_gpu_ memory_usedutilizati on	%	Group-dimension GPU memory utilization	groupId
group_gpu_ power_read ings_power_draw	W	Group-dimension GPU power	groupId

Query GPU monitoring data through the API

- See *QueryMetricList*.
- Parameter description: The "Project" parameter should be set to "acs_ecs_dashboard." For the values of the "Metric" and "Dimensions" parameters, see the GPU metrics in the preceding tables.

2 Site Monitoring

2.1 Overview of Site Monitoring

Application Scene

Site Monitoring is a monitoring product based on Internet network detection, it is mainly used to send detection requests to simulate real-world user access through Internet terminals all over the country, monitor the network end users of the national provincial and provincial operators to your service site access. The following are typical application scenarios for site monitoring.

Analysis of carrier network quality

The Detection Points monitored by the site simulate the end-user's access behavior, access data can be obtained from all over the country to the destination address, in order to know the geographical area, the network quality of operators, targeted network optimization.

Performance Analysis

By creating a site monitoring task, you can get the DNS domain name resolution time, connection time, first packet time, download to the destination address. time, etc, the performance bottlenecks of the service are analyzed.

Competition Analysis

Select a target probe point by adding your own service station and competitor sites, according to the analysis of the detection results, the quality analysis of their own service and Competition Service was obtained.

Probe coverage

Site Monitoring supports the launching of a probe request from a computer room in each area of the Ali cloud or from a nationwide terminal. At present, it covers seven regions from Alibaba computer room and 100 different provinces and cities that distinguish operators.

Region	Operator
Shanghai, Shanghai	Alibaba
Beijing	Alibaba
Qingdao, Shandong Province	Alibaba
Guangdong Province, Shenzhen	Alibaba

Region	Operator
Hebei Province Zhangjiakou	Alibaba
Hangzhou, Zhejiang Province	Alibaba
Hong Kong, Hong Kong	Alibaba
Of Zhoushan City in Zhejiang Province	Telecommunication
In Lishui City, Zhejiang Province	Telecommunication
Taizhou City, Zhejiang Province	China Unicom
Quzhou city, Zhejiang Province	China Unicom
Of Zhoushan City in Zhejiang Province	Move
Tianjin, Tianjin	Telecommunication
Kunming, Yunnan Province	Telecommunication
Chuxiong Yi Autonomous Prefecture, Yunnan Province	Telecommunication
Chuxiong Yi Autonomous Prefecture, Yunnan Province	Move
Yuxi City, Yunnan Province	Move
Zhaotong City, Yunnan Province	Move
Suining City, Sichuan Province	Telecommunication
Mianyang City, Sichuan Province	Telecommunication
Meishan City, Sichuan Province	Telecommunication
Chengdu, Sichuan Province	Telecommunication
Ya'an City, Sichuan Province	Telecommunication
Guang'an, Sichuan Province	China Unicom
Chengdu, Sichuan Province	China Unicom
Meishan City, Sichuan Province	Move
Yibin City, Sichuan Province	Move
Ya'an City, Sichuan Province	Move
Xi'an, Shaanxi Province	Telecommunication
Hanzhong, Shaanxi Province	Telecommunication
Xianyang city, Shaanxi Province	China Unicom
Xianyang city, Shaanxi Province	Move

Region	Operator
Luliang city, Shanxi Province	Telecommunication
Jincheng City, Shanxi Province	Telecommunication
Changzhi City, Shanxi Province	Telecommunication
Luliang city, Shanxi Province	Move
Dongying City, Shandong Province	Telecommunication
Zibo City, Shandong Province	Telecommunication
Jinan City, Shandong Province	Telecommunication
Shandong Province, Qingdao	China Unicom
Linyi City, Shandong Province	China Unicom
Shandong Province Dezhou	China Unicom
Yantai City, Shandong Province	China Unicom
Yantai City, Shandong Province	Dr. Peng
Laiwu City, Shandong Province	Move
The Inner Mongolia Autonomous Region City	Telecommunication
Chifeng City, Inner Mongolia Autonomous Region	China Unicom
Inner Mongolia Erdos city	China Unicom
Wulanchabu City	Move
Dandong City, Liaoning Province	Telecommunication
Panjin City, Liaoning Province	Telecommunication
Huludao city, Liaoning Province	China Unicom
Dalian, Liaoning Province	Dr. Peng
Dalian, Liaoning Province	Move
Panjin City, Liaoning Province	Move
Fushun city, Liaoning Province	Move
Dandong City, Liaoning Province	Move
Yingtan City, Jiangxi Province	Telecommunication
Fuzhou City, Jiangxi Province	China Unicom
Nanchang city, Jiangxi Province	Dr. Peng

Region	Operator
Pingxiang City, Jiangxi Province	Move
Nanchang city, Jiangxi Province	Move
Wuxi, Jiangsu Province	China Unicom
Suqian City, Jiangsu Province	Move
Zhenjiang City, Jiangsu Province	Move
Taizhou City, Jiangsu Province	Move
Nantong City, Jiangsu Province	Move
Yiyang City, Hunan Province	Telecommunication
Changsha city, Hunan Province	Dr. Peng
Xiangtan city, Hunan Province	Move
Yueyang City, Hunan Province	Move
Huanggang City, Hubei Province	China Unicom
Yichang City, Hubei Province	China Unicom
Hubei Province, Wuhan	Dr. Peng
Xianning City, Hubei Province	Move
Xiangfan City, Hubei Province	Move
Jingzhou, Hubei Province	Move
Hubei Province, Huangshi city	Move
Harbin, Heilongjiang Province	Telecommunication
Qiqihar City, Heilongjiang Province	Telecommunication
Heihe City, Heilongjiang Province	China Unicom
Hegang city, Heilongjiang Province	China Unicom
Yichun City, Heilongjiang Province	Move
City, Jixi City, Heilongjiang Province	Move
Daqing City, Heilongjiang Province	Move
Luoyang City, Henan Province	Telecommunication
Kaifeng City, Henan Province	Telecommunication
Xinyang City, Henan Province	Telecommunication
Anyang City, Henan Province	China Unicom

Region	Operator
Anyang City, Henan Province	Move
Hengshui City, Hebei Province	Telecommunication
Qinhuangdao City, Hebei Province	China Unicom
Sanya, Hainan Province	Telecommunication
Guizhou Province Tongren City	Telecommunication
Nanning, Guangxi Zhuang Autonomous Region	Move
Baise City, Guangxi Zhuang Autonomous Region	Move
Zhanjiang City, Guangdong Province	Telecommunication
Yangjiang City, Guangdong Province	Telecommunication
Jiangmen City, Guangdong Province	China Unicom
Meizhou City, Guangdong Province	China Unicom
Lanzhou, Gansu Province	Telecommunication
Zhangye city, Gansu Province	Telecommunication
Tianshui city, Gansu Province	Telecommunication
Jiayuguan city, Gansu Province	Move
Fujian Ningde	Telecommunication
Quanzhou, Fujian	China Unicom
Fujian Ningde	Tietong
Beijing	China Unicom
Chizhou city, Anhui Province	Telecommunication
Huangshan city, Anhui Province	Telecommunication
Wuhu City, Anhui Province	Chine Mobile

Probe protocol type

Probe Type	Feature
HTTP/HTTPS	Tests the specified URL or IP address based on HTTP to obtain the availability metrics, response time, and status code. In advanced settings, you can select the request method (GET/POST/HEAD), set cookie and header

Probe Type	Feature
	information, and determine whether the page content matches the specified content.
Ping	|Tests the specified URL or IP address based on ICMP Ping to obtain the availability metrics, response time, and packet loss rate.
TCP	|Tests the specified port based on TCP to obtain the availability metrics, response time , and status code. In advanced settings, you can configure the TCP request content and the matching response content.
UDP	|Tests the specified port based on UDP to obtain the availability metrics, response time , and status code. In advanced settings, you can configure the UDP request content and the matching response content.
DNS	Tests the specified domain name based on DNS to obtain the availability metrics, response time, and status code. You can go to advanced settings to query A, MX, NS, CNAME , TXT, and ANY records.
POP3	|Tests the specified URL or IP address based on POP3 to obtain the availability metrics, response time, and status code. In advanced settings, you can configure the port, username , password, and whether to use a secure link.
SMTP	|Tests the specified URL or IP address based on SMTP to obtain the availability metrics, response time, and status code. In advanced settings, you can configure the port, username , password, and whether to use a secure link.
FTP	Tests the specified URL or IP address based on FTP to obtain the availability metrics, response time, and status code. In advanced settings, you can configure the port and whether to use a secure link.

2.2 Managing Site monitoring tasks

Create a site monitoring task

The task of creating site monitoring is divided into three steps: Setting basic information, selecting Detection Points, and setting alarm rules. Set alarm rules to be optional and can not be set.

1. Log in to the cloud monitoring console and select site administration from the menu on the left side of the page to monitor the site, enter the site monitoring task list page.
2. Click the new task button in the upper-right corner of the page to enter the create site monitoring task page.
3. Fill in the basic information.
   - Monitoring type: Monitoring Protocol, HTTP (s) Enabled), ping, TCP, UDP, DNS, SMTP, POP3, FTP 8 protocols.
   - Task Name: the name of the monitoring task.
   - Monitor address: The target monitor address can fill in more than one monitor address at a time, it is convenient for the user to set up in bulk. Multiple Monitor addresses are split into multiple tasks on Save.
   - Monitor frequency: monitor cycle, for example, select a 1 minute frequency, the destination address is monitored at each geographic probe point at a frequency of 1 minute/times.
   - Advanced Settings: different protocols support different advanced settings, and you can choose to use them according to the actual situation.
4. Select a probe point
   - Quick Selection of Detection Points: the common Detection Points will be packaged, so that you can choose quickly in bulk.
   - Probe point advanced options: select the specified probe point on-demand.
5. Set alarm rules
   - Availability: divided into two options: the number of available points and the percentage of available points. Not available when the status code in the probe result is greater than 399 . Number of available probe points = the number of probe results with a status code of less than 400 during a cycle, available probe points % = number of probe results within one cycle (the probe point's status code is less than 400) /total number of probe results) * 100.
   - Average response time: the average response time for all probe points in each monitoring cycle.

- Alarm after several consecutive exceeds threshold: the actual monitoring value reaches the set threshold several times in succession before the alarm is made. This item is used to filter the occasional volatility of the monitoring data.
- Select Contact Group: The receiving object when sending the alarm notification.
- Alarm notification method: the sending channel of alarm notification.
- Advanced Settings: includes channel silence time, effective time, alarm callbacks.

Modify site monitoring tasks

1. Log in to the cloud monitoring console and select site administration from the menu on the left side of the page to monitor the site, enter the site monitoring task list page.
2. Select the task that needs to be modified, and click the modify button in the action.
3. Go to the modify page and modify the corresponding content.

Delete site monitoring task

1. Log in to the cloud monitoring console and select site administration from the menu on the left side of the page to monitor the site, enter the site monitoring task list page.
2. Select the task that needs to be modified, click the delete button in the action to delete the task.
3. When the task is deleted, the associated alarm rules are deleted in sync.

Enable or disable site monitoring tasks

1. Log in to the cloud monitoring console and select site administration from the menu on the left side of the page to monitor the site, enter the site monitoring task list page.
2. Select the tasks that need to be enabled or disabled, click the enable or disable button in the action, enable or disable tasks.

2.3 Viewing Monitoring Data

Overview

From availability, National Geographic real-time response time, error distribution, response time trends to present the current site access.

The error distribution counts the number of status codes exceeding 399 in the detection results of each regional operator over a period of time. For details on errors, click under the chart to view related data.

Map of China

Click the left mouse button in the appropriate province to display the secondary area

Details of monitoring data for relevant areas are provided below the map.

Indicator trends

Operator trends

Error rate trend

Click on the details in action, and you can use the city and operator as the filter criteria to see the details below.

1) Access Policy

The Access Strategy provides you with details of the detection results for each region and operator for each probe cycle.

Traceronte

This list provides you with traceronte results initiated by each probe point in the last 24 hours. Traceronte requests require proactive configuration, and clicking traceronte in the upper-right corner of the page will launch a traceronte Probe Based on the configuration.

Terms to explain

Noun	Description
Availability	The status code of the probe point in the probe cycle is less than 400 of the number of probe results/The total number of probe results * 100.
Total Response Time	The time from the Launch probe to the first byte that receives the HTTP response. This value contains the redirected time, if any, during the probe.
DNS time	That is, the DNS domain name resolution time , the number of milliseconds it takes to resolve the domain name.
Build connection time	How long it takes to start the probe, to write the HTTP request to complete, minus the time that the DNS domain name is resolved.
Redirected time	From the Launch probe to the time taken to launch the first non-redirected request.
First package time	From the Launch probe to the time it takes to receive the first byte of the HTTP response packet.
Preparation Time	How long it takes to start the probe, to write the HTTP request to complete.
SSL time	The amount of time it takes to start a probe to complete an SSL authentication.
Download speed	The speed of the network while reading the HTTP response.
Total download size	The size of the HTTP response, if there is Content-Length in the response, that value, if none, the number of bytes actually read.
TCP connection time	The amount of time, including DNS domain name resolution time, taken from the start-up probe to the completion of the TCP connection).

2.4 状态码说明

站点监控的每种协议在进行探测时，都会返回状态码，以下为常见状态码说明。

云监控自定义状态码含义

协议	状态码	含义
HTTP	610	超时(连接超时、SSL证书交换超时，超时时间为30s)
HTTP	613	DNS解析错误
HTTP	615	内容不匹配
HTTP	616	认证失败
HTTP	611	其他原因导致的探测失败
Ping	550	网络不通
Ping	610	网络稳定，但发出的所有包在2秒内均无响应
Ping	613	无法通过host解析出IP地址
TCP	550	无法打开socket(通常是因为系统资源耗尽)
TCP	610	接收回应失败(超时或无回应)
TCP	611	连接失败(超时或对端拒绝)
TCP	615	内容不匹配
UDP	550	无法打开socket(通常是因为系统资源耗尽)
UDP	611	连接失败(host无法解析)
UDP	610	发送或接收失败
UDP	615	内容不匹配
DNS	610	DNS解析失败
DNS	613	DNS query通信出现异常
DNS	615	内容不匹配
SMTP	610	连接超时
SMTP	611	无法成功访问您的站点，失败原因包含但不限于DNS解析失败、Email格式不正确、初始化SMTP客户端失败等

协议	状态码	含义
SMTP	616	登录被拒绝
POP3	611	无法成功访问您的站点
FTP	610	FTP传输失败
FTP	611	其它原因导致的失败，如DNS解析失败，TCP连接失败等
FTP	616	登录失败

HTTP协议常用标准状态码含义

状态码	含义	备注
200	请求已完成	2XX状态码均为正常状态码返回。
300	多种选择	服务器根据请求可执行多种操作。服务器可根据请求者 (User agent) 来选择一项操作，或提供操作列表供请求者选择。
301	永久移动	请求的网页已被永久移动到新位置。服务器返回此响应（作为对 GET 或 HEAD 请求的响应）时，会自动将请求者转到新位置。您应使用此代码通知 Googlebot 某个网页或网站已被永久移动到新位置。
302	临时移动	服务器目前正从不同位置的网页响应请求，但请求者应继续使用原有位置来进行以后的请求。此代码与响应 GET 和 HEAD 请求的 301 代码类似，会自动将请求者转到不同的位置。
303	查看其他位置	当请求者应对不同的位置进行单独的 GET 请求以检索响应时，服务器会返回此代码。对于除 HEAD 请求之外的所有请求，服务器会自动转到其他位置。

状态码	含义	备注
304	未修改	自从上次请求后，请求的网页未被修改过。服务器返回此响应时，不会返回网页内容。
305	使用代理	请求者只能使用代理访问请求的网页。如果服务器返回此响应，那么，服务器还会指明请求者应当使用的代理。
400	错误请求	服务器不理解请求的语法。
401	未授权	请求要求进行身份验证。登录后，服务器可能会对页面返回此响应。
403	已禁止	服务器拒绝请求。
404	未找到	服务器找不到请求的网页。例如，如果请求是针对服务器上不存在的网页进行的，那么，服务器通常会返回此代码。
405	方法禁用	禁用请求中所指定的方法。
406	不接受	无法使用请求的内容特性来响应请求的网页。
407	需要代理授权	此状态代码与401（未授权）类似，但却指定了请求者应当使用代理进行授权。如果服务器返回此响应，那么，服务器还会指明请求者应当使用的代理。
408	请求超时	服务器等候请求时超时。
409	冲突	服务器在完成请求时发生冲突。服务器的响应必须包含有关响应中所发生的冲突的信息。服务器在响应与前一个请求相冲突的PUT请求时可能会返回此代码，同时会提供两个请求的差异列表。
411	需要有效长度	服务器不会接受包含无效内容长度标头字段的请求。

状态码	含义	备注
412	未满足前提条件	服务器未满足请求者在请求中设置的其中一个前提条件。
413	请求实体过大	服务器无法处理请求，因为请求实体过大，已超出服务器的处理能力。
414	请求的URI过长	请求的URI（通常为网址）过长，服务器无法进行处理。
415	不支持的媒体类型	请求的格式不受请求页面的支持。
416	请求范围不符合要求	如果请求是针对网页的无效范围进行的，那么，服务器会返回此状态代码。
417	未满足期望值	服务器未满足期望请求标头字段的要求。
499	客户端断开连接	因服务端处理时间过长，客户端关闭了连接。
500	服务器内部错误	服务器遇到错误，无法完成请求。
501	尚未实施	服务器不具备完成请求的功能。例如，当服务器无法识别请求方法时，服务器可能会返回此代码。
502	错误网关	服务器作为网关或代理，从上游服务器收到了无效的响应。
503	服务不可用	目前无法使用服务器（由于超载或进行停机维护）。通常，这只是一种暂时的状态。
504	网关超时	服务器作为网关或代理，未及时从上游服务器接收请求。
505	HTTP版本不受支持	服务器不支持请求中所使用的HTTP协议版本。

3 Event monitoring

3.1 Use event monitoring

Event monitoring provides reporting, querying, and warning capabilities for event type data. You can conveniently collect and report exceptions or important changes in services to CloudMonitor, and receive alerts when exceptions occur.

What are the differences between event monitoring and custom monitoring?

Event monitoring is used when monitored data of non-continuous events is reported and queried, and alerts are generated. Custom monitoring is used when monitored data collected cyclically and continuously in the time series is reported and queried and alerts are generated.

Process

- Reporting event data

  See *#unique_26*.

- Querying event data

  Once you have finished reporting the event, you can view the data that has been reported in the console. You can view all the events in event monitoring, or you can enter a specific application grouping, view related events for this grouping.

  View all reported incidents:

  1. Log in to the cloud monitoring console to enter event monitoring.
  2. View all events, as shown in the following figure.

  3. Click action View Details in to view the content of a specific event.

     To query events of the specified group, go to the event monitoring page of the group.

- Set alert policies.

  Set an alert rule Event monitoring provides the alerting function. When setting the alert rule, select the corresponding application group. After an alert is generated, a message is sent to all contacts in the group. If alerts must be generated for an reported event, configure the alert rule using the following methods:

- Method one:

  1. Log in to the cloud monitoring console to enter event monitoring.
  2. On the event list page, click **Create Alert Rule** next to an event.
  3. Go to the alert rule creation page, enter the alert rule name, select the application group, and set the alert policy and notification mode.

- Method two:

  1. Log in to the cloud monitoring console and enter the application cluster.
  2. Select an application group and go to the **Event Monitoring** page of the group.
  3. On the event list page, click **Create Alert Rule** next to an event.
  4. Go to the alert rule creation page, enter the alert rule name and set the alert policy and notification mode.

-

3.2 Report event data

The event monitoring function provides APIs to report events, allowing you to collect and report service exceptions to CloudMonitor. You can configure policies for reported events to receive alerts and notifications.

CloudMonitor supports data reporting using open APIs, Java SDK, and AliCloudCLI.

Restrictions

- Single cloud account QPS is limited to 20.
- Report up to 100 incidents in a single time.
- Report a maximum of 500kb of data in a single time.

Report data using open APIs

- Service address: *https://metrichub-cms-cn-hangzhou.aliyuncs.com*
- Request syntax

```
POST /event/custom/upload HTTP/1.1
Authorization: <authorizationstring>
Content-Length:<Content Length>
Content-MD5:<Content MD5>
Content-Type:application/json
Date: <GMT date>
HOST: maid
x-cms-signature:hmac-sha1
x-cms-api-version:1.0
x-cms-ip:30.27.84.196
```

```
User-Agent:cms-java-sdk-v-1.0
[{"content":"EventContent","groupId":GroupId,"name":"EventName","
time":"20171023T144439.948+0800"}]
```

- Request Parameters

Name	Type	Required	Description
name	String	Yes	Event name
groupId	Numerical	Yes.	APP grouping ID to which the event belongs
time	String	Yes.	Event occurrence time
content	String	Yes.	Event details

Request header definition

Signature Algorithm

- Response Element

  The system returns the HTTP status code 200.

- Example

  — Request example

```
POST /event/custom/upload HTTP/1.1
Host: metrichub-cms-cn-hangzhou.aliyuncs.com
x-cms-api-version:1.0
Authorization:YourAccKey:YourAccSecret
Host:metrichub-cms-cn-hangzhou.aliyuncs.com"
Date:Mon, 23 Oct 2017 06:51:11 GMT
Content-Length:180
x-cms-signature:hmac-sha1
Content-MD5:E9EF574D1AEAAA370860FE37856995CD
x-cms-ip:30.27.84.196
User-Agent:cms-java-sdk-v-1.0
Content-Type:application/json
[{"Content": "123, ABC", "groupid": 100, "name": "event_0", "Time
": "loud. 948 + 0800 "}]
```

  — Response example

```
{
   "Code": 200 ",
   "msg": "// return MSG is empty when reporting normally
```

```
}
```

Report data using the Java SDK

- Maven dependency

```
<dependency>
    <groupId>com.aliyun.openservices</groupId>
    <artifactId>aliyun-cms</artifactId>
    <version>0.1.2</version>
</dependency>
```

- Sample code

```
public void uploadEvent() throws CMSException, InterruptedException
 {
        // Initialize Client
        CMSClient cmsClient = new CMSClient(endpoint, accKey, secret
);
       // Build 2 incident reports
         CustomEventUploadRequest request = CustomEventUploadRequest
.builder()
                    .append(CustomEvent.builder()
                            .setContent("abc,123")
                            .setGroupId(101l)
                            .setName("Event001").build())
                    .append(CustomEvent.builder()
                            .setContent("abc,123")
                            .setGroupId(101l)
                            .setName("Event002").build())
                    .build();
            CustomEventUploadResponse response = cmsClient.
putCustomEvent(request);
            List<CustomEvent> eventList = new ArrayList<CustomEvent
>();
            eventList.add(CustomEvent.builder()
                    .setContent("abcd,1234")
                    .setGroupId(101l)
                    .setName("Event001").build());
            eventList.add(CustomEvent.builder()
                    .setContent("abcd,1234")
                    .setGroupId(101l)
                    .setName("Event002").build());
            request = CustomEventUploadRequest.builder()
                    .setEventList(eventList).build();
            response = cmsClient.putCustomEvent(request);
    }
```

Ali cloud command line (CLI) Way to report data

```
With an Ali cloud account, and generate Sub-Account AK with cloud
 monitoring privileges (with Sub-Account Security better ).
```

- Create a sub-account.

- Generate accesskeyid and accesskeysecret for the sub-account.

- Assign CloudMonitor permissions for the sub-account.

Operation procedure

1. Install the tool aliyuncli.

   ```
   System requirements: Linux, UNIX, or Mac OS Environment requirements:
    Python 2.7.x has been installed.
   ```

   a. Install Python

   - If your device is installed with Python 2.7.x, skip this step.
   - If your device is not installed with Python 2.7.x, run the following command in the command line window to install Python: Make sure that your device is installed with wget.

     ```
     wget https://www.python.org/ftp/python/2.7.8/Python-2.7.8.tgz (
     or download it in other ways and put it in a certain path)
     tar -zxvf Python-2.7.8.tgz
     cd Python-2.7.8
     ./configure
     make
     sudo make install
     ```

   b. Install pip

   - If your device is installed with pip, skip this step.
   - If your device is not installed with pip, run the following command in the command line window to install pip:

     ```
     curl "https://bootstrap.pypa.io/get-pip.py" -o "pip-install.py"
     sudo python pip-install.py
     ```

   - The system displays the following similar information, indicating that the installation is successful:

     ```
     Successfully installed pip-7.1.2 setuptools-18.7 wheel-0.26.0
     ```

   c. Install the command line tool

   If the pip version is too low in the system, it will cause an error in the CLI installation. You can use the following command to upgrade the pip software before performing other operations: Use pip 7.x or later. If your pip is already the latest, skip this step.

A. Run the following command in the command line window to upgrade the pip:

```
sudo pip install -U pip
```

The system displays the following similar information, indicating that the upgrade is successful:

```
Successfully uninstalled pip-7.1.2
Successfully installed pip-8.1.2
```

A. Run the following command to install the Alibaba Cloud command line tool:

```
sudo pip install aliyuncli
```

The system displays the following similar information, indicating that the installation is successful:

```
Successfully installed aliyuncli-2.1.2 colorama-0.3.3 jmespath-
0.7.1
```

d. Configure the command-line tool

```
~ Sudo aliyuncli configure
Aliyun Access Key ID [********************a]: youraccesskeyid
Aliyun Access Key Secret [********************b]: youraccess
keysecret
Default Region Id [cn-hangzhou]: cn-hangzhou
Default output format [json]: json
```

2. Install the CmsSDK

- For the Windows operating system, run the following command in the command line window:

```
cd C:\Python27\Scripts
pip install aliyun-python-sdk-cms
```

- To update the SDK, run the following command:

```
pip install --upgrade aliyun-python-sdk-cms
```

- Linux Run the following command in the command line window:

```
sudo pip install aliyun-python-sdk-cms
```

- To update the SDK, run the following command:

```
sudo pip install –upgrade aliyun-python-sdk-cms
```

3. Report monitoring data

Use the API **PutEvent**.

- Reporting example for Windows:

```
aliyuncli.exe cms PutEvent --EventInfo "[{'content':'helloworld','
time':'20171013T170923.456+0800','name':'ErrorEvent','groupId':'
27147'}]"
```

- Linux Reporting example

```
aliyuncli cms PutEvent --EventInfo "[{'content':'helloworld','time
':'20171023T180923.456+0800','name':'ErrorEvent','groupId':'27147
'}]"
```

- If data is reported successfully, the system returns status code 200.

```
{
"Code":"200"
}
```

Error codes

Error code	Meaning
200	Normal
400	Syntax error in the client request
403	Verification failed, speed limit, not authorized
500	Internal server error

Sub-account authorization description

Subaccount authorization description When the AccessKey of a subaccount is used to report an event, the subaccount must be authorized to manage CloudMonitor. The "cannot upload event " prompt when reporting data if the sub-account is not authorized for cloud monitoring administra tion, Please use Ram to auth ".

1. Login access control Ram console.
2. Enter the user management menu.
3. Click **Authorize** next to the subaccount that is used to report data.

4. On the authorization page, select manage permissions for cloud monitoring, and click OK to save the authorization.

3.3 Signature Algorithm

Signing API requests.

1. Prepares the access secret key for the available Alibaba Cloud.

   The API Request to generate a signature that requires a pair of access secret keys (AccessKeyId/AccessKeySecret). You can use an existing AccessKey pair or create a new one . The AccessKey pair must be in the "Active" state.

2. Generate the request's signature string.

   The API signature string is used by the method, header, and body in the HTTP request. The information is generated together.

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

   `\n` from the formula above Represents a wrap escape character, `+` (plus sign) means a string connection operation, and other sections are defined as follows.

Name	Defining	Example
VERB	Method Name for HTTP Request	PUT, GET, POST, etc.
CONTENT-MD5	The MD5 value of the body section in the HTTP request (must be an upper-case string)	875264590688CA6171F6 228AF5BBB3D2
CONTENT-TYPE	HTTP	The type of body section in the request: application/json
DATE	Standard timestamp header in an HTTP request (following the RFC 1123 format, using the GMT Standard Time)	Mon, 3 Jan 2010 08:33:47 GMT
CanonicalizedHeaders	A string constructed by a custom header prefixed with X-CMS and X-ACS in an HTTP request	x-cms-api-version:0.1.0\nx-cms-signature
CanonicalizedResource	A string constructed by an HTTP request Resource (	/event/custom/upload

Name	Defining	Example
	specific construction method to meet in detail)	

The "CanonicalizedSLSHeaders" construction method is as follows:

1. All HTTP prefixed with `x-cms` and `x-acs` The name of the request header is converted to lower case letters.
2. All SLS custom request headers obtained in the previous step are sorted alphabetically in ascending order.
3. Any space separators at either end of the request headers and content are deleted.
4. Separate all the headers and content using the `\n` separator to form the final CanonicalizedLOGHeader.

The CanonicalizedResource construction method is as follows:

a. Set CanonicalizedResource to an empty string ("").
b. Put the URI you want to access, such as`/event/custom/upload`
c. If the request contains a query string (`QUERY_STRING`), then add "?" and the query string String tail add `?` at the end of the CanonicalizedResource string.

   Where`QUERY_STRING` is The string in the URL where the request parameters are sorted in classical order, where the parameter names and values are used `=` The string is formed, and the parameter name-value pair is sorted in ascending order, and then `&` The symbolic connection constitutes a string. This formula is illustrated below:

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

3. Generate the request's digital signature

   Currently, event reporting only supports one digital signature algorithm, that is, the default signature algorithm. hmac-sha1。 The entire signature formula is as follows:

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

3.4 Request header definition

The request header of event monitoring interface is defined as follows:

Header	Type	Description
Authorization	String	Content: acckeyid: signString
User-Agent	String	Client descriptions
Content-MD5	String	String produced after the request Body undergoes MD5 computation, results in uppercase. If the request has no Body, you can skip this request header.
Content-Length	Value	The length of the HTTP Request body defined in RFC 2616. If the request does not have a body part, the request header is not required.
Content-Type	String	Only support for application/ json.
date	String	Standard time stamp header of the HTTP request (follows RFC 1123 format and uses the GMT standard time) Mon, 3 Jan 2010 08:33:47 GMT. GMT
Host	string	The full Host Name of the HTTP request (does not include such as https :// Such an agreement head). For example, metrichub-cms-cn-hangzhou.aliyuncs.com
x-cms-api-version	string	API version current: 1.0
x-cms-signature	string	Signature algorithm, current: hmac-sha1.
x-cms-ip	String	IP of the machine reporting the event, 10.1.1.1.

3.5 Event monitoring best practices

Use cases

Exceptions may occur when the service is running. Some exceptions can be automatically restored by retry and other methods, while the others cannot. Serious exceptions can even lead

to customer business interruption. Therefore, a system is necessary to record these exceptions and trigger alarms when specific conditions are met. The traditional method is to print file logs and collect the logs to specific systems, for example, open-source ELK (ElasticSearch, Logstash , and Kibana). These open-source systems consist of multiple complex distributed systems. The complicated technology and high cost make independent maintenance challenging. CloudMonitor provides the event monitoring feature to effectively solve these problems.

The following examples explain how to use the event monitoring feature.

Case studies

1. Report exceptions

   Event monitoring provides two methods for data reporting, namely, JAVA SDK and OpenAPI. The following describes how to report data by using JAVA SDK.

   a. Add Maven dependency

   ```
   <dependency>
       <groupId>com.aliyun.openservices</groupId>
       <artifactId>aliyun-cms</artifactId>
       <version>0.1.2</version>
   </dependency>
   ```

   b. Initialize SDK

   ```
   // Here, 118 is the application grouping ID of CloudMonitor.
   Events can be categorized by applications. You can view group IDs
   in CloudMonitor application grouping list.
   CMSClientInit.groupId = 118L;
   // The address is the reporting entry of the event system, which
   is currently the public network address.  AccessKey and Secret/key
    are used for personal identity verification.
   CMSClient c = new CMSClient("https://metrichub-cms-cn-hangzhou.
   aliyuncs.com", accesskey, secretkey);
   ```

   c. Determine whether to asynchronously report the data.

   CloudMonitor event monitoring provides synchronous reporting policy by default. The good thing is that writing code is simple, and the reported events are reliable and free from data loss.

   However, such policy also brings some problems as well. Event reporting codes are embedded in business codes, which may block code running and affect the normal business in case of network fluctuations. Many business scenarios do not require events to be 100% reliable, so a simple asynchronous reporting encapsulation is sufficient. Write the event into

a LinkedBlockingQueue and perform batch reporting on the backend asynchronously using ScheduledExecutorService.

```
//Initialize queue and Executors:
private LinkedBlockingQueue<EventEntry> eventQueue = new
LinkedBlockingQueue<EventEntry>(10000);
private ScheduledExecutorService schedule = Executors.newSingleT
hreadScheduledExecutor();
// Report event:
//Every event contains its name and content. The name is for
identification and the content contains details of the event, in
which the full-text search is supported.
public void put(String name, String content) {
    EventEntry event = new EventEntry(name, content);
     // When the event queue is full, additional events are
discarded directly. You can adjust this policy as needed.
    boolean b = eventQueue.offer(event);
    if (! b) {
        logger.warn("The event queue is full, discard: {}", event
);
    }

//Submit events asynchronously. Initialize scheduled tasks.
Report events in batch by run every second.  You can adjust the
reporting interval as needed.
schedule.scheduleAtFixedRate(this, 1, 1, TimeUnit.SECONDS);
public void run() {
    do {
        batchPut();
    } while (this.eventQueue.size() > 500);

private void batchPut() {
    // Extract 99 events from the queue for batch reporting.
    List<CustomEvent> events = new ArrayList<CustomEvent>();
    for (int i = 0; i < 99; i++) {
        EventEntry e = this.eventQueue.poll();
        if (e == null) {
            break;

        events.add(CustomEvent.builder().setContent(e.getContent
()).setName(e.getName()).build());

    if (events.isEmpty()) {
        return;

     // Report events in batch to CloudMonitor. No retry or retry
 in SDK is added here. If you have high requirement for event
reliability, add retry policies.
    try {
        CustomEventUploadRequestBuilder builder = CustomEven
tUploadRequest.builder();
        builder.setEventList(events);
        CustomEventUploadResponse response = cmsClient.putCustomE
vent(builder.build());
        if (!" 200".equals(response.getErrorCode())) {
            logger.warn("event reporting error: msg: {}, rid:
 {}", response.getErrorMsg(), response.getRequestId());

    } catch (Exception e1) {
         logger.error("event reporting exception", e1);
```

d. Event reporting demo

- Demo1：http Controller exception monitoring

  The main purpose is to monitor if a large number of exceptions exist in HTTP requests . If the number of exceptions per minute exceeds a certain limit, an alarm is triggered. The implementation principle is to intercept HTTP requests by using Spring interceptor, servlet filter and other technologies. Logs are created in case of exceptions and alarms are triggered by setting alarm rules.

  The event reporting demo is as follows:

```
// Each event should be informative for searching and locating
. Here, map is used for organizing events and converted to Json
 format as event content.
Map<String, String> eventContent = new HashMap<String, String
>();
eventContent.put("method", "GET"); // http request method
eventContent.put("path", "/users"); // http path
eventContent.put("exception", e.getClass().getName()); //
Exception class name for searching
eventContent.put("error", e.getMessage()); // Error message of
exception
eventContent.put("stack_trace", ExceptionUtils.getStackTrace(e
)); // Exception stack for locating
// Finally submit the events in the preceding asynchronous
reporting method. Since no retry is performed in asynchronous
reporting, event loss of small probability may happen. However
, it is sufficient for alarms of unknown http exceptions.
put("http_error", JsonUtils.toJson(eventContent));
image.png](http://ata2-img.cn-hangzhou.img-pub.aliyun-inc.com/
864cf095977cf61bd340dd1461a0247c.png)
```

- Demo2: Monitoring of scheduled tasks on the backend and message consumption

  Like the preceding http events, many similar business scenarios require alarms. In the business scenarios such as backend tasks and message queue consumption, the events can be reported by using similar methods to achieve effective monitoring. When any exception occurs, alarms are triggered immediately.

```
//Event organization of the message queue:
Map<String, String> eventContent = new HashMap<String, String
>();
eventContent.put("cid", consumerId); // Consumer ID
eventContent.put("mid", msg.getMsgId()); // Message ID
eventContent.put("topic", msg.getTopic()); // Message topic
eventContent.put("body", body); // Message body
eventContent.put("reconsume_times", String.valueOf(msg.
getReconsumeTimes())); // The number of retries after message
failure
eventContent.put("exception", e.getClass().getName()); //
Exception class name in case of exception
```

```
eventContent.put("error", e.getMessage()); // Exception message
eventContent.put("stack_trace", ExceptionUtils.getStackTrace(e
)); // Exception stack
// Finally, report the event
put("metaq_error", JsonUtils.toJson(eventContent));
```

Check the event after reporting:

- Set alarms for queue message consumption exceptions:

- Demo 3: Record important events

  Another use case of events is to record important actions for later check without sending alarms. For example, operation logs for important business, password change/order change, remote logon, and so on.

3.6 Cloud product system event monitoring

System event monitoring provides users with unified statistics and query entry points for system events generated by different types of cloud products, enable users to clearly understand the state of the use of cloud products, making the cloud more transparent.

After Resource Classification by applying grouping, the system events generated by the product are automatically associated with the resources in the group, to help you integrate the information of all kinds of monitoring information, and to facilitate problems in your business, quickly analyze and locate problems.

The alarm function of the event is also provided, and the user can configure the alarm according to the level of event, receive notifications by SMS, mail, DingTalk, and so on or set alarm callbacks. Let users know the first time serious events and timely handling, the formation of online automation operation and operation closed loop.

Viewing System Events

- Approach 1

  1. Log in to the cloud monitoring console and enter the *event monitoring page*.
  2. The filter box selects system events to view events that occur over a specified period of time.

3. Click View Details in actions to view related event details.

- Approach 2

  If your instance is classified and managed by applying grouping, you can also enter a specific application grouping to view system events for related instances within the grouping.

  1. Log in to the cloud monitoring console and enter the application grouping page.
  2. Select go to the grouping details page and select event monitoring in the menu.
  3. The system events shown on the page are system events related to the instances in the group.

Set alert policies.

All system events can be configured to alert you when an event occurs. You can set this feature as follows:

1. Enter the System Events page, click Create alarm rules action for the appropriate event, and enter the create alarm Rules Page.
2. Select the event information and contacts you want to receive. When you select a contact, the contact receives events from all instances under the cloud account. When you select to apply a grouping, contacts that apply a grouping Association receive events generated by instances within the group.

Supported cloud Product System Events

- ECS System Events

Event name	Status	Event meaning	Event level
Instance: maid. Reboot	正在执行	Instance restart started due to instance error	Critical
Instance: maid. Reboot	Executed	Instance restart end due to instance error	CRITICAL
Instance:SystemFailure.Reboot	Executing	Restart started due to system error instance	CRITICAL
Instance:SystemFailure.Reboot	Executed	End of reboot due to system error instance	CRITICAL

Event name	Status	Event meaning	Event level
Instance:SystemMaintenance.Reboot	Scheduled	Scheduled reboot due to system maintenance instance	CRITICAL
Instance:SystemMaintenance.Reboot	Avoided	Due to system maintenance instance scheduled restart has been circumserted	CRITICAL
Instance:SystemMaintenance.Reboot	Executing	Due to system maintenance instance plan restart execution	CRITICAL
Instance:SystemMaintenance.Reboot	Executed	Due to system maintenance instance scheduled restart completed	CRITICAL
Instance:SystemMaintenance.Reboot	Canceled	Due to system maintenance instance scheduled restart canceled	CRITICAL
Instance:SystemMaintenance.Reboot	Failed	Failed to restart due to system maintenance instance schedule	CRITICAL
Disk:Stalled	Executing	Disk performance has been severely affected to start	CRITICAL
Disk:Stalled	Executed	Disk performance is severely affected to end	CRITICAL

- SLB System Events

Event name	Event meaning	Event level
CertKeyExpired_1	The certificate will expire in 1 day	WARN
CertKeyExpired_3	The certificate will expire in 3 days	WARN
CertKeyExpired_7	The certificate will expire in 7 days	WARN

Event name	Event meaning	Event level
CertKeyExpired_15	The certificate will expire in 15 days	WARN
CertKeyExpired_30	The certificate will expire in 30 days.	WARN
CertKeyExpired_60	The certificate will expire in 60 days.	WARN

- OSS System Events

Event name	Event meaning	Event level
BucketEgressBandwidth	Bucket downstream bandwidth exceeds reporting threshold	INFO
BucketEgressBandwidthThresholdExceeded	Bucket downstream bandwidth exceeds streaming threshold	WARN
BucketIngressBandwidth	Bucket upstream bandwidth exceeds reporting threshold	INFO
BucketIngressBandwidthThresholdExceeded	Bucket upstream bandwidth exceeds flow control threshold	WARN
UserEgressBandwidth	User downstream bandwidth exceeds reporting threshold	INFO
UserEgressBandwidthThresholdExceeded	User downstream bandwidth exceeds streaming threshold	WARN
UserIngressBandwidth	User upstream bandwidth exceeds reporting threshold	INFO
UserIngressBandwidthThresholdExceeded	User upstream bandwidth exceeds flow control threshold	WARN

3.7 Use the system event alarm function

Scenario

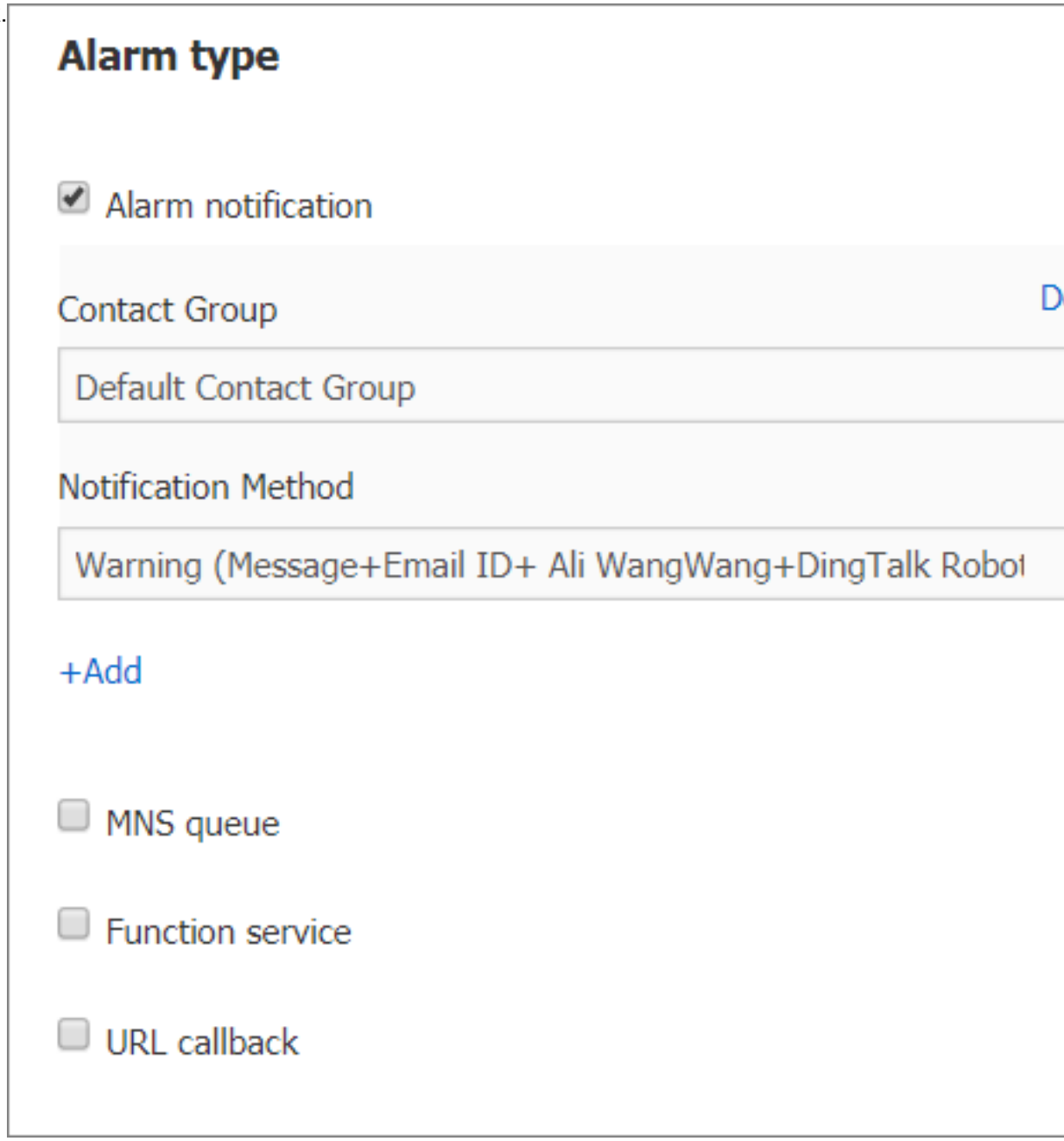
When the Alibaba Cloud product encounters a system abnormality, the alarm function of event monitoring provides you with the following two notification capabilities, so that you can know the event and automate the abnormality handling in time:

- Provides alarms for the event by means of voice calls, text messages, emails, and DingTalk group.
- Distributes the event to the user's MNS queue, function service, and URL callback.

Create an alarm rule

1. Log on to the *CloudMonitor console*.
2. In the left navigation pane, select **Event Monitoring**.
3. On the **Alarm Rules** tab page, click **Create event alerts** in the upper right corner. The **Create / modify event alerts** dialog box appears.
4. In the **Basic Information** area, fill in the alarm rule name.
5. In the **Event alert** area, complete the following information:
   a. Event Type: Select **System Event**.
   b. Product Type, Event Level, Event Name: fill in according to the actual situation
   c. Resource Range: If you select **All Resources**, notifications are sent in accordance with the configuration for any resource-related events. If you select **Application Groups**, notifications are sent only when the event occurs for the resources in the specified group.

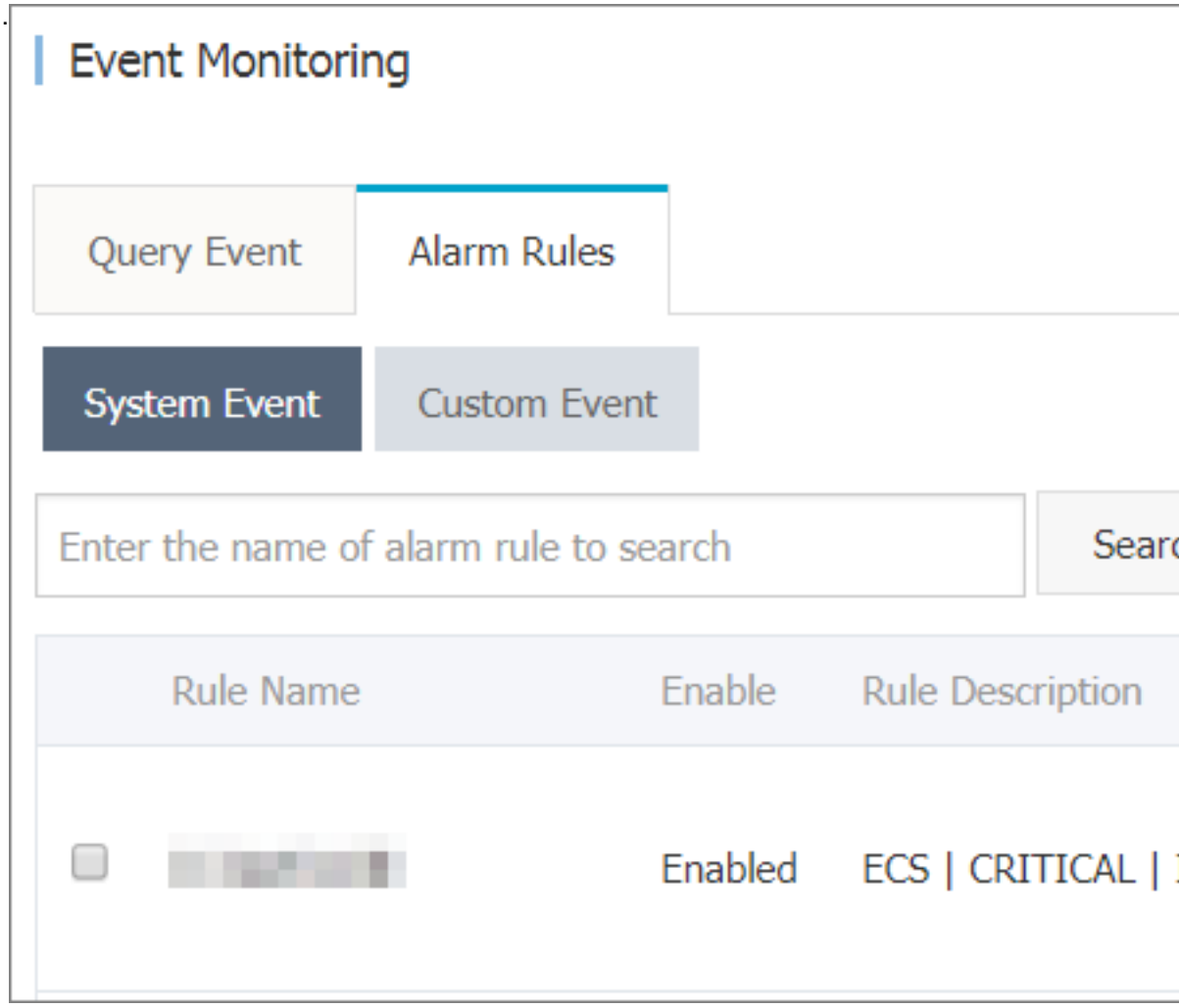
6. Select the **Alarm type**. CloudMonitor supports four alarm types: alarm notification, MNS queue, function service, and URL callback.



Test an alarm rule

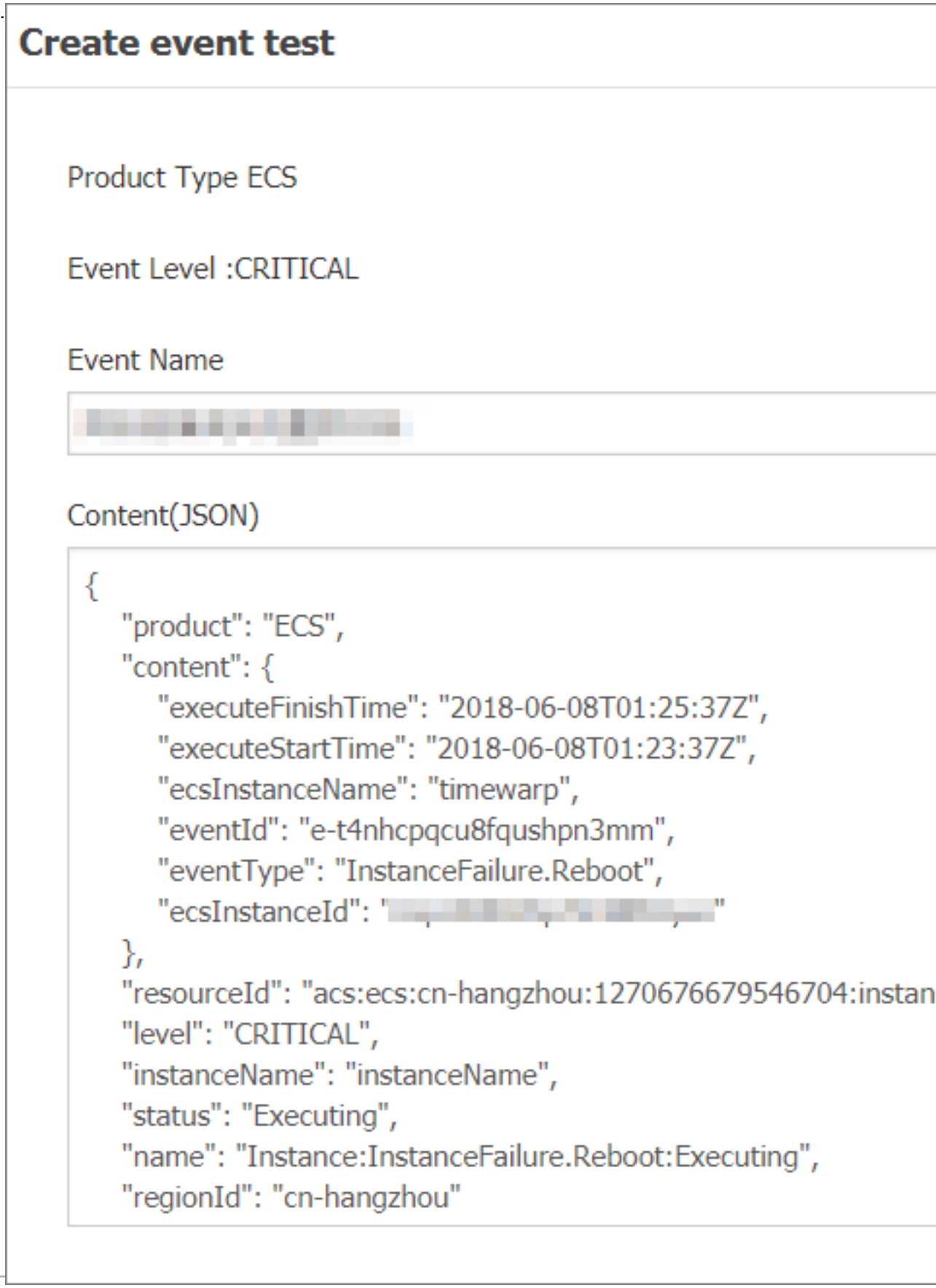
You can use the testing function of the system event to simulate the occurrence of system events , so as to verify whether the MNS queue set in the alarm rule can receive the time normally, and whether the function of Function Compute can be triggered normally.

1. Go to the Alarm Rules tab page for event monitoring.



2. Click **test** in the Actions column.
3. Select the event to be tested. The corresponding event content will be displayed. You can change such fields as the instance ID in the content according to the actual situation.

4. Click **OK**. The system will send an event based on the content, triggering alarm notification, MNS queue, function service, and URL callback set in the alarm rule.



4 Availability monitoring

4.1 Manage availability monitoring

Availability monitoring periodically detects the responsiveness of specified local paths or ports and sends an alarm notification when the response lapses or an error status code is returned. This helps you to immediately detect when the local or remote services are unresponsive.

Note:

- The availability monitoring function requires the CloudMonitor agent to work appropriately. You should ensure that the CloudMonitor agent is preinstalled on the relevant machines.
- Monitoring is performed every minute.

View availability monitoring tasks

1. Log on to the *CloudMonitor console*.
2. Select **Application Groups** from the left-side navigation pane to go to the **Application Groups** page.
3. Select the application group for which you want to create an availability monitoring task, and click the **Group name** to go to the **Application Groups** page.
4. Select **Availability Monitoring** from the left-side navigation pane to go to the **Availability Monitoring** page.
5. Click **Create Configuration** in the upper-right corner of the page to go to the **Create Local Health Check** page.
6. Select a test source. You can configure the same testing rules for some or all machines in the group.
7. Select the test type and test target. This function supports URL/IP address, RDS, OSS, and Redis. If you select RDS or Redis, the interface will show the relevant instances and addresses in the group.

   Note:

   - If you select HTTP for the test, it will allow you to configure matching rules for HEAD, GET, and POST request methods and returned values.
8. Select an **Alarm Configuration**. Alarms can be configured by status code or response time. An alarm is triggered when the returned status code is the same as the setting or no response

is returned after the predefined timeout threshold has lapsed. The alarm will be sent to the contact group associated with the application group.

Note:

- Status code alarm: An alarm is triggered when the returned status code is the same as the setting.
- Notification method: It is the method by which alarm notifications are sent.
- Advanced configuration: Either channel silence time or effective time can be used. The channel silence time is the period after which an alarm is sent again. And also, if the exception persists even after the alarm is triggered. The effective time is the time when an alarm rule becomes effective. The availability monitoring function checks the metric data and determines whether to trigger an alarm at the time when the alarm rule is effective.

View availability monitoring tasks

1. Log on to the *CloudMonitor console*.
2. Select **Application Groups** from the left-side navigation pane to go to the **Application Groups** page.
3. Select the application group for which you want to create an availability monitoring task, and click the **Group name** to go to the **Application Groups** page.
4. Select **Availability Monitoring** from the left-side navigation pane to go to the **Availability Monitoring** page.
5. The list will display all the monitoring tasks available for that application group.

View monitoring results

1. Log on to the *CloudMonitor console*.
2. Select **Application Groups** from the left-side navigation pane to go to the **Application Groups** page.
3. Select the application group for which you want to create an availability monitoring task, and click the **Group name** to go to the **Application Groups** page.
4. Select **Availability Monitoring** from the left-side navigation pane to go to the **Availability Monitoring** page.

Note:

The list will display the following monitoring results:

- When no alarm is triggered, the list shows that the number of machines that have triggered alarm is zero.
- When an alarm is triggered, the list shows the number of machines that have triggered alarm. Click the number to view the machine details.

Modify availability monitoring tasks

1. Log on to the *CloudMonitor console*.
2. Select **Application Groups** from the left-side navigation pane to go to the **Application Groups** page.
3. Select the application group for which you want to create an availability monitoring task, and click the **Group name** to go to the **Application Groups** page.
4. Select **Availability Monitoring** from the left-side navigation pane to go to the **Availability Monitoring** page.
5. Select the task you want to modify and click **Modify** from the **Actions** column to go to the edit page.
6. Enter all the relevant details and click **Save** to confirm the changes.

View alarm history

1. Log on to the *CloudMonitor console*.
2. Select **Application Groups** from the left-side navigation pane to go to the **Application Groups** page.
3. Select the application group for which you want to create an availability monitoring task, and click the **Group name** to go to the **Application Groups** page.
4. Select **Alarm History** from the left-side navigation pane to go to the **Alarm History** page and here you can view the alarm history.

Enable or disable a monitoring task

You can enable or disable availability monitoring tasks. A disabled task does not monitor or trigger alarms. The availability monitoring task can only restart monitoring and triggering alarms as per the set alarm rules, when the tasks are reinstated.

1. Log on to the *CloudMonitor console*.
2. Select **Application Groups** from the left-side navigation pane to go to the **Application Groups** page.

3. Select the application group for which you want to create an availability monitoring task, and click the **Group name** to go to the **Application Groups** page.
4. Select **Availability Monitoring** from the left-side navigation pane to go to the **Availability Monitoring** page.
5. Select the task you want to enable or disable and click **Enable** or **Disable** from the **Actions** column to modify the task status as per the requirement.

4.2 Local service availability check

Following are the guidelines that will help you to monitor the availability of local service processes and send alarms when the service response lapses or returns an error code.

Note:

- This function requires the CloudMonitor agent to work appropriately. Hence, ensure that CloudMonitor agent is preinstalled on the relevant machines.
- An availability test is performed every minute.
- Before using this function, *create application groups*.

Procedure

1. In the *CloudMonitor console*, select **Application Groups** from the left-side navigation pane.
2. Select the target application group and click **Group Name** to go to the application group details page.
3. Select **Availability Monitoring** from the left-side navigation pane.
4. Click **Create Configuration** in the upper-right corner of the page. The **Create Local Health Check** dialog box is displayed.

   Monitoring Configurations area:

   - **`Target Server`**: This is the machine that initiates the test. The local service availability monitoring test source and test target are the same machine.
   - **`Detection Type`**: Select `URL or IP address`.
   - **`Detection Target`**: The syntax of `HTTP(S)` is `localhost:port/path` and that of **TELNET** is `127.0.0.1:port`. For example, to test whether Tomcat is responsive, select `HTTP(S)` and enter `localhost:8080/monitor`; to test MySQL connectivity, select `TELNET` and enter `127.0.0.1:3306`.

   Alarm Configuration area:

Alarms can be configured by **`status code`** or **`response time`**. An alarm is triggered when the returned status code is the same as the setting or no response is returned after the predefined timeout threshold has lapsed. The alarm notification will be sent to the contact group associated with the application group. For local availability monitoring, set the status code setting to greater than 400.

- **Status code**: An alarm is triggered when the returned status code is the same as the setting.
- **Notification method**: It is the method by which alarm notifications are sent.
- **Advanced Configuration**
  - **`Muted For`**: the period of time after which an alarm is sent again if the exception persists after the alarm is triggered.
  - **`Effective From`**: the time when an alarm rule becomes effective. You can configure this parameter based on your actual needs.

5. Click **OK** to save the configurations. A local service availability monitoring task has been created successfully. If your service does not respond, a message or an email will be sent to you and the number of abnormal instances will be displayed in the list. Then, click the **number of exceptions** to view details about the abnormal instances.
6. Click the **number of abnormal machines** to view details about the abnormal machines.

4.3 Status code description

The following lists the custom status codes returned when an exception is detected through availability check.

Protocol type	Status code	Definition
HTTP	610	Timeout. No response within 5 seconds after the HTTP request was issued as a timeout.
HTTP	611	The probe failed.
Telnet	630	Timeout, no response within 5 seconds, as a timeout.
Telnet	631	The probe failed.

5 Log monitoring

5.1 Log monitoring overview

In the enterprise-class business operations and operations scene, Log is playing an increasingly important role. Simple localized storage of business logs makes it difficult to mine the real value of the data behind the log. After the logs are stored on the centralized server, it is an increasingly urgent demand for enterprises to process it as an indicator of Operation Guidance and operation guidance.

Difficulties to be faced

While log processing, visualization, and alarms are urgently needed by many businesses, but it is never easy to process the valuable data that is coming true of the log. For example, the following questions:

- The diversity of log format and the logic of data acquisition and processing are complicated.
- Ability to analyze massive log data.
- The storage of processing results.
- Visualization of data.
- Communication with alarm service and implementation of automation operation and operation.
- Integration with basic monitoring data such as servers.

In general, a log-based Monitoring and Analysis Service needs to address all of the above issues in order to form a closed-loop business, perfect solution to corporate monitoring operations and operational demands.

Traditional Architecture

The classic scheme of log monitoring is elk, and it is believed that everyone is not new. Elk is a mature log monitoring scheme with simple configuration and gorgeous front-end display, open source and many other features. But ELKis still a big investment cost for the general business:

- The architecture and technology Stack are complex, and the cost of development and operation is high.
- You can only resolve some of the issues in log monitoring. Unable to address alarm, data integration and other important needs.

Log monitoring Solution

Due to the large cost of elk investment, most of the corporate log processing scenarios are simple , such

- Alarm the keywords in the log
- QPS, RT in statistical unit time
- PV, UV in unit of measure time

Traditional enterprise users who use traditional architectures to address these common simple requirements, put in a lot of time and people to build a huge attack on the city weapons, pay a heavy cost of operation and operation, indeed, there are some unpaid losses.

In response to the above issues, Alibaba Cloud monitoring and logging services combined, launched a very lightweight, but a comprehensive, easy-to-use solution-log monitoring.

Cloud monitoring-the goal of log monitoring is to achieve complex traditional log monitoring capabilities, convert to mouse several times gently click.

Log monitoring Closed Loop

Overview of using processes

1. Collects logs through the Log service.
2. Authorization logs give cloud monitoring readable permissions to query your logs.
3. Use log monitoring to define how log data is processed for monitoring metrics.
4. Set alarm rules for monitoring metrics, define chart displays (optional).

Our advantage

- Easy to use, good to use.
- Be free from provisioning at any time (you only need to provision the Log service to collect the Log Service locally), the details of the complex, low-level technology are all transparent to you.
- Perfect Combination of cloud monitoring host monitoring, cloud service monitoring, site monitoring, application grouping, dashboard, alarm service, A complete closed loop of monitoring is formed. Provide you with a unified, comprehensive perspective on everything you need to know about monitoring.
- Based on the Alibaba Cloud Apsara monitor service, it gives you a stable and reliable experience.

- Complete SaaS services with virtually no operating costs.
- Cost Advantage: virtually no time and labor costs will help you complete your log monitoring needs faster.

5.2 Managing log monitoring

You can create, view, modify, and delete monitor items in log monitoring.

Create log Monitor

Create a log monitor to define how the log data is processed and whether the monitor entries belong to application groups.

Parameter descriptions

The following are the parameter descriptions for the new log monitor page:

- Group name: the name of the apply grouping. You can add monitoring items to specific application groups.
- Associated resources: select the processed Log service data source.
- Geographic: the geographic area of the log service.
- Log project: Project for the log service.
- Log logstore: The logstore for the log service.
- Analyze logs: defines how the Log Service parses log data.
- Monitor name: defines the name of a monitor indicator.
- Statistical Methods: A function method that refers to how log data is computed during a statistical period. Includes: Sum, maximum, minimum, average, sumps, countps, P50, request p75, P90, P95, p98, P99.
  - Sum: calculates the sum of the specified field values in 1 minute.
  - Maximum Value: calculates the maximum value of the specified field value during the statistics period.
  - Minimum value: calculates the minimum value of the specified field value during the statistics period.
  - Average: calculates the average of the specified field values during the statistics cycle.
  - Countps: calculates the average per second after the specified field during the statistics cycle for count.
  - Sumps: calculates the average per second after a specified field during the statistics cycle for sum.

- Distinct: calculates the number of times a specified field appears during the statistics cycle after being resounding.
- Ask for p75: calculates a 75th-Cent number of digits for the specified field in 1 minute. Take the statistical results of RT as 30 ms for example, indicating 75% The request rt is less than 30 MS.
- Distribution: calculates the number of log lines for a range specified during a period, for example, by counting the number of status codes with an HTTP request of 5xx in 1 minute, it is defined (499,599). Statistics are left open and right closed.

- Extension field: the extension field provides the functionality of four operations for the results in the statistical method. For example, the total number of HTTP status code requests configured in the statistics method totalnumber, HTTP status code greater than 499 request 5 xxnumber , then you can calculate the server error rate by extending the field: 5 xxnumber/totalnumber * 100.
- Log Filtering: equivalent to where conditions in SQL. Processing all data is indicated by not filling out. Assume that there is a level: Error field in the log, and you need to count every minute The number of times error occurred, and the statistical method can be defined as a sum for level, and level = error.
- Group-by: spatial dimension aggregation of data, equivalent to group by in SQL, groups monitoring data based on the specified dimension. If the group You do not select any dimensions. Aggregating all monitoring data according to the aggregation method.
- Select SQL: converts the above analysis into a SQL-like statement, it is convenient for you to understand how the data is processed.

Operation Steps

1. Log in to cloud monitor and enter the log monitor page.
2. Click new log monitor in the upper-right corner of the page to enter the new log monitor page.
3. Select associated resources.
4. Defines how log data is parsed. Click Preview to see the latest statistics for reference.
5. (Optional) quickly create alarm rules to send mail by default.
6. (Optional) add monitoring items to an application grouping to manage.

View log monitoring

Here, you can view the monitor entries of the log, and if you want to view the processed monitor data, you can refer.

1. Log in to cloud monitor and enter the log monitor page.
2. You can view information such as the monitor's log data source, filter, and statistical method definitions in the list.

Modify log monitoring

1. Log in to cloud monitor and enter the log monitor page.
2. Select the monitor name that needs to be modified, click the edit button to enter the Edit page.
3. Refer to the create log monitor step to modify the parameters that need to be modified.

Delete log Monitor

Note:

After the monitor is deleted, you can still query through the API to the monitor data before the delete point in time.

1. Log in to cloud monitor and enter the log monitor page.
2. Select the name of the monitor item that needs to be modified and click the delete button to specify that the monitor item will be deleted.

5.3 Viewing Monitoring Data

Once the monitoring entries for log monitoring have been defined, cloud monitoring provides three ways to view monitoring data:

- View directly on the monitor tab of the log monitor.
- Adds a log-monitored chart to the app grouping.
- Add a log monitor chart to the dashboard (please look forward).

To view monitor data directly

1. Log in to cloud monitor and enter the log monitor page.
2. Select the monitor item for which you want to view data, and click the monitor chart in the monitor item name or action. You can view monitoring data from the monitoring details page.

Adding log monitor data to app grouping

Before adding a log monitor chart in the app grouping, add the corresponding monitor to the log grouping first. The following are the steps to add a log monitor chart to an app grouping.

1. Log in to cloud monitoring, enter application grouping, and select the grouping that needs to be added to the monitor chart, enter the grouping details page.

2. Click the Add monitor Chart Button in the monitor Chart Section of the page to enter the Add monitor chart page.
3. After you select the information about the log monitor in the page, click Save to finish adding the monitor chart.

5.4 Authorization log monitoring

Master account authorization log monitoring authorization

When you use the log monitoring feature, you need to authorize cloud monitoring to query the permissions of your log service, please refer to the steps below for the authorization method.

1. Log on to the log monitoring page by logging in to the cloud monitoring console. If the master account does not authorize cloud monitoring access to your log service, prompt: "You have not yet authorized cloud monitoring to read your log, click authorize ".
2. Click on the authorization after entering the authorization page, click agree to the authorization , and then complete the authorization.

Sub-accounts using log monitoring

- Sub-account authorization log monitoring

  Sub-accounts require the following permissions to authorize cloud monitoring to read Log service data:

  - Cloud monitoring read-only (aliyuncloudmonitorreadonlyaccess) or read-write (aliyuncloudmonitorfullaccess) permissions.
  - Manages access management service (RAM) (maid) permissions.

  With the above conditions, the sub-account can authorize log monitoring to the same as the main account, the authorization process is consistent with the master account.
- Sub-accounts using log monitoring

  - Manage log monitoring (view, new, modify, and so on): You need to authorize cloud monitoring Read and Write Permissions Read-Only permissions for maid and Log Service Aliyunramfullaccess.
  - Query log monitoring data: you only need to authorize cloud monitoring read-only Permissions Only if you can.

5.5 Log monitoring common problems troubleshooting

1. The creation of the monitor was successful, but the monitor chart has no data.
   - Checks if the accesskey has been activated. See ############ of <keyword> prerequisite.
   - Click Log monitor list corresponding to the Monitor's edit, in SQL, check to see if the generated SQL contains Chinese, and that the SQL cannot contain Chinese.
   - Ensure that the statistics methods set and the LOG filter criteria match the log data on them, you can click the log monitor list for the editing of the monitor item, see if there is any matching log data in the log Preview (displays the last 100 in the last 1 hour) strip data), or go to the log service console to see if there is any matching log data for longer periods of time.
2. Insufficient alarm data

   Check if the monitor chart has data, if the chart does not have data, according to question 1, the alarm rule will have insufficient data.
3. Monitor Data reaches threshold, but no alarm is received

   Checks whether the alarm notification enters channel silence. When an alarm is issued, if the exception is not handled within 24 hours, the alarm is not triggered again within 24 hours.
4. Page error when creating log Monitor

   The following error occurred when creating the log monitor page, because the accesskey was not activated, see the usage prerequisite.

6 Cloud service monitoring

6.1 RDS monitoring

Cloud monitoring through monitoring metrics such as disk usage, iops usage, number of connections usage, CPU usage, and so on, gives you an insight into the running status of your RDS. The user buys the RDS After the product, cloud monitoring automatically collects data for the above four monitors, no additional action is required.

Note:

- The RDS only provides monitoring and alarm services for primary and read-only instances.
- Cloud monitoring creates alarm rules by default for each primary and read-only instance. Content is CPU usage> 80%, number of connections usage> 80%, iops usage> 80%, disk usage > 80%. SMS messages and mail notifications to cloud account contacts when the threshold is exceeded.

Monitoring Services

- Monitoring item description

Monitoring items	Meaning	Dimensions	Unit	Minimum monitor Granularity
Disk usage	Percentage of disk space used in a database instance	Instance	Percentage	5 minutes
IOPS usage	Number of IO requests per second for database instance	Instance	Percentage	5 minutes
Connections usage	The number of connections is the number of instances that an application can connect to an RDS. Number	Instance	Percentage	5 minutes

Monitoring items	Meaning	Dimensions	Unit	Minimum monitor Granularity
	of connection s usage is the percentage of the number of connections that have been used			
CPU utilization	Instance of CPU usage, database memory size depends on the performance of the CPU	Instance	Percentage	5 minutes
Memory usage	Memory Used ratio in database instance, only MySQL type database currently supports memory instance Rate	Instance	Percentage	5 minutes
Read-only instance Delay	MySQL read-only instance latency	Instance	Second	5 minutes
Network incoming traffic	Instance input flow per second	Instance	Bits/s	5 minutes
Network Traffic	Average output traffic per second	Instance	Bits	5 minutes
Instance failure	Event Type metrics, alarm rules can be set	-	-	-
Instance master standby switch	Event Type metrics, alarm rules can be set	-	-	-

In-network and out-of-network traffic is supported only for MySQL and SQL Server database types.

- Viewing Monitoring Data

  1. Log on to the *CloudMonitor console*.
  2. Go to cloud Database monitored by cloud services A list of RDS instances.
  3. Click the Instance name or the monitor chart in the operation to go to the monitor details page.
  4. Click the size chart toggle button to toggle the larger image display (optional).

Alarm service

- Parameter descriptions

  — Monitoring: the monitoring metrics provided by the RDS.

  — Statistical Cycle: the alarm system checks if your monitoring data exceeds the alarm threshold for this cycle. For example, to set a memory usage alarm rule, the statistics cycle is 1. Minutes, and an interval of 1 minute checks if memory usage exceeds the threshold.

  — Statistical Methods: Statistical Methods refer to settings that exceed the threshold range. You can set the average, maximum, minimum, count, and value in a statistical method.

    - Average: the average of the monitored data during the statistical cycle. The result is an average of all monitoring data collected within 15 minutes, when this average is greater than 80. Only when the threshold is exceeded.
    - Maximum: the maximum value of the monitor data during the statistics cycle. The maximum value of monitoring data collected during the statistical cycle exceeds the threshold of 80.
    - Minimum: the minimum value of the monitored data during the statistics cycle. The minimum value for monitoring data collected during the statistical cycle exceeds the threshold of 80.
    - Value: Sum of monitoring data during the statistics cycle. Sum up the monitoring data collected during the statistical period with more than 80% results after the sum That is, the threshold is exceeded. Such statistical methods are required for traffic-class metrics.

  — Alarm after several consecutive exceeds threshold: refers to a number of consecutive statistical cycle monitoring items whose values continue to exceed the threshold to trigger an alarm.

    For example, set CPU usage to more than 80% alarms, with a statistical cycle of 5 minutes, alarm after 3 consecutive times exceeds threshold, first time detection CPU usage exceeds 80% Alarm notification will not be issued when. If the CPU usage rate exceeds 80% again

in the following 5-minute period, it still does not trigger an alert. The third probe still exceeds 80% Alarm notification will be issued only when. That is, from the first time the actual data exceeds the threshold to the final alarm rule, the minimum time required is statistical cycle X (number of consecutive probes-1) = 5 x (3-1) = 10 minutes.

- Set alarm rules

  1. Log on to the *CloudMonitor console*.
  2. Go to cloud database RDS monitored by cloud services List of instances.
  3. Click the alarm rule in the instance List action to enter the alert Rule Page for the instance.
  4. Click new alarm rule in the upper-right corner of the alarm Rule Page to create an alarm rule based on the parameter.

6.2 Server Load Balancer monitoring

CloudMonitor displays the status of Server Load Balancer based on seven metrics, including inbound traffic and outbound traffic. This helps you to monitor the operational status of instances and allows you to configure alarm rules for these metrics. Once you create a Server Load Balancer instance, CloudMonitor automatically collects data for the following metrics.

Monitoring service

- Metrics

  — layer-4 metrics

Metric	Definition	Dimension	Unit	Minimum monitoring granularity
Inbound traffic	Traffic consumed by access to the Server Load Balancer from the Internet.	Instance	Bps	1 minute
Outbound traffic	Traffic consumed by access to the Internet from the Server Load Balancer.	Instance	Bps	1 minute

Metric	Definition	Dimension	Unit	Minimum monitoring granularity
Incoming packet count	Number of request packets Server Load Balancer receives per second	Instance	Count/second	1 minute
Outgoing packet count	Number of request packets Server Load Balancer sends per second	Instance	Count/second	1 minute
New connection count	The number of first-time SYN_SENT statuses for TCP three-way handshakes in a statistical period	Instance	Count	1 minute
Active connection count	The number of connections in the ESTABLISHED status in the current statistical period	Instance	Count	1 minute
Inactive connection count	The number of all TCP connections except connections in the ESTABLISHED status	Instance	Count	1 minute
				1 minute

Metric	Definition	Dimension	Unit	Minimum monitoring granularity
	The average number of dropped connections per second for a port			
		Instance	Count/Second	1 minute
Inbound instance-discarded packets count	Number of inbound packets discarded by the instance per second	Instance	Count/Second	1 minute
Outbound instance-discarded packets count	Number of outbound packets discarded by the instance per second	Instance	Count/Second	1 minute
Inbound instance-discarded traffic	Amount of inbound traffic discarded by the instance per second	Instance	bit/s	1 minute
Outbound instance-discarded traffic	Amount of outbound traffic discarded by the instance per second	Instance	bit/s	1 minute

Metric	Definition	Dimension	Unit	Minimum monitoring granularity
Maximum number of concurrent connections for the instance	Total number of connections for the instance (sum of the number of active connections and the number of inactive connections)	Instance	Count/Second	1 minute
Instance new connections	Number of times that the first SYN_SENT state occurs in the case of three TCP handshakes on average per second for the instance in a statistical period	Instance	Count/Second	1 minute
Instance inbound packet count	Number of request packets received by the instance per second	Instance	Count/Second	1 minute
Instance outbound packet count	Number of packets sent by the instance per second	Instance	Count/Second	1 minute
Instance inbound traffic	Traffic consumed by access to the Server Load Balancer instance from the Internet	Instance	bit/s	1 minute

Metric	Definition	Dimension	Unit	Minimum monitoring granularity
Instance outbound traffic	Traffic consumed by access to the Internet from the Server Load Balancer instance	Instance	bit/s	1 minute

- Layer-7 metrics

Metric	Definition	Dimension	Unit	Minimum monitoring granularity
Port QPS	QPS from listening dimension	Port	Count/Second	1 minute
Port RT	Average request delay from port dimension	Port	ms	1 minute
Port status codes 2xx count	Number of status codes 2xx the SLB returned to the client from port dimension	Port	Count/Second	1 minute
Port status codes 3xx count	Number of status codes 3xx the SLB returned to the client from port dimension	Port	Count/Second	1 minute
Port status codes 4xx count	Number of status codes 4xx the SLB returned to the client from port dimension	Port	Count/Second	1 minute

Metric	Definition	Dimension	Unit	Minimum monitoring granularity
Port status codes 5xx count	Number of status codes 5xx the SLB returned to the client from port dimension	Port	Count/Second	1 minute
Port other status codes count	Number of other status codes the SLB returned to the client from port dimension	Port	Count/Second	1 minute
Port upstream status codes 4xx count	Number of status codes 4xx the RS returned to the SLB from port dimension	Port	Count/Second	1 minute
Port upstream status codes 5xx count	Number of status codes 5xx the RS returned to the client from port dimension	Port	Count/Second	1 minute
Port UpstreamRT	Average request delay from RS to proxy from port dimension	Port	ms	1 minute
Instance QPS	QPS from instance dimension	Instance	Count/Second	1 minute
Instance RT	Average request delay from instance dimension	Instance	Count/Second	1 minute
Instance status codes 2xx count	Number of status codes	Instance	Count/Second	1 minute

Metric	Definition	Dimension	Unit	Minimum monitoring granularity
	2xx the SLB returned to the client from instance dimension			
Instance status codes 3xx count	Number of status codes 3xx the SLB returned to the client from instance dimension	Instance	Count/Second	1 minute
Instance status codes 4xx count	Number of status codes 4xx the SLB returned to the client from instance dimension	Instance	Count/Second	1 minute
Instance status codes 5xx count	Number of status codes 5xx the SLB returned to the client from instance dimension	Instance	Count/Second	1 minute
Instance other status codes count	Number of other status codes the SLB returned to the client from instance dimension	Instance	Count/Second	1 minute
Instance upstream status codes 4xx count	Number of status codes 4xx the RS returned to the SLB	Instance	Count/Second	1 minute

Metric	Definition	Dimension	Unit	Minimum monitoring granularity
	from instance dimension			
Instance upstream status codes 5xx count	Number of status codes 5xx the RS returned to the SLB from instance dimension	Instance	Count/Second	1 minute
Instance upstream RT	Average request delay from RS to proxy from instance dimension	Instance	ms	1 minute

Note:
New connection count, active connection count, and inactive connection count all indicate the TCP connection requests from clients to the Server Load Balancer.

- View metric data

  1. Log on to *CloudMonitor console*.
  2. Go to the **Server Load Balancer** instance list under **Cloud Service Monitoring**.
  3. Click an instance name in the product instance list or click **Monitoring Charts** from the **Actions** column to access the instance monitoring details page.
  4. (Optional) Click the Chart Size button to switch to large chart display.

Alarm service

- Parameter descriptions

  — Metrics: The monitoring indicators provided by Server Load Balancer.

  — Statistical cycle: The alarm system that checks whether your monitoring data has exceeded the alarm threshold value based on the statistical cycle. For example, if the statistical cycle of the alarm rule for memory usage is set to one minute, the system checks whether the memory usage has exceeded the threshold value every other minute.

— Statistic: This sets the method used to determine if the data exceeds the threshold. You can set Average, Maximum, Minimum, and Sum in Statistic.

- Average: The average value of metric data within a statistical cycle. The statistical result is the average of all metric data collected within 15 minutes. An average value of over 80 % is deemed to exceed the threshold.
- Maximum: The maximum value of metric data within a statistical cycle. When the maximum value of the metric data collected within the statistical cycle is over 80%, the value exceeds the threshold.
- Minimum: The minimum value of metric data within a statistical cycle. When the minimum value of the metric data collected within the statistical cycle is larger than 80%, then the value exceeds the threshold.
- Sum: The sum of metric data within the statistical cycle. When the sum of the metric data collected within the statistical cycle is over 80%, it exceeds the threshold. The preceding statistics are needed for traffic-based indicators.

— Trigger alarm after the threshold value has exceeded several times: This refers to the alarm that is triggered when the value of the metric continuously exceeds the threshold value in several consecutive statistical cycles.

For example, you may set the alarm to go off when the CPU usage rate exceeds 80% within a 5-minute statistical cycle after the threshold value is exceeded for three times. If the CPU usage rate is found to exceed 80% for the first time, no warning notification is sent. No alarm is reported if the CPU usage rate exceeds 80% only twice in a row. An alarm is reported only if the CPU usage rate exceeds 80% for the third time. That is, from the first time when the actual data exceeds the threshold to the time when the alarm rule is triggered , the minimum time consumed is the statistical cycle (the quantity of consecutive detection times - 1) = 5 * (3-1) = 10 minutes.

- Set an alarm rule

1. Log on to *CloudMonitor console*.
2. Go to the **Server Load Balancer** instance list under **Cloud Service Monitoring**.
3. Click **Alarm Rules** from the **Actions** column to access the instance's alarm rules page.
4. Enter all the relevant information in the required fields, and click **Confirm** to create a new alarm rule.

6.3 OSS monitoring

OSS The Object Service Storage (OSS) monitoring service provides you the metric data which describes basic system operation status, performance, and metering. It also provides a custom alarm service to help you track requests, analyze usage, collect statistics on business trends, and promptly discover and diagnose system problems.

Monitoring service

- Metric description

  OSS metric indicators are classified into groups such as basic service indicators, performance indicators, and metering indicators. For details, refer to *OSS metric indicator reference manual*.

  Note:

  To maintain consistency with the billing policies, the collection and presentation of metering indicators have the following special features:

  - Metering indicator data displays output per hour. This means that resource metering information for each hour is combined into a single value that represents the overall metering condition for that hour.
  - Metering indicator data has an output delay of nearly 30 minutes.
  - The data time of metering indicator data refers to the start time of the relevant statistical period.
  - The cutoff time of metering data acquisition is the end time of the last metering data statistical period of the current month. If no metering data is produced in the current month, the metering data acquisition cutoff is 00:00 on the first day of the current month.
  - A maximum amount of metering indicator data is pushed for presentation. For precise metering data, refer to *Consumption records*.

    For example, assume that you only use PutObject requests to upload data and perform this operation at an average of 10 times per minute. Then, in the hour between 2016-05-10 08:00:00 and 2016-05-10 09:00:00, the metering data value for your PUT requests will be 600 times (10*60 minutes), the data time will be 2016-05-10 08:00:00, this part of data will be output at around 2016-05-10 09:30:00. If this part of data is the last one since 2016-05-01 00:00:00, the metering data acquisition cutoff for the current month is 2016-05-10 09:00:00. If in May 2016, you have not produced any metering data, the metering data acquisition cutoff will be 2016-05-01 00:00:00.

Alarm service

> **Note:**
> OSS buckets must be globally unique. After deleting a bucket, if you create another bucket with the same name, the monitoring and alarm rules set for the deleted bucket will be applied to the new bucket with the same name.
>
> Besides metering indicators and statistical indicators, alarm rules can be configured for other metric indicators and be added to alarm monitoring. Moreover, multiple alarm rules may be configured for a single metric indicator.

User guide

- For information about the alarm rules service, see *Overview of alarm services*.
- For instructions on how to use the OSS alarm rules service, see *OSS Alarm rules service user guide*.

6.4 CDN monitoring

Cloud monitoring by monitoring CDN's QPS, BPS, byte hit ratio, and so on, helps users get domain name usage. After a user adds an accelerated domain name, cloud monitoring automatically begins to monitor it, you are logged in to CDN for cloud monitoring You can view monitoring details on the page. You can also set alarm rules on monitoring items so that you receive alarm information when the data is abnormal.

Monitoring Services

- Monitoring item description
-

Monitoring items	Meaning	Dimensions	Unit	Minimum monitor Granularity
Number of visits per second	Total number of visits/time granularity within the time grain	Domain Name	Times	1 minute
Network bandwidth BPS	Maximum network traffic per unit of time	Domain Name	BPS	1 minute
Hit rate	The probability of hit cache for the	Domain Name	Percentage	1 minute

Monitoring items	Meaning	Dimensions	Unit	Minimum monitor Granularity
	number of bytes requested in the time grain, note "bytes = number of requests x traffic ", the byte hit ratio more directly feedback back-to-back traffic			
Public network out of traffic	That is, CDN's public network downstream traffic.	Domain Name	Bytes	5 minutes
Return code 4xx	Percentage of HTTP return code 4xx as all return codes within the time grain	Domain Name	Percentage	1 minute
Return code 5xx share	Percentage of HTTP return code 5xx as all return codes within the time grain	Domain Name	Percentage	1 minute

- Viewing Monitoring Data

  1. Log on to the *CloudMonitor console*.
  2. Enter the list of CDN instances that the cloud service monitors.
  3. Click the Instance name or the monitor chart in the operation to go to the monitor details page.
  4. Click the size chart toggle button to toggle the larger image display (optional).

Alarm service

- Parameter descriptions

- Monitor: Monitoring metrics provided by CDN.
- Statistical Cycle: the alarm system checks if your monitoring data exceeds the alarm threshold for this cycle. For example, to set a memory usage alarm rule, the statistics cycle is 1 minute, an interval of 1 minute checks if memory usage exceeds the threshold.
- Statistical Methods: Statistical Methods refer to settings that exceed the threshold range. You can set the average, maximum, minimum, count, and value in a statistical method.
  - Average: the average of the monitored data during the statistical cycle. The statistic result is the average of all metric data collected within 15 minutes. An average value of over 80% is deemed to exceed the threshold.
  - Maximum: the maximum value of the monitor data during the statistics cycle. The maximum value of monitoring data collected during the statistical cycle exceeds the threshold of 80.
  - Minimum: the minimum value of the monitored data during the statistics cycle. The minimum value for monitoring data collected during the statistical cycle exceeds the threshold of 80.
  - Value: Sum of monitoring data during the statistics cycle. When the sum of the metric data collected within the period is over 80%, it exceeds the threshold. Such statistical methods are required for traffic-class metrics.
- Alarm after several consecutive exceeds threshold: refers to a number of consecutive statistical cycle monitoring items whose values continue to exceed the threshold to trigger an alarm.

  Example: Set CPU usage to exceed 80% Alarm, with a statistical cycle of 5 minutes, alarm three consecutive times after exceeding the threshold, when the first time the detection CPU usage exceeds 80%, no alarm notification is issued. Second Probe in 5 minutes CPU usage exceeds 80%, and no alarm will be issued. The third probe still exceeds 80% Alarm notification will be issued only when. That is, from the first time the actual data exceeds the threshold to the final alarm rule, the minimum time required is the statistical cycle (number of consecutive probes-1) = 5 (3-1) = 10 minutes.

- Set alarm rules
- **1.** Log in to the clLog on to the *CloudMonitor console*.oud monitoring console.
  2. Enter the list of CDN instances that the cloud service monitors.
  3. Click the alarm rule in the instance List action to enter the alert Rule Page for the instance.

4. Click new alarm rule in the upper-right corner of the alarm Rule Page to create an alarm rule based on the parameter.

6.5 Elastic IP monitoring

Cloud monitoring through monitoring the outgoing traffic, incoming traffic, the number of outgoing packets, incoming packets through the elastic public network IP four monitoring items, helps users monitor the running status of the service and enables users to set alarm rules on the monitoring items. User purchases elastic public network After the IP service, cloud monitoring automatically collects data for the above monitoring items.

Monitoring Services

- Monitoring item description

Monitoring items	Meaning	Dimensions	Unit	Minimum monitor Granularity
Network inflows bandwidth	Average flow to ECs via EIP per second	Instance	Bits/s	1 minute
Network outgoing bandwidth	The average flow of ECs out of EIP per second	Instance	Bits/s	1 minute
Number of incoming packets	The average number of packets that flow into ECs via EIP per second	Instance	Packages/s	1 minute
Number of outgoing packets	The average number of packets per second that ECs flows out through EIP	Instance	Packages/s	1 minute

- Viewing Monitoring Data

1. Log in to the cloud monitoring console.
2. Enter the list of elastic network IP instances monitored by the cloud service.

3. Click the Instance name or the monitor chart in the operation to go to the monitor details page.
4. Click the size chart toggle button to toggle the larger image display (optional).

Alarm service

- Parameter descriptions
  - Monitoring: Monitoring metrics provided by elastic IP.
  - Statistical Cycle: the alarm system checks if your monitoring data exceeds the alarm threshold for this cycle. For example, to set a memory usage alarm rule, the statistics cycle is 1 minute, an interval of 1 minute checks if memory usage exceeds the threshold.
  - Statistical Methods: Statistical Methods refer to settings that exceed the threshold range. You can set the average, maximum, minimum, count, and value in a statistical method.
    - Average: the average of the monitored data during the statistical cycle. The result is an average of all monitoring data collected within 15 minutes, when this average is greater than 80. Only when the threshold is exceeded.
    - Maximum: the maximum value of the monitor data during the statistics cycle. The maximum value of monitoring data collected during the statistical cycle exceeds the threshold of 80.
    - Minimum: the minimum value of the monitored data during the statistics cycle. The minimum value for monitoring data collected during the statistical cycle exceeds the threshold of 80.
    - Value: Sum of monitoring data during the statistics cycle. Sum up the monitoring data collected during the statistical period with more than 80% results after the sum That is, the threshold is exceeded. Such statistical methods are required for traffic-class metrics.
  - Alarm after several consecutive exceeds threshold: refers to a number of consecutive statistical cycle monitoring items whose values continue to exceed the threshold to trigger an alarm.

    Example: setting up the CPU The use rate is over 80% alarm, with a statistical cycle of 5 minutes and an alarm that exceeds the threshold three times in a row, the first time the CPU is detected When the usage rate exceeds 80%, no alarm notification is issued. If the CPU usage rate exceeds 80% again in the following 5-minute period, it still does not trigger an alert. An alert is reported only if the CPU usage rate exceeds 80% for a third time in the third period. That is, from the first time when the actual data exceeds the threshold to the time

when the alert policy is triggered, the minimum time consumed is: the period*(the quantity of consecutive detection times-1) = 5*(3-1) = 10 minutes.

- Set alarm rules

1. Log on to the *CloudMonitor console*.
2. Enter the list of elastic network IP instances monitored by the cloud service.
3. Click the alarm rule in the instance List action to enter the alert Rule Page for the instance.
4. Click new alarm rule in the upper-right corner of the alarm Rule Page to create an alarm rule based on the parameter.

6.6 ApsaraDB for Memcache

Cloud monitoring 7 monitors by monitoring the used cache, read hit ratio, and so on for cloud database memcache Edition Service instances item, helps the user monitor the running status of the instance and supports the user to set alarm rules on the monitoring item. User purchases After the memcache service, cloud monitoring automatically collects data for the above monitoring items.

Monitoring Services

- Monitoring item description

Monitoring items	Meaning	Dimensions	Unit	Minimum monitor Granularity
Cache used	The amount of cache that has been used	Instance	Bytes	1 minute
Read hit rate	Read down the probability of Kv success	Instance	Percentage	1 minute
QPS	Total number of read kV per second	Instance	Number	1 minute
Record count	The total number of current kV	Instance	Number	1 minute
Cache input bandwidth	Traffic generated by accessing the cache	Instance	BPS	1 minute

Monitoring items	Meaning	Dimensions	Unit	Minimum monitor Granularity
Cache output bandwidth	Traffic generated by reading the cache	Instance	BPS	1 minute
Eviction	The number of Kv evict per second	Instance	Number per second	1 minute

Note:

- Monitor Data is saved for up to 31 days.
- Users can view monitoring data for up to 14 days in a row.

- Viewing Monitoring Data

1. Log in to the cloud monitoring console.
2. Go to cloud database memcache monitored by cloud services Release List of monitoring instances.
3. Click the Instance name or the monitor chart in the operation to go To the instance monitoring details page to view the metrics.
4. Click the time range quick select button or the exact select function above the page.
5. Click the zoom in button in the upper-right corner of the monitor MAP to view the monitor larger image.

Alarm service

Cloud monitor for memcache The alarm service is provided by all monitoring items, after the user sets the alarm rules for the important monitoring items, you can receive alarm notifications in time after monitoring data exceeds the threshold, so you can process it quickly, reduce the possibility of failure.

- Parameter descriptions

— Monitoring items: Monitoring metrics provided by the redis edition of the cloud server.

— Statistical Cycle: the alarm system checks if your monitoring data exceeds the alarm threshold for this cycle. For example, to set a memory usage alarm rule, the statistics cycle is 1 minute, an interval of 1 minute checks if memory usage exceeds the threshold.

- Statistical Methods: Statistical Methods refer to settings that exceed the threshold range. You can set the average, maximum, minimum, count, and value in a statistical method.
  - Average: the average of the monitored data during the statistical cycle. The statistic result is the average of all metric data collected within 15 minutes. An average value of over 80% is deemed to exceed the threshold.
  - Maximum: the maximum value of the monitor data during the statistics cycle. The maximum value of monitoring data collected during the statistical cycle exceeds the threshold of 80.
  - Minimum: the minimum value of the monitored data during the statistics cycle. The minimum value for monitoring data collected during the statistical cycle exceeds the threshold of 80.
  - Value: Sum of monitoring data during the statistics cycle. When the sum of the metric data collected within the period is over 80%, it exceeds the threshold. Such statistical methods are required for traffic-class metrics.
- Continuous number of times: refers to the continuous number of statistical cycle monitoring items that continue to exceed the threshold value to trigger the alarm.

  Example: Set CPU usage to more than 80% alarm, statistical cycle to 5 minutes, 3 consecutive The alarm after the threshold is exceeded, the first time the detection CPU usage exceeds 80%, the alarm notification is not issued. The second time in 5 minutes to detect CPU usage exceeds 80% and no alarm will be issued. The third probe still exceeds 80% Alarm notification will be issued only when. That is, from the first time the actual data exceeds the threshold to the final alarm rule, the minimum time required is statistical cycle X (number of consecutive probes-1) = 5 x (3-1) = 10 minutes.

- Set single alarm rule

  1. Log on to the *CloudMonitor console*.
  2. Go to cloud database memcache monitored by cloud services Release List of monitoring instances.
  3. Click the Instance name or the monitor chart in the operation to enter the instance monitoring details page.
  4. Click the bell button in the upper-right corner of the monitor chart to set alarm rules for the monitoring items corresponding to the instance.

- Set up bulk alarm rules

1. Log on to the *CloudMonitor console*.
2. Go to cloud database memcache monitored by cloud services Release List of monitoring instances.
3. When the instance list page selects the desired instance, under the page, click set alarm rule, you can add alarm rules in bulk.

6.7 ApsaraDB for Redis monitoring

CloudMonitor displays the status and usage of ApsaraDB for Redis based on various metrics, including capacity usage and connection usage. Once you buy a Redis instance, CloudMonitor automatically starts monitoring the instance.

Once you buy a Redis instance, CloudMonitor automatically starts monitoring the instance. You can access the CloudMonitor **page** to view the metric data. You can configure alarm rules for metrics so that an alarm is generated when any data exception occurs.

Monitoring service

- Metrics

Metric	Definition	Dimension	Unit	Minimum monitor Granularity
Used capacity	Redis capacity is currently in use	Instance	Bytes	1 minute
Number of connections used	Current total number of client connections	Instance	Number	1 minute
Write speed	Current write network traffic per second	Instance	BPS	1 minute
Read Speed	Network Traffic is currently read per second	Instance	BPS	1 minute
Number of operation failures	Number of times the current operation kvstore failed	Instance	Number	1 minute

Metric	Definition	Dimension	Unit	Minimum monitor Granularity
Percentage used capacity	Proportion of current used capacity to total capacity	Instance	Percentage	1 minute
Connection percentage used	Current number of connections established as a percentage of total connections	Instance	Percentage	1 minute
Write bandwidth usage	Current write bandwidth as a percentage of total bandwidth	Instance	Percentage	1 minute
Read bandwidth usage	Current read bandwidth as a percentage of total bandwidth?	Instance	Percentage	1 minute
Instance failure	Event Type metrics, alarm rules can be set	-	-	-
Instance master standby switch	Event Type metrics, alarm rules can be set	-	-	-

- Viewing Monitoring Data

  1. Log on to the *CloudMonitor console*.
  2. Go to the **ApsaraDB for Redis** instance list under **Cloud Service Monitoring**.
  3. Click an instance name in the product instance list or click **Monitoring Charts** from the **Actions** column to access the instance monitoring details page.
  4. Click the Chart Size button to switch to large chart display (optional).

Alarm service

- Parameter description

  — Metrics: The monitoring indicators provided by ECS for Redis.

— Statistical cycle: The alarm rule system checks whether your monitoring data has exceeded the alarm rule threshold value based on the statistical cycle For example, if the statistical cycle of the alarm rule for memory usage is set to one minute, the system checks whether the memory usage has exceeded the threshold value every other minute.

— Statistics: This sets the method used to determine if the data exceeds the threshold. You can set Average, Maximum, Minimum, and Sum in Statistics.

- Average: The average value of metric data within a statistical cycle. The statistical result is the average of all metric data collected within 15 minutes. An average value of over 80 % is deemed to exceed the threshold.
- Maximum: The maximum value of metric data within a statistical cycle. When the maximum value of the metric data collected within the statistical cycle is over 80%, the value exceeds the threshold.
- Minimum: The minimum value of metric data within a statistical cycle. When the minimum value of the metric data collected within the statistical cycle is larger than 80%, the value exceeds the threshold.
- Sum: The sum of metric data within a statistical cycle. When the sum of the metric data collected within the statistical cycle is over 80%, it exceeds the threshold. The preceding statistical methods are required for traffic-based indicators.

— Trigger an alarm after the threshold value has exceeded several times: This refers to the alarm which is triggered when the value of the metric continuously exceeds the threshold value in several consecutive statistical cycles.

For example, you may set the alarm to go off when the CPU usage rate exceeds 80% within a 5-minute statistical cycle after the threshold value is exceeded for three times. If the CPU usage rate is found to exceed 80% for the first time, no warning notification is sent . The second time in 5 minutes to probe the CPU No alarm is reported if the CPU usage rate exceeds 80% only twice in a row. An alarm is reported only if the CPU usage rate exceeds 80% for the third time. That is, from the first time when the actual data exceeds the threshold to the time when the alarm rule is triggered, the minimum time consumed is the statistical cycle*(the quantity of consecutive detection times - 1) = 5*(3-1) = 10 minutes.

- Set alarm rules

1. Log on to the *CloudMonitor console*.
2. Go to the **ApsaraDB for Redis** instance list under **Cloud Service Monitoring**.
3. Click **Alarm Rules** in instance list **Actions** to access the instance's Alarm Rules page.

4. Enter all the relevant information in the required fields, and click **Confirm** to create a new alarm rule.

6.8 ApsaraDB for MongoDB

Cloud monitoring through monitoring multiple monitors such as CPU usage, memory usage, and so on for MongoDB service instances of cloud Database item, helps the user monitor the running status of the instance and supports the user to set alarm rules on the monitoring item. User purchases After the MongoDB service, cloud monitoring automatically collects data for the above monitoring items.

Monitoring Services

- Monitoring items

Monitoring items	Meaning	Dimensions	Unit	Minimum monitor Granularity
CPU utilization	CPU usage for instance	User dimension , instance dimension , Master dimension	Percentage	5 minutes
Memory usage	Memory usage for instance	User dimension , instance dimension , Master dimension	Percentage	5 minutes
Disk usage	Disk usage for an instance	User dimension , instance dimension , Master dimension	Percentage	5 minutes
IOPS usage	Iops usage for instances	User dimension , instance dimension , Master dimension	Percentage	5 minutes
Connections usage	The number of connections is the number of	User dimension , instance dimension	Percentage	5 minutes

Monitoring items	Meaning	Dimensions	Unit	Minimum monitor Granularity
	instances that an application can connect to a MongoDB . Number of connections usage is the percentage of the number of connections that have been used	, Master dimension		
Average number of SQL queries per second	Average number of SQL queries per second for MongoDB instances	User dimension , instance dimension , Master dimension	Number	5 minutes
Number of connections usage	The number of instances of MongoDB that the current application connects	User dimension , instance dimension , Master dimension	Number	5 minutes
The amount of disk space used by the instance	Total amount of disk space actually used by the instance	User dimension , instance dimension , Master dimension	Bytes	5 minutes
Amount of disk space occupied by data	The amount of disk space used by the data	User dimension , instance dimension , Master dimension	Bytes	5 minutes
Log usage of disk space	The amount of disk space occupied by the log	User dimension , instance dimension , Master dimension	Bytes	5 minutes

Monitoring items	Meaning	Dimensions	Unit	Minimum monitor Granularity
Inbound Intranet traffic	Network Flow Traffic for an instance	User dimension, instance dimension, Master dimension	Bytes	5 minutes
Outbound Intranet traffic	Network Flow Traffic for an instance	User dimension, instance dimension, Master dimension	Bytes	5 minutes
Request count	Total number of requests sent to the server	User dimension, instance dimension, Master dimension	Number	5 minutes
Number of insert operations	The number of times the INSERT command was last started from the MongoDB instance to the current cumulative receipt	User dimension, instance dimension, Master dimension	Number	5 minutes
Number of query operations	The number of times the query command was recently started from the MongoDB instance to the query command that is now cumulative	User dimension, instance dimension, Master dimension	Bytes	5 minutes

Monitoring items	Meaning	Dimensions	Unit	Minimum monitor Granularity
Number of update operations	The number of times the update command was recently started from the MongoDB instance to the update command that is now cumulative	User dimension, instance dimension, Master dimension	Number	5 minutes
Number of delete operations	The number of operations from the last time the MongoDB instance was started to now cumulative execution of Delete	User dimension, instance dimension, Master dimension	Number	5 minutes
Number of operations from getmore	The number of operations from the last time the MongoDB instance was started to the present cumulative execution of getmore	User dimension, instance dimension, Master dimension	Number	5 minutes
Command operation count	The total number of commands sent to the database since the last time MongoDB was started.	User, instance, and master/ backup	Number	5 minutes
Instance failure	Event-type metric, for which	-	-	-

Monitoring items	Meaning	Dimensions	Unit	Minimum monitor Granularity
	alarm rules can be set			

Note:

- Metric data can be saved for up to 31 days.
- You can view metric data for up to 14 consecutive days.

- View metric data

1. Log on to *CloudMonitor console*.
2. Go to the **ApsaraDB for MongoDB** instance list under **Cloud Service Monitoring**.
3. Click an instance name in the product instance list or click **Metric Chart** from the **Actions** column to view metrics on the Instance monitoring details page.
4. Click the **Time Range** shortcut at the top of the page or use the specific selection function. Data for up to 14 consecutive days can be viewed.
5. Click the Zoom In button in the upper-right corner of the metric chart to enlarge the graph.

Alarm service

- Parameter descriptions

— Metric items: The monitoring indicators provided by ApsaraDB for MongoDB.

— Statistical cycle: The alarm system checks whether your monitoring data has exceeded the alarm threshold value based on the statistical cycle. For example, if the statistical cycle of the alarm rule for memory usage is set to one minute, the system checks whether the memory usage has exceeded the threshold value every other minute.

— Statistical method: This sets the method used to determine if the data exceeds the threshold. You can set Average, Maximum, Minimum, and Sum in Statistical method.

■ Average: The average value of metric data within a statistical cycle. The statistical result is the average of all metric data collected within 15 minutes. An average value of over 80 % is deemed to exceed the threshold.

- Maximum: The maximum value of metric data within a statistical cycle. When the maximum value of the metric data collected within the statistical cycle is over 80%, the value exceeds the threshold.
- Minimum: The minimum value of metric data within a statistical cycle. When the minimum value of the metric data collected within the statistical cycle is larger than 80%, the value exceeds the threshold.
- Sum: The sum of metric data within a statistical cycle. When the sum of the metric data collected within the statistical cycle is over 80%, it exceeds the threshold. The preceding statistical methods are required for traffic-based indicators.

— Consecutive times: Refers to an alarm which is triggered when the value of the metric item continuously exceeds the threshold value in several consecutive statistical cycles.

For example, you may set the alarm to go off when the CPU usage rate exceeds 80% within a 5-minute statistical cycle after the threshold value is exceeded for three times. If the CPU usage rate is found to exceed 80% for the first time, no warning notification is sent. No alarm is reported if the CPU usage rate exceeds 80% only twice in a row. An alarm is reported only if the CPU usage rate exceeds 80% for the third time. That is, from the first time when the actual data exceeds the threshold to the time when the alarm rule is triggered , the minimum time consumed is the statistical cycle*(the quantity of consecutive detection times-1) = 5*(3-1) = 10 minutes.

- Set a single alarm rule

  1. Log on to *CloudMonitor console*.
  2. Choose **Cloud Service Monitoring** > **ApsaraDB for MongoDB** .
  3. Click the Instance name or the monitor chart in the operation to enter the monitoring details page for the instance.
  4. Click the bell button in the upper-right corner of the monitor chart to set alarm rules for the monitoring items corresponding to the instance.

- Set up bulk alarm rules

  1. Log in to the cloud monitoring console.
  2. Go to MongoDB, a cloud Database monitored by cloud services List of version instances.
  3. When the instance list page selects the desired instance, click set alarm rule below the page , you can add alarm rules in bulk.

6.9 Message Service monitoring

Cloud monitoring through the monitoring of Message Service delay messages, invalid messages, active messages, three monitoring items, help Users get message service Queue usage.

When users create message queues for message service, cloud monitoring automatically begins to monitor them, you are logged in to the cloud monitoring Message Service You can view monitoring details on the page. You can also set alarm rules on monitoring items so that you receive alarm information when the data is abnormal.

Monitoring Services

- Monitoring item description

Monitoring items	Meaning	Dimensions	Unit	Minimum monitor Granularity
Activemessages	The total number of messages that are active in this queue	Userid, region, bid, queue	Number	5 minutes
Inactiveme ssages	The total number of messages that are inactive in this queue	Userid, region, bid, queue	Number	5 minutes
Delaymessage	The total number of messages in the delayed state in this queue	Userid, region, bid, queue	Number	5 minutes
Sendmessag eecount	Send message requests	Userid, region, queue	Items	3600
Batchsendm essagecount	Number of bulk send message requests	Userid, region, queue	Items	3600
Receivemes sagecount	Number of receive message requests	Userid, region, queue	Items	3600
Batchrecei vemessagecount	Number of bulk receive message requests	Userid, region, queue	Items	3600

Monitoring items	Meaning	Dimensions	Unit	Minimum monitor Granularity
Batchdelet emessagecount	Bulk Delete message request quantity	Userid, region, queue	Items	3600
Changemess agevisibilitycount	Change message visibility count	Userid, region, queue	Items	3600

- Viewing Monitoring Data

  1. Log in to the cloud monitoring console.
  2. Enter the list of message service instances that the cloud service monitors.
  3. Click the Instance name or the monitor chart in the operation to go to the monitor details page.
  4. Click the size chart toggle button to toggle the larger image display (optional).

Alarm service

- Parameter descriptions

  — Monitor: the monitoring metrics provided by the message service.

  — Statistical Cycle: the alarm system checks if your monitoring data exceeds the alarm threshold for this cycle. For example, to set a memory usage alarm rule, the statistics cycle is 1 minute, an interval of 1 minute checks if memory usage exceeds the threshold.

  — Statistical Methods: Statistical Methods refer to settings that exceed the threshold range. You can set the average, maximum, minimum, count, and value in a statistical method.

    ■ Average: the average of the monitored data during the statistical cycle. The result is an average of all monitoring data collected within 15 minutes, when this average is greater than 80. Only when the threshold is exceeded.

    ■ Maximum: the maximum value of the monitor data during the statistics cycle. The maximum value of monitoring data collected during the statistical cycle exceeds the threshold of 80.

    ■ Minimum: the minimum value of the monitored data during the statistics cycle. The minimum value for monitoring data collected during the statistical cycle exceeds the threshold of 80.

- Value: Sum of monitoring data during the statistics cycle. Sum up the monitoring data collected during the statistical period with more than 80% results after the sum That is, the threshold is exceeded. Such statistical methods are required for traffic-class metrics.

— Alarm after several consecutive exceeds threshold: refers to a number of consecutive statistical cycle monitoring items whose values continue to exceed the threshold to trigger an alarm.

Example: Set CPU usage to more than 80% alarm with a statistical cycle of 5 In minutes, alarm after 3 consecutive times exceeds the threshold, when the first time the CPU usage is detected exceeds 80, no alarm notification will be issued. The second time in 5 minutes to probe the CPU Usage is more than 80%, and no alarm will be issued. The third time the probe is still over 80%, alarm notification will be issued. That is, from the first time the actual data exceeds the threshold to the final alarm rule, the minimum time required is the statistical cycle (number of consecutive probes-1) = 5 (3-1) = 10 minutes.

- Set alarm rules

1. Log in to the cloud monitoring console.
2. Enter the list of message service instances that the cloud service monitors.
3. Click the alarm rule in the instance List action to enter the alert Rule Page for the instance.
4. Click new alarm rule in the upper-right corner of the alarm Rule Page to create an alarm rule based on the parameter.

6.10 AnalyticDB monitoring

Cloud monitoring through the provision of analytic dB disk rated capacity, disk used capacity, disk usage 3 messages, help Users get analytic DB Service usage.

When users start using analytic dB services, cloud monitoring automatically begins to monitor them, analytic dB for cloud monitoring You can view monitoring details on the page. You can also set alarm rules on monitoring items so that you receive alarm information when the data is abnormal.

Monitoring Services

- Monitoring item description

Monitoring items	Meaning	Dimensions	Unit	Minimum monitor Granularity
Disksize	Disk rated capacity	Instanceid, tableschema, workerid	MB	1 minute
DiskUsed	Disk used capacity	Instanceid, tableschema, workerid	MB	1 minute
Diskusedpercent	Disk usage	Instanceid, tableschema, workerid	Percentage	1 minute

- Viewing Monitoring Data

  1. Log in to the cloud monitoring console.
  2. Enter the list of analytical database instances that the cloud service monitors.
  3. Click the Instance name or the monitor chart in the operation to go to the monitor details page.
  4. Click the size chart toggle button to toggle the larger image display (optional).

Alarm service

- Parameter descriptions

  — Monitoring: Monitoring metrics provided by the analytical database.

  — Statistical Cycle: the alarm system checks if your monitoring data exceeds the alarm threshold for this cycle. For example, to set a memory usage alarm rule, the statistics cycle is 1 minute, an interval of 1 minute checks if memory usage exceeds the threshold.

  — Statistical Methods: Statistical Methods refer to settings that exceed the threshold range. You can set the average, maximum, minimum, count, and value in a statistical method.

    ■ Average: the average of the monitored data during the statistical cycle. The result is an average of all monitoring data collected in 15 minutes, when this average is greater than 80%, the threshold is exceeded.

    ■ Maximum: the maximum value of the monitor data during the statistics cycle. The maximum value of monitoring data collected during the statistical cycle exceeds the threshold of 80.

- Minimum: the minimum value of the monitored data during the statistics cycle. The minimum value for monitoring data collected during the statistical cycle exceeds the threshold of 80.
- Value: Sum of monitoring data during the statistics cycle. To sum up the monitoring data collected during the statistical period, after sum, more than 80% of results exceed the threshold. Such statistical methods are required for traffic-class metrics.

— Alarm after several consecutive exceeds threshold: refers to a number of consecutive statistical cycle monitoring items whose values continue to exceed the threshold to trigger an alarm.

Example: Set CPU usage to more than 80% alarm with a statistical cycle of 5 In minutes, alarm after 3 consecutive times exceeds the threshold, when the first time the CPU usage is detected exceeds 80, no alarm notification will be issued. The second time in 5 minutes to detect CPU usage exceeds 80% and no alarm will be issued. The third probe still exceeds 80% Alarm notification will be issued only when. That is, from the first time the actual data exceeds the threshold to the final alarm rule, the minimum time required is statistical cycle X (number of consecutive probes-1) = 5 x (3-1) = 10 minutes.

- Set alarm rules

1. Log in to the cloud monitoring console.
2. Enter the list of analytical database instances that the cloud service monitors.
3. Click the alarm rule in the instance List action to enter the alert Rule Page for the instance.
4. Click new alarm rule in the upper-right corner of the alarm Rule Page to create an alarm rule based on the parameter.

6.11 Log service monitoring

CloudMonitor displays the usage of the Log Service based on 11 metrics, including outbound traffic, inbound traffic, overall QPS, and log statistic method. Once you create a Log Service instance, CloudMonitor automatically starts monitoring the service. You can access CloudMonitor Log Service page to view the metric data. You can configure alarm rules for metrics so that an alarm is triggered when any data exception occurs.

Monitoring Services

- Metrics

Metric	Definition	Dimension	Unit	Minimum monitor Granularity
Inflow	Logstore incoming and outgoing flows per minute	userId、Project、Logstore	Bytes	1 minute
Outflow	Logstore flow per minute	userId、Project、Logstore	Bytes	1 minute
SumQPS	Total number of writes per minute in the logstore	userId、Project、Logstore	Count	1 minute
LogMethodQPS	Total number of writes per minute to the logstore.	userId、Project、Logstore、Method	Count	1 minute
LogCodeQPS	Number of writes per minute mapped to a specific status code in the logstore.	userId、Project、Logstore、Status	Count	1 minute
SuccessdByte	Number of successfully resolved bytes in the logstore.	userId、Project、Logstore	Bytes	10 minutes.
SuccessdLines	Number of lines in resolved logs in the logstore.	userId、Project、Logstore	Count	10 minutes
Failedlines	Number of lines in logs failed to be resolved in the logstore.	userId、Project、Logstore	Count	10 minutes
AlarmPV	Total number of ECS configuration errors in the logStore	userId、Project、Logstore	Count	5 minutes
AlarmUv	Total number of ECS instances	userId、Project、Logstore	Count	5 minutes

Metric	Definition	Dimension	Unit	Minimum monitor Granularity
	with incorrect configurations in the logstore.			
AlarmIPCount	Number of errors incurred by a specific IP address in the logstore.	userId、Project 、Logstore、 alarm_type、 source_ip	Count	5 minutes

- View metric data

  1. Log on to the *CloudMonitor console*.
  2. Go to the **Log Service** instance list under **Cloud Service Monitoring**.
  3. Click an instance name from the product instance list or click **Monitoring Charts** from the **Actions** column to access the instance monitoring details page.
  4. Click the Chart Size button to switch to large chart display(optional).

Alarm service

- Parameter descriptions

  — Metrics: The monitoring indicators provided by the Log Service.

  — Statistical cycle: The alarm system checks whether your monitoring data has exceeded the alarm threshold value based on the statistical cycle. For example, if the statistical cycle of the alarm rule for memory usage is set to one minute, the system checks whether the memory usage has exceeded the threshold value every other minute.

  — Statistical method: This method is used to determine if the data exceeds the threshold. You can set Average, Maximum, Minimum, and Sum in the statistical method.

    ■ Average: The average value of the metric data within a statistical cycle. The statistical result is the average of the metric data collected within 15 minutes. An average value of over 80% is deemed to exceed the threshold.

    ■ Maximum: The maximum value of metric data within a statistical cycle. When the maximum value of the metric data collected within the statistical cycle is over 80%, the value exceeds the threshold.

- Minimum: The minimum value of metric data within a statistical cycle. When the minimum value of the metric data collected within the statistical cycle is larger than 80%, the value exceeds the threshold.
- Sum: The sum of metric data within a statistical cycle. When the sum of the metric data collected within the statistical cycle is over 80%, it exceeds the threshold. The preceding statistical methods are needed for traffic-based indicators.

— Trigger an alarm after the threshold value has exceeded several times: This refers to an alarm which is triggered when the value of the metric item continuously exceeds the threshold value in several consecutive statistical cycles.

For example, you may set the alarm to go off when the CPU usage rate exceeds 80% within a 5-minute statistical cycle after the threshold value is exceeded three times. If the CPU usage rate is found to exceed 80% for the first time, no warning notification is sent. No alarm is reported if the CPU usage rate exceeds 80% only twice in a row. An alarm is reported only if the CPU usage rate exceeds 80% for the third time. That is, from the first time when the actual data exceeds the threshold to the time when the alarm rule is triggered, the minimum time consumed is the statistical cycle*(the quantity of consecutive detection times - 1) = 5*(3-1) = 10 minutes.

Note:

- When you configure alarm rules, you can select a log method and a status code for QPS. If you do not select one, QPS collects statistical data for all log methods and status codes.
- The method fields include PostLogStoreLogs, GetLogtailConfig, PutData, GetCursorOrData、 GetData 、GetLogStoreHistogram 、GetLogStoreLogs、 ListLogStores、ListLogStoreTopics。
- The status fields include 200, 400, 401, 403, 405, 500, and 502.

- Set an alarm rule

1. Log on to the *CloudMonitor console*.
2. Go to the **Log Service** instance list under **Cloud Service Monitoring**.
3. Click **Alarm Rules** from the **Actions** column to access the instance's Alarm Rules page.
4. Enter all the relevant information in the required fields, and click **Confirm** to create a new alarm rule.

6.12 Container service monitoring

Cloud monitoring through monitoring CPU usage, memory usage, and so on for container services 7 Monitoring items to help users get use of Container Services. After the user creates the container service, cloud monitoring automatically begins to monitor the container service, you can log in to the Container Services page for cloud monitoring to view monitoring details. You can also set alarm rules on the monitor so that you receive an alarm notification when the data is abnormal .

Monitoring Services

- Monitoring item description

Monitoring items	Meaning	Dimensions	Unit	Minimum monitor Granularity
containerCpuUtilization	Container CPU usage	User dimension, container dimension	Percentage	30 seconds
Containermemoryutilization	Container memory usage	User dimension, container dimension	Percentage	30 seconds
Containermemoryamount	Container memory usage	User dimension, container dimension	Bytes	30 seconds
Containerinternetin	Container traffic into the network	User dimension, container dimension	Bytes	30 seconds
containerInternetOut	Container traffic out of the Network	User dimension, container dimension	Bytes	30 seconds
containerIORead	Container Io read	User dimension, container dimension	Bytes	30 seconds
containerIOWrite	Containe rIO write	User dimension, container dimension	Bytes	30 seconds

Note:

- Monitor Data is saved for up to 31 days.
- Users can view monitoring data for up to 14 days in a row.

- Viewing Monitoring Data

1. Log in to the cloud monitoring console.
2. Enter the list of Container service instances that the cloud service monitors.
3. Click the Instance name or the monitor chart in the operation to go To the instance monitoring details page to view the metrics.
4. Click the time range quick select button or the exact select function at the top of the page, maximum monitoring data support view continuous 14 Monitoring data for days.
5. Click the zoom in button in the upper-right corner of the monitor MAP to view the monitor larger image.

Alarm service

- Set single alarm rule: Click the bell button in the upper right corner of the monitor chart, alarm rules can be set for monitoring items corresponding to this instance.
- Sets the bulk alarm rule: the list of instances page selects the desired instance, you can add alarm rules in bulk by clicking set alarm rules below the page.

6.13 Shared Bandwidth

CloudMonitor monitors network access, bandwidth, and so on by monitoring shared bandwidth, helps users monitor network usage of shared bandwidth and enables users to set alarm rules on monitoring items. After you buy the auto scaling service, CloudMonitor will automatically collect data on the metrics listed above.

Monitoring Services

- Monitoring items

Monitoring items	Dimensions	Unit	Minimum monitor Granularity
Bandwidth packet network inflows bandwidth	User dimension, instance dimension	Bits/s	1 minute

Monitoring items	Dimensions	Unit	Minimum monitor Granularity
Bandwidth packet network outgoing bandwidth	User dimension, instance dimension	Bits/s	1 minute
Bandwidth packets network inflows packets	User dimension, instance dimension	packages/s	1 minute
Bandwidth packet network flow Packet	User dimension, instance dimension	packages/s	1 minute
Bandwidth packet network outgoing bandwidth usage	User dimension, instance dimension	%	1 minute

Note:

- Monitor Data is saved for up to 31 days.
- Users can view monitoring data for up to 7 days in a row.

- Viewing Monitoring Data

1. Log on to the *CloudMonitor console*.
2. Enter the list of instances of shared bandwidth that the cloud service monitors.
3. Click the Instance name or the monitor chart in the operation to go To the instance monitoring details page to view the metrics.
4. Click the time range on the top of the page to quickly select a button or select an exact function, monitoring data supports viewing monitoring data for seven consecutive days.
5. Click the zoom button in the upper-right corner of the monitor MAP to view the monitor larger image.

Alarm service

- Parameter descriptions

— Monitor: that is, the monitoring metrics provided by services that share bandwidth.

— Statistical Cycle: the alarm system checks if your monitoring data exceeds the alarm threshold for this cycle. For example, to set a memory usage alarm rule, the statistics cycle is 1 minute, an interval of 1 minute checks if memory usage exceeds the threshold.

— Continuous number of times: refers to the continuous number of statistical cycle monitoring items that continue to exceed the threshold value to trigger the alarm.

- Set single alarm rule

  1. Log on to the *CloudMonitor console*.
  2. Enter the list of instances of shared bandwidth that the cloud service monitors.
  3. Click the Instance name or the monitor chart in the operation to go To the instance monitoring details page.
  4. Click the bell button in the upper right corner of the monitor chart or the new alarm rule in the upper right corner of the page, alarm rules can be set for monitoring items correspond ing to this instance.

- Set up bulk alarm rules

  1. Log on to the *CloudMonitor console*.
  2. Enter the list of shared bandwidth instances that the cloud service monitors.
  3. When the instance list page selects the desired instance, click set alarm rule below the page , you can add alarm rules in bulk.

6.14 Global acceleration monitoring

CloudMonitor monitors multiple monitoring metrics, such as inbound and outbound network bandwidth of Global Acceleration. It helps you monitor the network usage of Global Accelerati on and allows you to set alarm rules for the monitoring metrics. After you purchase the Global Acceleration service, CloudMonitor automatically collects data on the preceding monitoring metrics.

Monitoring service

- Metrics

metric	Dimension	Unit	Minimum monitor Granularity
Inbound bandwidth	User and instance	Bits/s	1 minute
outbound bandwidth	User and instance	Bits/s	1 minute
Inbound package	User and instance	pps	1 minute
outbound package	User and instance	pps	1 minute

Note:

- Monitoring data is saved for up to 31 days.
- You can view the monitoring data for up to 7 consecutive days.

- View monitoring data

  1. Log on to the *CloudMonitor console*.
  2. Go to the **Global Acceleration** instance list under **Cloud Service Monitoring** .
  3. Click an instance name or click **Monitoring Chart** in the **Actions** column to access the instance monitoring details page and view various metrics.
  4. Click the **Time Range** quick selection button from the upper menu of the page or use the specific selection function. You can view the monitoring data for up to 7 consecutive days.
  5. Click Zoom In in the upper-right corner of the monitoring chart to enlarge the chart.

Alarm service

- Parameter descriptions

  — Monitoring metrics: The monitoring metrics provided by Global Acceleration service.

  — Statistical cycle: The alarm system checks whether your monitoring data has exceeded the alarm threshold based on the cycle. For example, if the statistical cycle of the alarm rule for memory usage is set to one minute, the system checks whether the memory usage has exceeded the threshold value every other minute.

  — Consecutive times: An alarm is triggered when the value of the monitoring metrics continuously exceeds the threshold value for the set consecutive cycles.

- Set an alarm rule

  1. Log on to the *CloudMonitor console*.
  2. Go to the **Global Acceleration** instance list under **Cloud Service Monitoring** .
  3. Click an instance name or click **Monitoring Chart** in the **Actions** column to access the instance monitoring details page.
  4. Click bell icon in the upper-right corner of the monitoring chart or **New Alarm Rule** in the upper-right corner of the page to set an alarm rule for corresponding monitoring metrics of this instance.

- Set multiple alarm rules

  1. Log on to the *CloudMonitor console*.

2. Go to the **Global Acceleration** instance list under **Cloud Service Monitoring** .
3. Select the appropriate instances on the instance list page. Click **Set Alarm Rules** to add multiple alarm rules.

6.15 High performance time series database hitsdb

CloudMonitor monitors multiple monitoring metrics, such as HiTSDB disk usage, the number of timelines, and the number of time points. It helps you monitor the network use of NAT Gateway and allows you to set alarm rules for the monitoring metrics. When you purchase hitsdb, cloud monitoring automatically collects data for the hitsdb monitor.

Monitoring service

- Monitoring items

Monitoring items	Dimensions	Unit	Minimum monitor Granularity
Disk usage	User and instance	%	20 seconds
Timeline quantity	User and instance	Count	20 seconds
Point in time the growth rate	User and instance	Count/Second	20 seconds

Note:

- Monitoring data is saved for up to 31 days.
- You can view the monitoring data for up to 14 consecutive days.

- View metric data

1. Log on to the *CloudMonitor console*.
2. 2. Go to the HiTSDB instance list under Cloud Service Monitoring.
3. 3. Click an instance name or click Monitoring Chart in the Action column to access the instance monitoring details page and view various metrics.
4. Click a "Time Range" shortcut on the top of the page or use the specific selection function. Up to 14 consecutive days of metric data can be viewed.
5. Click the zoom button in the upper-right corner of the monitor MAP to view the monitor larger image.

Alarm service

- Description
  - Monitor: the monitoring indicator provided by hitsdb's service.
  - Statistical Cycle: the alarm system checks if your monitoring data exceeds the alarm threshold for this cycle. For example, if the statistical cycle of the alarm rule for memory usage is set to one minute, the system checks whether the memory usage has exceeded the threshold value every other minute.
  - Consecutive times: an alarm is triggered when the value of the monitoring metrics continuously exceeds the threshold value for the set consecutive cycles.
- Set an alarm rule
  1. Log on to the *CloudMonitor console*.
  2. Go to the HiTSDB instance list under Cloud Service Monitoring.
  3. Click the Instance name or the monitor chart in the operation to go To the instance monitoring details page.
  4. Click the Bell button in the upper-right corner of the monitoring chart or New Alarm Rule in the upper-right corner of the page to set an alarm rule for corresponding monitoring metrics of this instance.
- Set batch alarm rules
  1. Log on to the *CloudMonitor console*.
  2. Go to the HiTSDB instance list under Cloud Service Monitoring.
  3. When the instance list page selects the desired instance, click set alarm rule below the page , you can add alarm rules in bulk.

6.16 VPN gateway

CloudMonitor monitors multiple monitoring metrics, such as inbound and outbound network bandwidth of VPN gateway. It helps you monitor the network usage of VPN gateway and allows you to set alarm rules for the monitoring metrics. After you purchase the VPN gateway service, CloudMonitor automatically collects data on the preceding monitoring metrics.

Monitoring service

- Monitoring metrics

  CloudMonitor provides the following monitoring metrics:

Monitoring metrics	Dimensions	Unit	Minimum monitoring granularity
Inbound network bandwidth of a bandwidth package	User and instance	Bit/s	1 minute
Outbound network bandwidth of a bandwidth package	User and instance	Bit/s	1 minute
Incoming packet of a bandwidth package	User and instance	PPS	1 minute
Outgoing packet of a bandwidth package	User and instance	PPS	1 minute

Note:

- Monitoring data is saved for up to 31 days.
- You can view the monitoring data for up to 7 consecutive days.

- View monitoring data

1. Log on to the *CloudMonitor console*.
2. Go to the **VPN Gateway** instance list under **Cloud Service Monitoring**.
3. Click an instance name or click **Monitoring Chart** in the **Actions** column to access the instance monitoring details page and view various metrics.
4. Click the **Time Range** quick selection button at the top of the page or use the specific selection function. You can view the monitoring data for up to 7 consecutive days.
5. Click the **Zoom In** button in the upper-right corner of the monitoring chart to enlarge the chart.

Alarm service

- Parameter description

— Monitoring metrics: the monitoring metrics provided by the VPN gateway service.

— Statistical cycle: the alarm system checks whether your monitoring data has exceeded the alarm threshold based on the cycle. For example, if the statistical cycle of the alarm rule

for memory usage is set to one minute, the system checks whether the memory usage has exceeded the threshold value every other minute.

- Consecutive times: an alarm is triggered when the value of the monitoring metrics continuously exceeds the threshold value for the set consecutive cycles.

- Set an alarm rule

  1. Log on to the *CloudMonitor console*.
  2. Go to the **VPN Gateway** instance list under **Cloud Service Monitoring**.
  3. Click an instance name or click **Monitoring Chart** in the **Actions**column to access the instance monitoring details page.
  4. Click the bell icon in the upper-right corner of the monitoring chart or **New Alarm Rule** in the upper-right corner of the page to set an alarm rule for corresponding monitoring metrics of this instance.

- Set alarm rules in batches

  1. Log on to the *CloudMonitor console*.
  2. Go to the **VPN Gateway** instance list under **Cloud Service Monitoring**.
  3. Select the appropriate instance on the instance list page. Click **Set Alarm Rules** at the bottom of the page to add alarm rules in batches.

6.17 API Gateway

CloudMonitor provides inbound traffic, outbound traffic, response time, and other metric data at the API Gateway, and helps you obtain the API Gateway service's use information. After you activate your API Gateway instance, CloudMonitor automatically starts monitoring the instance. After you activate your API Gateway instance, CloudMonitor automatically starts monitoring the instance. You can access the CloudMonitor API Gateway page to view the metric data. You can configure alert policies for metrics so that an alert is reported when a data exception occurs.

Monitoring Services

- Metrics

Metric	Definition	Dimension	Unit	Minimum monitor Granularity
Error Distribution	Number of times of 2XX, 4XX,	User and API	Count	1 minute

Metric	Definition	Dimension	Unit	Minimum monitor Granularity
	and 5XX status codes returned for an API in one monitoring period .			
Inbound traffic	The sum of traffic of requests from an API in one monitoring period	User and API	Bytes	1 minute
Outbound traffic	The sum of traffic of requests from an API in one monitoring period .	User and API	Bytes	1 minute
Response time	The difference between the time when the gateway calls a backend service through an API and the time when the backend service receives the return result in one monitoring period.	User and API	Second	1 minute
The sum of requests	received by an API in one monitoring period .	User and API	per time	1 minute

- View metric data

  1. Log on to the *CloudMonitor console*.
  2. Go to the **API Gateway** instance list under **Cloud Service Monitoring**.

3. Click an instance name in the product instance list or click **Metric Chart** in the **Actions** column to access the instance monitoring details page.
4. Click the Chart Size button to switch to large chart display (optional).

Alarm service

- Parameter descriptions
  - Metrics: The monitoring indicators provided by the API Gateway.
  - Period: The alert system checks whether your monitoring data has exceeded the alert threshold value based on the period. For example, if the period of the alert policy for memory usage is set to one minute, the system checks whether the memory usage has exceeded the threshold value every other minute.
  - Statistic: This sets the method used to determine if the data exceed the threshold. Average, maximum, minimum, and sum can be set in the statistic.
    - Average: The average value of metric data within a statistical period. The statistic result is the average of all metric data collected within 15 minutes. An average value of over 80 % is deemed to exceed the threshold.
    - Maximum: The maximum value of metric data within a statistical period. When the maximum value of the metric data collected within the period is over 80%, the value exceeds the threshold.
    - Minimum: The minimum value of metric data within a statistical period. When the minimum value of the metric data collected within the period is larger than 80%, the value exceeds the threshold.
    - Sum: The sum of metric data within a statistical period. When the sum of the metric data collected within the period is over 80%, it exceeds the threshold. The above statistics are needed for traffic-based indicators.
  - Trigger Alert After Threshold Value Is Exceeded Several Times: This refers to an alert which is triggered when the value of the metric continuously exceeds the threshold value in several consecutive periods.

    For example, you may set the alert to go off when the CPU usage rate exceeds 80% within a 5-minute period after the threshold value is exceeded for three times. If the CPU usage rate is found to exceed 80% for the first time, no alert is triggered. If the CPU usage rate exceeds 80% again in the following 5-minute period, it still does not trigger an alert. n alert is reported only if the CPU usage rate exceeds 80% for a third time in the third period.

That is, from the first time when the actual data exceeds the threshold to the time when the alert policy is triggered, the minimum time consumed is: the period*(the quantity of consecutive detection times-1) = 5*(3-1) = 10 minutes.

- Set an alarm rule

1. Log on to the *CloudMonitor console*.
2. Go to the **API Gateway** instance list under **Cloud Service Monitoring**.
3. Click an instance name in the product instance list or click **Alarm Rules** in the **Actions** column to access the instance monitoring details page.
4. Click **Create Alarm Rules** at the upper right of the alert policies page to create an alert policy based on the entered parameters.

6.18 DDoS high security IP

Cloud monitoring by providing DDoS high anti-IP outgoing bandwidth monitor, helps users monitor DDoS high-security IP usage, it also allows users to set alarm rules on monitoring items. After a user buys a DDoS high-security IP, cloud monitoring automatically collects data for the above monitoring items.

Monitoring Services

- Monitoring items

Monitoring items	Dimensions	Unit	Minimum monitor Granularity
Network bandwidth	Instance dimension, IP dimension	Bits/s	30 s

Note:

- Monitor Data is saved for up to 31 days.
- Users can view monitoring data for up to 14 days in a row.

- Viewing Monitoring Data

1. Log in to the cloud monitoring console.
2. Enter the list of instances of DDoS high-security IP that the cloud service monitors.
3. Click the Instance name or the monitor chart in the operation to go To the instance monitoring details page to view the metrics.

4. Click the time range on the top of the page to quickly select a button or select an exact function, the maximum monitoring data allows you to view the monitored data for 14 consecutive days.
5. Click the zoom button in the upper-right corner of the monitor MAP to view the monitor larger image.

Alarm service

- Parameter descriptions
  - Monitoring: that is, the monitoring metrics provided by the DDoS high-security IP service.
  - Statistical Cycle: the alarm system checks if your monitoring data exceeds the alarm threshold for this cycle. For example, to set a memory usage alarm rule, the statistics cycle is 1 minute, an interval of 1 minute checks if memory usage exceeds the threshold.
  - Continuous number of times: refers to the continuous number of statistical cycle monitoring items that continue to exceed the threshold value to trigger the alarm.
- Set single alarm rule
  1. Log in to the cloud monitoring console.
  2. Enter the list of instances of DDoS high-security IP that the cloud service monitors.
  3. Click the Instance name or the monitor chart in the operation to go To the instance monitoring details page. Click the bell button in the upper right corner of the monitor chart or the new alarm rule in the upper right corner of the page, alarm rules can be set for monitoring items corresponding to this instance.

6.19 Direct Mail monitoring

CloudMonitor provides monitoring metrics for Direct Mail, including WEB/API messaging, SMTP messaging, and account exceptions, to help you monitor the service status of Direct Mail in real time and set alarm rules for the monitoring metrics. After you purchase and use the Direct Mail service, CloudMonitor automatically collects data on the preceding monitoring metrics.

Monitoring service

- Metrics

Metric	Unit	Minimum monitor Granularity
Web/API error-QPS delayed	Count/Min	1 minute

Metric	Unit	Minimum monitor Granularity
Web/API error-over-quota QPS	Count/Min	1 minute
Web/API error-spam QPS	Count/Min	1 minute
Web/API message success QPS	Count/Min	1 minute
SMTP authentication failed QPS	Count/Min	1 minute
SMTP authentication is successful QPS	Count/Min	1 minute
SMTP error-length exceeded QPS	Count/Min	1 minute
SMTP error-over-quota QPS	Count/Min	1 minute
SMTP error-spam QPS	Count/Min	1 minute

Note:

- Monitor Data is saved for up to 31 days.
- Users can view monitoring data for up to 14 days in a row.

- Viewing Monitoring Data

  1. Log on to the *CloudMonitor console*.
  2. Go to the**Direct Mail monitoring** page under **Cloud Service Monitoring**, and view the monitoring information of the Direct Mail service.

Alarm service

CloudMonitor provides alarm functions for Direct Mail monitoring metrics, so that you are notified immediately in case of any metric exceptions.

Set alarm rules

1. Log on to the *CloudMonitor console*.
2. Go to the**Direct Mail monitoring** page under **Cloud Service Monitoring**.
3. Click Alarm Rules to go to the Alarm Rules list page. Click Create Alarm Rules in the upper-right corner to create alarm rules.

Or click the bell icon in the upper-right corner of the monitoring chart or New Alarm Rule in the upper-right corner of the page to set an alarm rule for corresponding monitoring metrics of this instance.

6.20 Elasticsearch monitoring

CloudMonitor enables the user to monitor the usage of Elasticsearch services by collecting monitoring metrics such as the cluster status of Elasticsearch, the cluster query QPS, and the cluster writing QPS. Users can also set alarm rules for monitoring metrics. After you purchase the Elasticsearch, CloudMonitor automatically collects data on the preceding monitoring metrics.

Monitoring service

- Monitoring metrics

Monitoring metrics	Dimension	Unit	Minimum monitoring granularity
Cluster status	Cluster		1 minute
Cluster query QPS	Cluster	Count/Second	1 minute
Cluster writing QPS	Cluster	Count/Second	1 minute
Node CPU usage	Node	%	1 minute
Node disk usage	Node	%	1 minute
Node heapmemory usage	Node	%	1 minute
Node: load_1m	Node		1 minute
Node FullGc times	Node	Count	1 minute
Node Exception times	Node	Count	1 minute
Cluster snapshot status	Cluster	-1 indicates that there is no snapshot; 0 indicates success; 1 indicates in progress; 2 indicates failure	1 minute

Note:

- Monitoring data is saved for up to 31 days.

- You can view the monitoring data for up to 14 consecutive days.

- View monitoring data

  1. Log on to the *CloudMonitor console*.
  2. Go to the **Elasticsearch** instance list under **Cloud Service Monitoring**.
  3. Click an instance name or click **Monitoring Chart** in the **Actions** column to access the instance monitoring details page and view various metrics.
  4. Click a **Time Range** shortcut on the top of the page or use the specific selection function. Up to 14 consecutive days of metric data can be viewed.
  5. Click Zoom In in the upper-right corner of the monitoring chart to enlarge the chart.

Alarm service

- Parameter description

  — Monitoring metrics: the monitoring metrics provided by the Elasticsearch service.

  — Statistical cycle: the alarm system checks whether your monitoring data has exceeded the alarm threshold based on the cycle. For example, if the statistical cycle of the alarm rule for memory usage is set to one minute, the system checks whether the memory usage has exceeded the threshold value every other minute.

  — Consecutive times: an alarm is triggered when the value of the monitoring metrics continuously exceeds the threshold value for the set consecutive cycles.

- Set an alarm rule

  1. Log in to the cloud monitoring console.
  2. Go to the **Elasticsearch** instance list under **Cloud Service Monitoring**.
  3. Click an instance name or click **Monitoring Chart** in the **Actions** column to access the instance monitoring details page.
  4. Click Bell icon in the upper-right corner of the monitoring chart or **New Alarm Rule** in the upper-right corner of the page to set an alarm rule for corresponding monitoring metrics of this instance.

6.21 E-MapReduce monitoring

To help you monitor the operation of clusters, CloudMonitor offers multiple monitoring metrics for E-MapReduce clusters, including CPU idleness, memory capacity, and disk capacity. It also

allows you to set alarm rules for these monitoring metrics. After you purchase the E-MapReduce service, CloudMonitor auto collects data for the aforementioned monitoring metrics.

Monitoring service

- Metrics

Metric	Dimension	Unit	Minimum monitoring granularity
Inbound traffic rate	User, cluster, and role	bits/s	30s
Outbound network rateNetwork drain Rate	User, cluster, and role	bits/s	30s
CPU idleness	User, cluster, and role	%	1 minute
User-mode CPU usage	User, cluster, and role	%	30s
System-mode CPU usage	User, cluster, and role	%	30s
Idle disk capacity	User, cluster, and role	Bytes	30s
Total disk capacity	User, cluster, and role	Bytes	30s
Average load within 15 minutes	User, cluster, and role	-	30s
Average load within 5 minutes	User, cluster, and role	-	30s
Average load within 1 minutes	User, cluster, and role	-	30s
Idle memory capacity	User, cluster, and role	Bytes	30s
Total memory capacity	User, cluster, and role	Bytes	30s
Inbound data packet rate	User, cluster, and role	Packets/s	30s
Outbound data packet rate	User, cluster, and role	Packets/s	30s
Number of running processes	User, cluster, and role	Processes	30s

Metric	Dimension	Unit	Minimum monitoring granularity
Total number of processes	User, cluster, and role	Processes	30s
Number of blocked processes	User, cluster, and role	Processes	30s
Number of created processes/threads	User, cluster, and role	Processes/threads	30s
MemNonHeapUsedM	User, cluster, and role	Bytes	30s
MemNonHeap CommittedM	User, cluster, and role	Bytes	30s
Memnonheapmaxm	User, cluster, and role	Bytes	30s
MemHeapUsedM	User, cluster, and role	Bytes	30s
MemHeapCom mittedM	User, cluster, and role	Bytes	30s
MemHeapMaxM	User, cluster, and role	Bytes	30s
MemMaxM	User, cluster, and role	Bytes	30s
Threadsnew	User, cluster, and role	-	30s
ThreadsRunnable	User, cluster, and role	-	30s
ThreadsBlocked	User, cluster, and role	-	30s
ThreadsWaiting	User, cluster, and role	-	30s
ThreadsTimedWaiting	User, cluster, and role	-	30s
ThreadsTerminated	User, cluster, and role	-	30s
GcCount	User, cluster, and role	-	30s
GcTimeMillis	User, cluster, and role	-	30s
CallQueueLength	User, cluster, and role	-	30s
NumOpenCon nections	User, cluster, and role	-	30s
ReceivedBytes	User, cluster, and role	-	30s
SentBytes	User, cluster, and role	-	30s
BlockCapacity	User, cluster, and role	-	30s

Metric	Dimension	Unit	Minimum monitoring granularity
BlocksTotal	User, cluster, and role	-	30s
CapacityRemaining	User, cluster, and role	-	30s
CapacityTotal	User, cluster, and role	-	30s
CapacityUsed	User, cluster, and role	-	30s
CapacityUsedNonDFS	User, cluster, and role	-	30s
CorruptBlocks	User, cluster, and role	-	30s
ExcessBlocks	User, cluster, and role	-	30s
ExpiredHeartbeats	User, cluster, and role	-	30s
MissingBlocks	User, cluster, and role	-	30s
PendingDataNodeMessageCount	User, cluster, and role	-	30s
PendingDeletionBlocks	User, cluster, and role	-	30s
PendingReplicationBlocks	User, cluster, and role	-	30s
PostponedMisreplicatedBlocks	User, cluster, and role	-	30s
ScheduledReplicationBlocks	User, cluster, and role	-	30s
TotalFiles	User, cluster, and role	-	30s
TotalLoad	User, cluster, and role	-	30s
UnderReplicatedBlocks	User, cluster, and role	-	30s
BlocksRead	User, cluster, and role	-	30s
BlocksRemoved	User, cluster, and role	-	30s
BlocksReplicated	User, cluster, and role	-	30s
BlocksUncached	User, cluster, and role	-	30s
BlocksVerified	User, cluster, and role	-	30s

Metric	Dimension	Unit	Minimum monitoring granularity
BlockVerificationFailures	User, cluster, and role	-	30s
BlocksWritten	User, cluster, and role	-	30s
BytesRead	User, cluster, and role	-	30s
BytesWritten	User, cluster, and role	-	30s
FlushNanosAvgTime	User, cluster, and role	-	30s
FlushNanosNumOps	User, cluster, and role	-	30s
FsyncCount	User, cluster, and role	-	30s
VolumeFailures	User, cluster, and role	-	30s
ReadBlockOpNumOps	User, cluster, and role	-	30s
ReadBlockOpAvgTime	User, cluster, and role	ms	30s
WriteBlockOpNumOps	User, cluster, and role	-	30s
WriteBlockOpAvgTime	User, cluster, and role	ms	30s
BlockChecksumOpNumOps	User, cluster, and role	-	30s
BlockChecksumOpAvgTime	User, cluster, and role	ms	30s
CopyBlockOpNumOps	User, cluster, and role	-	30s
CopyBlockOpAvgTime	User, cluster, and role	ms	30s
ReplaceBlockOpNumOps	User, cluster, and role	-	30s
ReplaceBlockOpAvgTime	User, cluster, and role	ms	30s
BlockReportsNumOps	User, cluster, and role	-	30s

Metric	Dimension	Unit	Minimum monitoring granularity
BlockReportsAvgTime	User, cluster, and role	ms	30s
NodeManager_AllocatedContainers	User, cluster, and role	-	30s
ContainersCompleted	User, cluster, and role	-	30s
ContainersFailed	User, cluster, and role	-	30s
ContainersIniting	User, cluster, and role	-	30s
ContainersKilled	User, cluster, and role	-	30s
ContainersLaunched	User, cluster, and role	-	30s
ContainersRunning	User, cluster, and role	-	30s
ActiveApplications	User, cluster, and role	-	30s
ActiveUsers	User, cluster, and role	-	30s
AggregateContainersAllocated	User, cluster, and role	-	30s
AggregateContainersReleased	User, cluster, and role	-	30s
AllocatedContainers	User, cluster, and role	-	30s
AppsCompleted	User, cluster, and role	-	30s
AppsFailed	User, cluster, and role	-	30s
AppsKilled	User, cluster, and role	-	30s
AppsPending	User, cluster, and role	-	30s
AppsRunning	User, cluster, and role	-	30s
AppsSubmitted	User, cluster, and role	-	30s
AvailableMB	User, cluster, and role	-	30s
AvailableVCores	User, cluster, and role	-	30s
PendingContainers	User, cluster, and role	-	30s
ReservedContainers	User, cluster, and role	-	30s

Note:

- Monitoring data is preserved for at most 31 days.
- - You can view monitoring data for a maximum of 14 consecutive days.

- Viewing Monitoring Data

1. Log in to the *cloud monitoring console*.
2. Go to the **E-MapReduce** instance list under **Cloud Service Monitoring**.
3. Click an instance name or click Monitoring Chart in the Action column to access the instance monitoring details page and view various metrics.
4. Click the Time Range quick selection button at the top of the page or use the specific selection function. You can view the monitoring data for up to 14 consecutive days.
5. Click the Zoom In button in the upper-right corner of the monitoring chart to enlarge the chart.

Alarm service

- Parameter descriptions

— Monitoring metrics: the monitoring metrics provided by the E-MapReduce service.

— Statistical cycle: the alarm system checks whether your monitoring data has exceeded the alarm threshold based on the cycle. For example, if the statistical cycle of the alarm rule for memory usage is set to one minute, the system checks whether the memory usage has exceeded the threshold value every other minute.

— Statistical method: refers to the method used to determine if the data exceeds the threshold . The average value, maximum value, minimum value, and sum value can be set as the statistical method.

1. Average: The average value of metric data within a statistical period. For example, when the average value of all monitoring data collected within 15 minutes is adopted as the statistical method, an average value over 80% is deemed to exceed the threshold.
2. Maximum: The maximum value of metric data within a statistical period. For example, when the maximum value of all monitoring data collected within 15 minutes is adopted as the statistical method, a maximum value over 80% is deemed to exceed the threshold.
3. Minimum: The minimum value of metric data within a statistical period. For example, when the minimum value of all monitoring data collected within 15 minutes is adopted as the statistical method, a minimum value over 80% is deemed to exceed the threshold.
4. Sum: The sum of metric data within a statistical period. For example, when the sum value of all monitoring data collected within 15 minutes is adopted as the statistical

method, a sum value over 80% is deemed to exceed the threshold. The above statistic methods are needed for traffic-based indexes.

- Consecutive times: an alarm is triggered when the value of the monitoring metrics continuously exceeds the threshold value for the set consecutive cycles.

  Example: Set CPU usage to more than 80% alarm, statistical cycle to 5 minutes, 3 consecutive The alarm after the threshold is exceeded, the first time the detection CPU usage exceeds 80%, the alarm notification is not issued. The second time in 5 minutes to probe the CPU Usage is more than 80%, and no alarm will be issued. The third probe still exceeds 80% Alarm notification will be issued only when. Therefore, from the first time when the actual data exceeds the threshold to the time when the alarm rule is triggered, the minimum time consumed is: the statistical cycle*(the number of consecutive detections-1), which is 5*(3-1) = 10 minutes in this case.

- Set an alarm rule

  1. Log in to the *cloud monitoring console* .
  2. Go to the **E-MapReduce** instance list under **Cloud Service Monitoring**.
  3. Click an instance name or click Monitoring Chart in the Action column to access the instance monitoring details page.
  4. Click the Bell button in the upper-right corner of the monitoring chart or New Alarm Rule in the upper-right corner of the page to set an alarm rule for corresponding monitoring metrics of this instance.

6.22 Auto Scaling

CloudMonitor monitors multiple metrics, such as the minimum and maximum numbers of instances in an auto scaling group. It helps you monitor the status of instances in an auto scaling group and set alert policies for metrics. After you buy the auto scaling service, CloudMonitor will automatically collect data on the metrics listed above.

Monitoring Services

- Monitoring items

Monitoring items	Dimensions	Unit	Minimum monitor Granularity
Minimum number of instances	User dimension, elastic scaling group	Items	5 minutes

Monitoring items	Dimensions	Unit	Minimum monitor Granularity
Maximum number of instances	User dimension, elastic scaling group	Items	5 minutes
Total number of instances	User dimension, elastic scaling group	Items	5 minutes
Number of running instances	User dimension, elastic scaling group	Items	5 minutes
Joining instance number	User dimension, elastic scaling group	Items	5 minutes
Removing number of instances	User dimension, elastic scaling group	Items	5 minutes

Note:

- Monitor Data is saved for up to 31 days.
- Users can view monitoring data for up to 14 days in a row.

- Viewing Monitoring Data

1. Log in to the cloud monitoring console.
2. Go to the auto scaling group list in "Auto scaling" under "Cloud Service Monitoring".
3. Click the Instance name or the monitor chart in the operation to go To the instance monitoring details page to view the metrics.
4. Click the time range quick select button or the exact select function at the top of the page , the maximum monitoring data allows you to view the monitored data for 14 consecutive days.
5. Click the zoom in button in the upper-right corner of the monitor MAP to view the monitor larger image.

Alarm service

- Parameter descriptions

— Metrics: Monitoring indexes provided by the auto scaling service.

— Statistical Cycle: the alarm system checks if your monitoring data exceeds the alarm threshold for this cycle. For example, to set a memory usage alarm rule, the statistics cycle is 1 minute, an interval of 1 minute checks if memory usage exceeds the threshold.

- Statistical Methods: Statistical Methods refer to settings that exceed the threshold range. You can set the average, maximum, minimum, count, and value in a statistical method.
  - Average: the average of the monitored data during the statistical cycle. For example, the statistical method selects the average of all monitoring data collected in 15 minutes, when the average is greater than 80% Only when the threshold is exceeded.
  - Maximum: the maximum value of the monitor data during the statistics cycle. For example, when the statistic result is the maximum value of all metric data collected within 15 minutes, an average value of over 80% is deemed to exceed the threshold. Only when the threshold is exceeded.
  - Minimum: the minimum value of the monitored data during the statistics cycle. For example, when the statistic result is the minimum value of all metric data collected within 15 minutes, an average value of over 80% is deemed to exceed the threshold. Only when the threshold is exceeded.
  - Value: Sum of monitoring data during the statistics cycle. For example, Statistical Methods select the requirements and values for all monitoring data collected in 15 minutes, when the value is greater than 80% Only when the threshold is exceeded. Such statistical methods are required for traffic-class metrics.
- Continuous number of times: refers to the continuous number of statistical cycle monitoring items that continue to exceed the threshold value to trigger the alarm.

  Example: Set CPU usage to more than 80% alarm, statistical cycle to 5 minutes, 3 consecutive The alarm after the threshold is exceeded, the first time the detection CPU usage exceeds 80%, the alarm notification is not issued. The second time in 5 minutes to detect CPU usage exceeds 80% and no alarm will be issued. The third probe still exceeds 80% Alarm notification will be issued only when. That is, from the first time the actual data exceeds the threshold to the final alarm rule, the minimum time required is statistical cycle X (number of consecutive probes-1) = 5 x (3-1) = 10 minutes.

- Set single alarm rule

1. Log in to the cloud monitoring console.
2. Go to the auto scaling group list in "Auto scaling" under "Cloud Service Monitoring".
3. Click the Instance name or the monitor chart in the operation to enter the instance monitoring details page.

4. Click the bell button in the upper right corner of the monitor chart or the new alarm rule in the upper right corner of the page, alarm rules can be set for monitoring items correspond ing to this instance.

- Set up bulk alarm rules

1. Log in to the cloud monitoring console.
2. Enter the list of elastic scale monitoring instances monitored by the cloud service.
3. Select the appropriate instance on the instance list page. Then, click "Set Alert Policies" at the bottom of the page to add multiple alert policies.

6.23 Express Connect monitoring

CloudMonitor monitors multiple metrics, such as the inbound and outbound network traffic of the Express Connect instance. It monitors the network usage of the instance and allows you to set alarm rules for various metrics. Once you buy the Express Connect service, CloudMonitor automatically collects the data for the following metrics.

Monitoring services

- Monitoring items

Monitoring item	Dimension	Unit	Minimum monitoring granularity
Inbound network traffic	User and instance	Bytes	1 minute
Outbound network traffic	User and instance	Bytes	1 minute
Inbound network bandwidth	User and instance	Bits/s	1 minute
Outbound network bandwidth	User and instance	Bits/s	1 minute
Latency	User and instance	ms	1 minute
Packet loss rate	User and instance	%	1 minute

Note:

- Monitoring data is saved for up to 31 days.

- You can view the monitoring data for up to 14 consecutive days.

- View monitoring data

1. Log on to the *CloudMonitor console*.
2. Enter the instance list of **Express Connect** under **Cloud Service Monitoring**.
3. Click an instance name or click **Monitoring Chart** in the **Action** column to access the instance monitoring details page and view metrics.
4. Click a **Time Range** shortcut on the top of the page or use the specific selection function. Up to 14 consecutive days of metric data can be viewed.
5. Click the zoom-in button in the upper-right corner of the monitoring chart to view a large image.

Alarm service

- Parameter description

  - Metrics: metric items provided by the Express Connect service.
  - Statistical Cycle: indicates how often the alarm system checks whether monitoring data exceeds the alarm threshold. For example, if the statistical cycle of the alarm rule for memory usage is set to one minute, the system checks whether the memory usage has exceeded the threshold value every other minute.
  - Statistical Methods: determines whether the data exceeds the threshold. Average, maximum, minimum, and sum can be set in the Statistical Methods.
    - Average value: the average value of monitoring data within the statistical cycle. For example, when the average value of all monitoring data collected within 15 minutes is used as the statistical method, an average value over 80% is deemed to exceed the threshold.
    - Maximum value: the maximum value of monitoring data within the statistical cycle. For example, when the maximum value of all monitoring data collected within 15 minutes is used as the statistical method, a maximum value over 80% is deemed to exceed the threshold.
    - Minimum value: the minimum value of monitoring data within the statistical cycle. For example, when the minimum value of all monitoring data collected within 15 minutes is used as the statistical method, a minimum value over 80% is deemed to exceed the threshold.

- Sum value: the sum of monitoring data within the statistical cycle. For example, when the sum value of all monitoring data collected within 15 minutes is used as the statistica l method, a sum value over 80% is deemed to exceed the threshold. This method is required for traffic metrics.

— Consecutive times: An alarm is triggered when the value of the monitoring metrics continuously exceeds the threshold value for the set consecutive cycles.

For example, you have set the alarm to go off when the CPU usage exceeds the threshold value of 80% for three consecutive 5-minute statistical cycles. That is to say, no alarm is triggered when the CPU usage is found to exceed 80% for the first time. No alarm is triggered either when the CPU usage exceeds 80% again in the second detection five minutes later. The alarm is triggered when the CPU usage exceeds 80% again in the third detection. Therefore, from the first time when the actual data exceeds the threshold to the time when the alarm rule is triggered, the minimum time consumed is: the statistical cycle x (the number of consecutive detections - 1), which is 5 x (3 - 1) = 10 minutes in this case.

- Set an alarm rule

  1. Log on to *CloudMonitor console*.
  2. Enter the instance list of **Express Connect** under **Cloud Service Monitoring**.
  3. Click an instance name or click **Monitoring Chart** in the **Action** column to access the instance monitoring details page and view metrics.
  4. Click the Bell button in the upper-right corner of the monitoring chart or **New Alarm Rule** in the upper-right corner of the page to set an alarm rule for corresponding monitoring metrics of this instance.

- Set alarm rules in batches

  1. Log on to *CloudMonitor console*.
  2. Enter the instance list of **Express Connect** under **Cloud Service Monitoring**.
  3. Select instances on the instance list page. Click **Set Alarm Rules** to add multiple alarm rules.

6.24 Function Compute monitoring

CloudMonitor provides monitoring metrics for Function Compute on the Service and Function levels, including TotalInvocations, average duration, and request status distribution, to help you monitor the service status of Function Compute in real time and set alarm rules for the monitoring

metrics. After you purchase and use the Function Compute service, CloudMonitor automatically collects data on the preceding metrics.

Monitoring service

- Metrics

Metric	Dimension	Unit	Minimum monitor Granularity
Billableinvocations	User, service, and function	Count	1 minute
BillableInvocationsRate	User, service, and function	Percent	1 minute
ClientErrors	User, service, and function	Count	1 minute
ClientErrorsRate	User, service, and function	Percent	1 minute
ServerErrors	User, service, and function	Count	1 minute
ServerErrorsRate	User, service, and function	Percent	1 minute
Throttles	User, service, and function	Count	1 minute
ThrottlesRate	User, service, and function	Percent	1 minute
Totalinvocations	User, service, and function	Count	1 minute
Average duration	User, service, and function	Millisecond	1 minute

Note:

- Monitoring data is saved for up to 31 days.
- You can view the monitoring data for up to 14 consecutive days.

- View monitoring data

1. Log on to the *CloudMonitor console*.

2. Go to the Function Compute monitoring page under **Cloud Service Monitoring**, and view the overall monitoring data of the **Function Compute** service.
3. Click **Service List** to view the monitoring information on the Service or Function level.

Alarm service

CloudMonitor provides alarm functions for Function Compute monitoring metrics, so you are notified immediately in case of any metric exceptions.

Set alarm rules

- Method 1
  1. Log on to the *CloudMonitor console*.
  2. Go to the **Function Compute** monitoring page under **Cloud Service Monitoring**.
  3. In the Service or Function list, click Monitoring Chart in the Action column to access the monitoring details page.
  4. Click the bell icon in the upper-right corner of the monitoring chart or **New Alarm Rule** in the upper-right corner of the page to set an alarm rule for corresponding monitoring metrics of this instance.
- Method 2
  1. Log on to the *CloudMonitor console*.
  2. Go to the **Function Compute** monitoring page under **Cloud Service Monitoring**.
  3. Click the Alarm Rules to go to the **Alarm Rules** list page. Click **Create** in the upper-right corner to create alarm rules.

6.25 StreamCompute

CloudMonitor provides service latency metrics of StreamCompute to help you monitor the performance of the StreamCompute service and set alarm rules for the monitoring metrics. After you purchase the StreamCompute service, CloudMonitor auto collects data on the preceding metrics.

Monitoring service

- Metrics

Metric	Dimension	Unit	Description	Minimum monitor Granularity
Service latency	Project, job	Second	Data processing latency of the current job	1 minute
Read in RPS	Project, job	RPS	Average number of data lines read per second for tasks	1 minute
Write RPS	Project, job	RPS	Average number of data lines written per second for tasks	1 minute
FailoverRate	Project, job	%	Measure the current job failover frequency, the lower the better.	1 minute

Note:

- Monitoring data is saved for up to 31 days.
- You can view the monitoring data for up to 14 consecutive days.

- Viewing Monitoring Data

1. Log on to the *CloudMonitor console*.
2. Go to the **StreamCompute** instance list under **Cloud Service Monitoring**.
3. Click an instance name or click **Monitoring Chart** in the **Actions** column to access the instance monitoring information page and view various metrics.
4. Click **Time Range** quick selection button from the upper menu of the page or use the specific selection function. You can view the monitoring data for up to 14 consecutive days.
5. Click Zoom In in the upper-right corner of the monitoring chart to enlarge the chart.

Alarm service

- Parameter descriptions

  — Monitoring metrics: The monitoring metrics provided by the StreamCompute service.

- Statistical cycle: The alarm system checks whether your monitoring data has exceeded the alarm threshold based on the cycle. For example, if the statistical cycle of the alarm rule for memory usage is set to one minute, the system checks whether the memory usage has exceeded the threshold value every other minute.
- Statistical method: Indicates the method used to determine if the data exceeds the threshold. The average value, maximum value, minimum value, and sum value can be set as the statistical method.
  - Average value: The average value of monitoring data within the statistical cycle. For example, when the average value of all monitoring data collected within 15 minutes is adopted as the statistical method, an average value over 80% is deemed to exceed the threshold.
  - Maximum value: The maximum value of monitoring data within the statistical cycle. For example, when the maximum value of all monitoring data collected within 15 minutes is adopted as the statistical method, a maximum value over 80% is deemed to exceed the threshold.
  - Minimum value: The minimum value of monitoring data within the statistical cycle. For example, when the minimum value of all monitoring data collected within 15 minutes is adopted as the statistical method, a minimum value over 80% is deemed to exceed the threshold.
  - Sum value: The sum of monitoring data within the statistical cycle. For example, when the sum value of all monitoring data collected within 15 minutes is adopted as the statistical method, a sum value over 80% is deemed to exceed the threshold. This method is required for traffic metrics.
- Consecutive times: An alarm is triggered when the value of the monitoring metrics continuously exceeds the threshold value for the set consecutive cycles.

  For example, you have set the alarm to go off when the CPU usage exceeds the threshold value of 80% for three consecutive 5-minute statistical cycles. That is to say, no alarm is triggered when the CPU usage is found to exceed 80% for the first time. No alarm is triggered either when the CPU usage exceeds 80% again in the second detection five minutes later. The alarm is triggered when the CPU usage exceeds 80% again in the third detection. Therefore, from the first time when the actual data exceeds the threshold to the time when the alarm rule is triggered, the minimum time consumed is: the statistical cycle(the number of consecutive detections-1), which is 5(3-1) = 10 minutes in this case.

- Set an alarm rule

  1. Log on to the *CloudMonitor console*.
  2. Go to the **StreamCompute** instance list under **Cloud Service Monitoring**.
  3. Click an instance name or click **Monitoring Chart** in the **Actions** column.
  4. Click the bell icon in the upper-right corner of the monitoring chart or **New Alarm Rule** in the upper-right corner of the page to set an alarm rule for corresponding monitoring metrics of this instance.

- Set multiple alarm rules

  1. Log on to the *CloudMonitor console*.
  2. Go to the **StreamCompute** instance list under **Cloud Service Monitoring**.
  3. Select the expected instances on the instance list page. Click **Set Alarm Rules** to add multiple alarm rules.

6.26 ApsaraDB for HybridDB

Cloud monitoring through monitoring hybriddb's CPU usage, memory usage, and so on, helps the user monitor the usage of the hybridgedb instance and enables the user to set alarm rules on the monitor item. After you purchase After hybridgedb, cloud monitoring automatically collects data for the above monitoring items.

Monitor

- Monitoring items

Monitoring items	Dimension	Unit	Minimum monitor Granularity
Disk usage	User and instance	%	5 minutes
Connection usage	User and instance	%	5 minutes
CPU usage	User and instance	%	5 minutes
Memory usage	User and instance	%	5 minutes
I/O throughput usage	User and instance	%	5 minutes

Note:

- Monitor Data is saved for up to 31 days.
- Users can view monitoring data for up to 14 days in a row.

- View monitored data.

  1. Log in to the *cloud monitoring console*.
  2. Go to the HybridDB instance list under Cloud Service Monitoring.
  3. Click an instance name or click **Monitoring Chart** in the **Actions** column to access the instance monitoring information page and view various metrics.
  4. Click the time range quick select button or the exact select function at the top of the page, maximum monitoring data support view continuous 14 Monitoring data for days.
  5. Click the zoom in button in the upper-right corner of the monitor MAP to view the monitor larger image.

Alarm service

6.27 NAT gateway monitoring

CloudMonitor provides multiple monitoring metrics for NAT Gateway, including the SNAT connections to help you monitor network usage of the NAT Gateway service and set alarm rules for the monitoring metrics. After you purchase the NAT gateway service, CloudMonitor automatica lly collects data on the preceding monitoring metrics.

Monitoring Service

- Metrics

Metric	Dimension	Unit	Minimum monitor Granularity
SNAT connections	User and instance	Count/Min	1 minute
Package inbound bandwidth	User and instance	Bits/s	1 minute
Package outbound bandwidth	User and instance	Bits/s	1 minute
Package inbound packet	User and instance	pps	1 minute
Package outbound packet	User and instance	pps	1 minute
Package outbound bandwidth usage	User and instance	%	1 minute

Note:

- Monitoring data is saved for up to 31 days.
- You can view the monitoring data for up to 14 consecutive days.

- View monitoring data

1. Log on to the *CloudMonitor console*.
2. Go to the **NAT Gateway** instance list under **Cloud Service Monitoring**.
3. Click an instance name or click **Monitoring Chart** in the **Actions** column to access the instance monitoring details page and view various metrics.
4. Click **Time Range** quick selection button from the upper menu or use the specific selection function. You can view the monitoring data for up to 14 consecutive days.
5. Click Zoom In in the upper-right corner of the monitoring chart to enlarge the chart.

Alarm service

- Parameter descriptions

  — Monitoring metrics: The monitoring metrics provided by the NAT Gateway service.

  — Statistical cycle: The alarm system checks whether your monitoring data has exceeded the alarm threshold based on the cycle. For example, if the statistical cycle of the alarm rule for memory usage is set to one minute, the system checks whether the memory usage has exceeded the threshold value every other minute.

  — Consecutive times: An alarm is triggered when the value of the monitoring metrics continuously exceeds the threshold value for the set consecutive cycles.

- Set an alarm rule

1. Log on to the *CloudMonitor console*.
2. Go to the **NAT Gateway** instance list under **Cloud Service Monitoring**.
3. Click an instance name or click **Monitoring Chart** in the **Actions** column to access the instance monitoring details page.
4. Click the bell icon in the upper-right corner of the monitoring chart or **New Alarm Rule** in the upper-right corner of the page to set an alarm rule for corresponding monitoring metrics of this instance.

- Set multiple alarm rules

1. Log on to the *CloudMonitor console*.

2. Go to the **NAT Gateway** instance list under **Cloud Service Monitoring**.
3. Select the appropriate instances on the instance list page. Click **Set Alarm Rules** to add multiple alarm rules.

6.28 Open Ad monitoring

CloudMonitor provides 13 monitoring metrics for Open Ad, including RTB PV, RTB QPS, and ad click PV, to help you monitor the service status of Open Ad in real time and set alarm rules for the monitoring metrics. After you purchase and use the Open Ad service, CloudMonitor automatically collects data on the preceding metrics.

Monitoring service

- Metrics

Metric	Dimension	Unit	Minimum monitor Granularity
RTB PV	User	Count	1 minute
RTB QPS	User	Times/second	1 minute
Ad click PV	User	Count	1 minute
Ad click QPS	User	Times/second	1 minute
Ad click Delay	User	Millisecond	1 minute
Ad exposure PV	User	Count	1 minute
Ad exposure QPS	User	Times/second	1 minute
Ad exposure Delay	User	Milliseconds	1 minute
DMP active crowd count	User	Days/day	1 hour
DMP valid crowd requests	User	Next/day	1 hour
Storage space utilized by DMP	User	Bytes/day	1 hour
League + dip effective crowd count	User	Days/day	1 hour
Valid audience number in Umeng + DIP	User	Next/day	1 hour

Note:

- Monitor Data is saved for up to 31 days.
- Users can view monitoring data for up to 14 days in a row.

- Viewing monitoring data

  1. Log on to the *CloudMonitor console*.
  2. Go to the **Open Ad monitoring page** under **Cloud Service Monitoring,** and view the overall monitoring data of the Open Ad service.

Alarm service

CloudMonitor provides alarm functions for Open Ad monitoring metrics, so that you are notified immediately in case of any metric exceptions.

Set alarm rules

- Method 1

  1. Log on to the *CloudMonitor console*.
  2. Go to the **Open Ad monitoring page** under **Cloud Service Monitoring**.
  3. Click the bell icon in the upper-right corner of the monitoring chart or New Alarm Rule in the upper-right corner of the page to set an alarm rule for corresponding monitoring metrics of this instance.

- Method 2

  1. Log on to the *CloudMonitor console*.
  2. Go to the **Open Ad monitoring page** under **Cloud Service Monitoring**.
  3. Click **Alarm Rules** to go to the Alarm Rules list page. Click **Create Alarm Rules** in the upper-right corner to create alarm rules.

6.29 OpenAPI monitoring

Cloud monitoring by providing calls to the Ali cloud openapi, the number of errors, the rate of errors, helps users monitor the usage of the Ali cloud openapi, and enables users to set alarm rules on monitoring items. When users use the Ali cloud openapi, cloud monitoring automatically collects data for the above monitoring items.

Monitoring Services

- Monitoring items

Monitoring items	Dimensions	Unit	Minimum monitor Granularity	Description
Number of calls	Product Dimension, API dimension	Items	60 s	The total number of calls to interfaces during the statistics cycle
Number of errors	Product Dimension, API dimension	Items	60 s	Number of times the return status code is greater than or equal to 500 called during the statistics cycle
Error Rate	Product Dimension, API dimension	%	60 s	Number of times the return status code is greater than or equal to 500 in the statistics cycle/ total number of calls * 100

Note:

- Monitor Data is saved for up to 31 days.
- Users can view monitoring data for up to 14 days in a row.

- Viewing Monitoring Data

1. Log in to the cloud monitoring console.
2. Enter the list of interfaces to the openapi that the cloud service monitors.
3. Click the Instance name or the monitor chart in the operation to go To the instance monitoring details page to view the metrics.

4. Click the time range on the top of the page to quickly select a button or select an exact function, the maximum monitoring data allows you to view the monitored data for 14 consecutive days.
5. Click the zoom button in the upper-right corner of the monitor MAP to view the monitor larger image.

Alarm service

- Parameter descriptions
  - Monitoring: that is, the monitoring metrics provided by the Ali cloud openapi.
  - Statistical Cycle: the alarm system checks if your monitoring data exceeds the alarm threshold for this cycle. For example, to set a memory usage alarm rule, the statistics cycle is 1 minute, an interval of 1 minute checks if memory usage exceeds the threshold.
  - Continuous number of times: refers to the continuous number of statistical cycle monitoring items that continue to exceed the threshold value to trigger the alarm.
- Set single alarm rule
  1. Log in to the cloud monitoring console.
  2. Enter the list of interfaces to the openapi that the cloud service monitors.
  3. Click the Instance name or the monitor chart in the operation to go To the instance monitoring details page.
  4. Click the bell button in the upper right corner of the monitor chart or the new alarm rule in the upper right corner of the page, alarm rules can be set for monitoring items correspond ing to this instance.

6.30 OpenSearch Monitor

Cloud Monitoring monitors the storage capacity of open searches, the total number of documents , queries QPS, and other monitoring items, helps users monitor the usage of open search services and enables users to set alarm rules on monitoring items. After you buy the ExpressConnect service, CloudMonitor will automatically collect data on the metrics listed above.

Monitoring Services

- Monitoring items

Monitoring items	Dimensions	Unit	Minimum monitor Granularity
Storage Capacity	APP dimension	Bytes	10 minutes.
Storage capacity usage	APP dimension	%	10 minutes.
Total number of documents	APP dimension	Items	10 minutes.
Querying QPS	APP dimension	Count/second	20 seconds
Query flow limit QPS	APP dimension	Count/second	20 seconds
Time-consuming Query	APP dimension	MS	20 seconds
Calculate Resources	APP dimension	Lcu	20 seconds
Calculate resource usage	APP dimension	%	20 seconds
Calculation of consumption by single query	APP dimension	LCU	20 seconds

Note:

- Monitor Data is saved for up to 31 days.
- Users can view monitoring data for up to 14 days in a row.

- Viewing Monitoring Data

1. Log in to the cloud monitoring console.
2. Enter the list of instances of the open search that the cloud service monitors.
3. Click the Instance name or the monitor chart in the operation to go To the instance monitoring details page to view the metrics.
4. Click the time range on the top of the page to quickly select a button or select an exact function, the maximum monitoring data allows you to view the monitored data for 14 consecutive days.
5. Click the zoom button in the upper-right corner of the monitor MAP to view the monitor larger image.

Alarm service

- Parameter descriptions
  - Monitoring item: that is, the monitoring indicator provided by the open search service.
  - Statistical Cycle: the alarm system checks if your monitoring data exceeds the alarm threshold for this cycle. For example, to set a memory usage alarm rule, the statistics cycle is 1 minute, an interval of 1 minute checks if memory usage exceeds the threshold.
  - Continuous number of times: refers to the continuous number of statistical cycle monitoring items that continue to exceed the threshold value to trigger the alarm.
- Set single alarm rule
  1. Log in to the cloud monitoring console.
  2. Enter the list of instances of the open search that the cloud service monitors.
  3. Click the Instance name or the monitor chart in the operation to go To the instance monitoring details page.
  4. Click the bell button in the upper right corner of the monitor chart or the new alarm rule in the upper right corner of the page, alarm rules can be set for monitoring items correspond ing to this instance.
- Set up bulk alarm rules
  1. Log in to the cloud monitoring console.
  2. Enter the list of open search instances that the cloud service monitors.
  3. Select the appropriate instance on the instance list page. Then, click "Set Alert Policies" at the bottom of the page to add multiple alert policies.

6.31 ApsaraDB for PetaData

CloudMonitor provides multiple monitoring metrics, including the minimum and maximum numbers of ApsaraDB for PetaData instances to help you monitor the instance status in a scaling group and set alarm rules for the monitoring metrics. After you purchase the Auto Scaling service , CloudMonitor automatically collects data on the preceding metrics.

Monitoring service

- Metrics

Metric	Dimension	Unit	Minimum monitor Granularity
Disk usage	User and instance	Bytes	5 minutes
Inbound bandwidth	User and instance	Bytes/Second	5 minutes
Outbound bandwidth	User and instance	Bytes/Second	5 minutes
QPS	User and instance	Count/Second	5 minutes

Note:

- Monitor Data is saved for up to 31 days.
- Users can view monitoring data for up to 14 days in a row.

- Viewing monitoring data

1. Log on to the *CloudMonitor console*.
2. Go to the **ApsaraDB for PetaData** instance list under **Cloud Service Monitoring**.
3. Click an instance name or click **Monitoring Chart** in the **Actions** column to access the instance monitoring details page and view various metrics.
4. Click **Time Range** quick selection button from the upper menu of the page or use the specific selection function. You can view the monitoring data for up to 14 consecutive days.
5. Click Zoom In in the upper-right corner of the monitoring chart to enlarge the chart.

Alarm service

- Parameter descriptions

  — Monitoring metrics: The monitoring metrics provided by ApsaraDB for PetaData.

  — Statistical cycle: The alarm system checks whether your monitoring data has exceeded the alarm threshold based on the cycle. For example, if the statistical cycle of the alarm rule for memory usage is set to one minute, the system checks whether the memory usage has exceeded the threshold value every other minute.

  — Statistical method: Indicates the method used to determine if the data exceeds the threshold. The average value, maximum value, minimum value, and sum value can be set as the statistical method.

    ■ Average value: The average value of monitoring data within the statistical cycle. For example, when the average value of all monitoring data collected within 15 minutes is

adopted as the statistical method, an average value over 80% is deemed to exceed the threshold.

- Maximum value: The maximum value of monitoring data within the statistical cycle. For example, when the maximum value of all monitoring data collected within 15 minutes is adopted as the statistical method, a maximum value over 80% is deemed to exceed the threshold.
- Minimum value: The minimum value of monitoring data within the statistical cycle. For example, when the minimum value of all monitoring data collected within 15 minutes is adopted as the statistical method, a minimum value over 80% is deemed to exceed the threshold.
- Sum value: the sum of monitoring data within the statistical cycle. For example, when the sum value of all monitoring data collected within 15 minutes is adopted as the statistica l method, a sum value over 80% is deemed to exceed the threshold. This method is required for traffic metrics.

— Consecutive times: An alarm is triggered when the value of the monitoring metrics continuously exceeds the threshold value for the set consecutive cycles.

For example, you have set the alarm to go off when the CPU usage exceeds the threshold value of 80% for three consecutive 5-minute statistical cycles. The second time in 5 minutes to detect CPU usage exceeds 80% and no alarm will be issued. The third probe still exceeds 80% Alarm notification will be issued only when. That is, from the first time the actual data exceeds the threshold to the final alarm rule, the minimum time required is statistical cycle X (number of consecutive probes-1) = 5 x (3-1) = 10 minutes.

- Set an alarm rule

  1. Log on to the *CloudMonitor console*.
  2. Go to the **ApsaraDB for PetaData** instance list under **Cloud Service Monitoring**.
  3. Click an instance name or click **Monitoring Chart** in the **Actions** column to access the instance monitoring information page.
  4. Click the bell icon or **New Alarm Rule** in the upper-right corner of the monitoring data page to set an alarm rule for corresponding monitoring metrics of this instance.

- Set multiple alarm rules

  1. Log on to the *CloudMonitor console*.
  2. Go to the **ApsaraDB for PetaData** instance list under **Cloud Service Monitoring**.

3. Select the appropriate instances on the instance list page. Click **Set Alarm Rules** to add multiple alarm rules.

7 Custom monitoring

7.1 Custom monitoring

Custom monitoring overview

Custom monitoring is a function that gives users the freedom to define monitoring items and alarm rules. You can monitor concerned services and report collected monitoring data to CloudMonitor in an agreed format through OpenAPI of CloudMonitor, so that CloudMonitor processes the data and generates alarms based on the result.

What is the difference between event monitoring and custom monitoring?

Event monitoring is used to resolve non-continuous event type data monitoring data reporting, querying, and warning scenarios. Custom monitoring scenario used to resolve periodic continuous acquisition of time series monitoring data reporting, querying and warning.

Procedure

- *Reporting Monitoring Data*
- 2) query Monitoring Data

  Once the report of the monitored data is complete, you can view the data that has been reported in the console. You can view all monitoring data in custom monitoring, you can also go to a specified application group to view the relevant Custom monitoring data for this grouping

  — View All custom Monitor Data

  1. Log in to the cloud monitoring console and enter custom monitoring.
  2. Select the corresponding application grouping and monitoring items to enter the time series details page.
  3. Check the time series you want to view.

  — View custom monitoring data under application grouping

  1. Log in to the cloud monitoring console and enter the app grouping list page.
  2. Select the appropriate application grouping to enter the grouping details page.
  3. Click the Customize monitoring menu to go to the custom monitoring details page.
  4. Select the appropriate monitoring item to enter the time series details page.
  5. Check the time series you want to view.

6.

- Set alarm rules

  Custom monitoring provides you with the alarm function, and when you set up an alarm, you need to select the appropriate application grouping, when the alarm is triggered, a notification is sent to the contacts that apply the grouping. If the monitoring data you report requires an alarm, you can configure the alarm rules as follows.

  — Mode one:

  1. Log in to the cloud monitoring console and enter custom monitoring.
  2. Select the corresponding application grouping and monitoring items to enter the time series details page.
  3. Select the time series in which you want to create the alarm, and click set alarm rule in the action.
  4. Enter the create alarm Rule Page, fill in the alarm rule name, set up the appropriate alarm policy and notification method.

  — Mode two:

  1. Log in to the cloud monitoring console and enter the app grouping list page.
  2. Select the appropriate application grouping to enter the custom monitoring page within the app grouping. Select the time series for which you want to create the alarm rule, and in action, tap set alarm rule.
  3. Go to the create alarm Rule Page, fill in the alarm rule name, select the appropriate monitoring item, dimension, alarm policy and notification method.

7.3 Configure a Dashboard

After your monitoring data is reported to custom monitoring, you can create a Dashboard for easy monitoring report query.

- Create a Dashboard

  1. Log on to the *CloudMonitor console*.
  2. On the Dashboard page, click **Create Dashboard**.

- Add a View

  1. On the Dashboard page, click **Add View**.

2. Select the custom monitor module and define the chart name.
3. Select the monitor, statistics, and dimensions that need to be displayed.
4. Click the publish button to save the configuration.

After the release, you can see the following large plates:

8 Alarm Service

8.1 Overview of alarm services

Users can monitor the monitoring items in the host monitor, probe points in the site monitor, instances in the cloud service monitor and customize the monitoring items in the monitor to set alarm rules. You can set alarm rules on all resources, apply grouping, and single instance dimensions.

Host Monitoring Alarm rules

Users can set alarm rules on all monitoring items in the host monitor, cloud monitoring provides a minimum alarm detection frequency of 1 per minute.

- Site Monitoring Alarm rules

  You can create an alarm rule for a probe point in a site monitor. The statistical cycle of the alarm rule in site monitoring is consistent with the detection cycle of the probe point. That is, you create a probe point with a period of 5 minutes, then the statistical cycle of the alarm rule is also 5 minutes, the data returned from the probe point is monitored for 5 minutes to compare whether the actual value exceeds the threshold.

Cloud Service alarm rule

Users can set alarm rules on instances of each product in cloud service monitoring. Alarm rules can be set for the monitoring items of each product.

Custom Monitoring Alarm rules

After the user creates the monitor item, alarm rules can be set for monitoring items such as response time, status code, packet loss rate, and so on for the probe point. The statistics cycle of the alarm rule is consistent with the statistics cycle during the creation of the monitor item.

The alarm service supports SMS, mail, Wangwang, and event subscription in four ways. Wangwang only supports PC-side alarm message push. If you have an Ali cloud app installed, you can also receive alarm Notifications via the Ali cloud app.

8.2 Manage alarm rules

The alarm service is to provide monitoring and alarm capability for users on the cloud, helping you to know the monitoring data anomaly for the first time, deal with problems in a timely manner.

Parameter descriptions

- Products: such as host monitoring, RDS, OSS, etc.
- Resource scope: the scope of action of the alarm rule. It is divided into three areas: all resources, application grouping and instance.
- When a resource range is selected for all resources, the maximum number of resources that are reported is 1000, more than 1000 problems may occur that reach the threshold without warning, it is recommended that you use application grouping to divide resources by business before setting up alarms.
  - All resources: indicates that the rule works on all instances of the corresponding product under the user name. For example, MongoDB with all the resource granularity set The CPU usage is greater than 80% alarm, as long as the MongoDB CPU usage is greater than 80% under the user, it hits this rule.
  - Apply grouping: indicates that the rule works on all instances under an application grouping . For example, set the application grouping granularity of the host. The CPU usage is greater than 80% alarm, as long as there is a host CPU usage greater than 80% under this grouping, it hits this rule.
  - Instance: indicates that the rule only works on a specific instance. For example, a host CPU with instance granularity is set. The usage rate is greater than 80% alarm, and only this instance of CPU usage is greater than 80% will hit this rule.
- Rule name: the name of the alarm rule.
- Rule Description: The body of the alarm rule that defines what conditions the monitoring data meets, trigger alarm rules. For example, the rule is described as a 1 minute average of CPU usage> = 90, the alarm service checks once a minute if the data within 1 minute meets the average of> = 90?

  Alarm rules example: Take host monitoring as an example, A single server monitoring indicator is reported to a data base for 15 seconds and 20 data points for 5 minutes.
  - CPU usage is 5 minutes, with an average of> 90, the meaning is that the average of 20 data points with CPU usage of 5 minutes is greater than 90.

  - CPU usage is 5 minutes, always> 90, the meaning is that the number of 20 data points with CPU usage of 5 minutes is all greater than 90.
  - CPU usage for 5 minutes, as soon as one time> 90, the meaning is that there are at least 1 Number of 20 data points with CPU usage of 5 minutes greater than 90.
  - Public Network Flow flow of 5 minutes, total> 50 m, the meaning is that the result of 20 data points sum for 5 minutes of public network flow is greater than 5 m.
- Alarm after the threshold is exceeded several times in a row: After continuous detection, the results are in accordance with the description of the alarm rules to send alarm notifications.
- Effective time: the effective time of the alarm rule, the alarm rule checks whether the monitoring data requires an alarm only during the effective time.
- Notification object: the contact group that sent the alarm.
- Alarm level: it is divided into critical, warning, info three levels, different levels correspond to different notification methods.
  - Critical: phone voice + mobile phone SMS + mail + DingTalk Robot
  - Warning: SMS + email + DingTalk Robot
  - Info: Mail + DingTalk Robot
- Message Note: Customize alarm message replenishment information. When you fill in your email remarks, your comments are included in the Message notification that is being sent to the alarm.

Managing alarm rules

Cloud monitoring provides users with three portal management alarm rules, respectively, it applies the grouping page, the monitoring list page of various types of monitoring and the alarm rule list page of the alarm service..

- Manage alarm rules in apply groups.
- Manage alarm rules in host monitoring.
- Manage alarm rules in each cloud service monitor.
- Use alarm rules in site monitoring.
- Managing alarm rules in custom monitoring

8.3 Manage alarm contact and alarm contact group

Contact and contact group information is the basis for sending alarm notifications. You need to create the contact and contact group first, and then select the corresponding contact group when creating an alarm rule, to receive alarm notifications.

Manage an alarm contact

You can create, edit, or delete the contact information, such as the email address.

- Create an alarm contact

  1. Log on to the *CloudMonitor console*.
  2. Go to the *Alarm Contact Management* page.
  3. Click **Create Alarm Contact** in the upper-right corner of the page. In the displayed dialog box, enter your email address.

     The email address will be verified when it is being added, in case you enter wrong information and cannot receive alarm notifications in a timely manner.

- Edit an alarm contact

  1. Log on to the *CloudMonitor console*.
  2. Go to the *Alarm Contact Management* page.
  3. Click **Edit** in the **Actions** column to edit the contact information.

- Delete an alarm contact

  1. Log on to the *CloudMonitor console*.
  2. Go to the *Alarm Contact Management* page.
  3. Click **Delete** in the **Actions** column.

Note:

Once a contact is deleted, no CloudMonitor alarm notification is sent to the contact.

Manage an alarm contact group

An alarm contact group may contain one or more alarm contacts. The same alarm contact can be added to multiple alarm contact groups. When alarm rules are being set, all alarm notifications are sent through the alarm contact group.

- Create an alarm contact group

  1. Log on to the *CloudMonitor console*.

2. Go to the *Alarm Contact Management* page.
3. Click the **Alarm Contact Group** menu at the top of the page to switch to the alarm contact group list.
4. Click **Create Alarm Contact Group** in the upper-right corner of the page.
5. Enter the group name and the contacts you want to add to the group.

- Edit an alarm contact group

1. Log on to the *CloudMonitor console*.
2. Go to the *Alarm Contact Management* page.
3. Click the **Alarm Contact Group** menu at the top of the page to switch to the alarm contact group list.
4. Click **Edit** in the **Actions** column to edit the contact group information.

- Delete an alarm contact group

1. Log on to the *CloudMonitor console*.
2. Go to the *Alarm Contact Management* page.
3. Click the **Alarm Contact Group** menu at the top of the page to switch to the alarm contact group list.
4. Click **Delete** in the **Actions** column to delete the contact group.

- Add contacts to a contact group in batches

1. Log on to the *CloudMonitor console*.
2. Go to the *Alarm Contact Management* page.
3. Select the contacts you want to add from the alarm contact list.
4. Click **Add to a contact group** at the bottom of the page.
5. In the displayed dialog box, select the target contact group and click OK.

8.4 Alarm callback

Alarm callback feature allows you to integrate the alarm notifications sent by CloudMonitor into existing maintenance systems or message notification systems. CloudMonitor pushes alarm notifications to a specified public URL through the POST request of HTTP protocol. When you receive the alarm notification, you can make further process according to the notification content.

Note:
The retry policy of alarm callback is three times, and the timeout duration is five seconds.

Create an alarm callback

1. Log on to the *CloudMonitor console*.
2. Select the alarm rule that you want to add a callback to.
3. Enter the URL address to callback in the notification method.

Callback parameter

When an alarm rule callbacks a URL address, the pushed POST request is as follows:

Name	Data types	Description
userId	string	User ID
alertName	string	Alarm name
timestamp	string	Time stamp when the alarm is generated
alertState	string	Alarm status. One of three statuses is returned accordingly, namely OK, ALERT, and INSUFFICIENT_DATA
dimensions	string	The object that has triggered an alarm. For example: [{“userId”:”12345”,”instanceId”:”i-12345”}]
expression	string	Alarm conditions. For example: [{“expression”:”$value>12”,”level”:4,”times”:2}] which indicates that an alarm is triggered when the threshold value is greater than 12 for 2 times in a row. Level=4 means that the alarms are sent to you through email, and level=3 means that the alarms are sent to you through SMS and email. The times field indicates how many times the alarm threshold value is reached in a row when setting alarm rules.
curValue	string	The current value of the monitoring metrics when an alarm is triggered or restored.

Name	Data types	Description
metricName	string	metricName
metricProject	string	Product name. For more information about monitoring metrics and product name, see *Preset monitoring metrics reference*.

The following is an example of a POST request.

```
    "userId":"12345",
    "alertName":"putNewAlarm_group_a37cd898-ea6b-4b7b-a8a8-de017a8327
f6",
    "timestamp":"1508136760",
    "alertState":"ALARM",
    "dimensions":[

            "userId":"12345",
            "instanceId":"i-12345"


   "expression":"[{\"expression\":\"$Average>90\",\"level\":4,\"times
\":2}]" ,
    "Curvalue": "95 ",
    "metricName":"CPUUtilization",
    "metricProject":"acs_ecs_dashboard"
```

8.5 Using the alarm Template

Function description

The alert template function enables you to set and store the alert policies of the metrics of cloud products in templates. When creating alert policies, you can directly use alert templates without defining alert policies all over again. When your account has many cloud resources (ECS, ApsaraDB for RDS, Server Load Balancer, and OSS), it is recommended that you create application groups for these resources from the service perspective and then create and apply alert templates to the application groups. This provides a simple way of creating and maintaining alert policies.

To use the alert template function and application group function in combination, you can create alert templates and apply these templates to application groups so that alert policies can be quickly created for service modules.

By default, CloudMonitor provides an initialized alert template that contains the common alert metrics for ECS、RDS、SLB、CDN、Redis、Mongodb、OSS, allowing you to quickly start using the template.

Note:

- Alert templates can only be used with application groups. That is, alert templates are only applicable to alert policies with the resource range set to "Application Group".
- Up to 100 alert templates can be created under each Alibaba Cloud account.
- Each alert template can contain up to 30 metrics.
- The alert template function only provides a shortcut to create alert policies. There is no one-to-one binding relationship between alert templates and alert policies. After an alert template is modified, the alert policies generated using this template remain unchanged. To modify the alert policies for an application group in batches, modify the corresponding alert template and apply the template to the application group.

Creating or editing a template

1. Log in to the cloud monitor console and click on**Alarm service** > **Alarm Template**Enter the alarm template page.
2. At the upper-right corner of the page, click **Create Alert Template** to go to the page for creating an alert template.
3. Fill out the alert template with the basic information, including the name and description, to facilitate subsequent management of the template and its purpose.
4. Configure the alarm policy, click Add alarm rule, add rule description.
5. Click confirm to save the template.

Using the alarm Template

- Apply an alert template to the application group to be created

  When you create an apply grouping for a resource, you can select the alarm template that is required to apply the grouping directly at the last step. After applying grouping creation success, cloud monitoring generates alarm rules for you to apply grouping dimensions according to the alarm template.

- Apply an alert template directly to an application group

If you have created an application group but have not created alert policies for the group, you can create an alert template and then quickly apply the template to the group.

- Apply an alert template when creating alert policies

  To add alert policies to an application group, select "Application Group" for the resource range on the page for creating alert policies and then select "Create from Template" and the corresponding alert template during alert policy setup. This method enables quick creation of alert policies.

9 Event subscription

9.1 Overview of event subscription services

Event subscription is a way of getting alarm information from cloud monitoring, write the generated alarm information to the user's message queue for the user to consume, docking your own alarm notification system.

You can subscribe to alarm information in the cloud monitor console after the *message service* is turned on. The service flow chart is as follows.

9.2 Usage

By creating an event subscription, cloud monitoring will push the alarm information into the user-specified message queues, users can connect to their own business systems through the alarm information in the consumer queue.

Note:
The frequency at which alarm information is pushed to the queue of the Message Service is also limited by channel silence, the alarm notification is no longer sent when the state of the same alarm rule changes within 24 hours after the alarm.

Operation Steps

1. Provision message service.
2. Authorization for cloud monitoring.

   Select an event subscription in the console. If you are using event subscription for the first time, you need to authorize message to the cloud Monitor Service Message Queuing write permission.

3. Create an event subscription.

   a. Click Create event in the upper-right corner to create an event that receives alarm rules.

b. Select the queue information that needs to receive alarm rules and the alarm category that needs to be received.

4. Consumer alarm information.

You can consume alarm data through the Message Service's API, you can also view the receiving information through the console of the message service.

Alarm information example

ECS

```
    "Message ":{
        "Expression": "average> 80%", // alarm Rule Description
        Curvalue: 85.65 ",
        "Unit": "%", // units
        "Leveldescription": "alarm occurred", // alarm status,
contains "occurrence alarm" and "recovery alarm"
        "Time": 1464257700000, // alarm occurrence time
        "Metricproject": "acs_ecs", // Product Name
        Userid: 1078500464551219 ",
        "Dimensions:" cloud server name = maid, cloud server instance
id = maid, IP = maid, mountpoint =/mnt ", // monitor dimension
        "Collaborationcount": "1", // Number of Retries
        "Period": "5 minutes", // statistics cycle
        Metricname: disk usage, // monitor Indicator Name
        "Alertname": "maid"

    "Type": 0
```

SLB

```
    "Message ":{
        "Expression": "Maximum> 02 kb/s", // alarm Rule Description
        "Curvalue": "5 ",
        "Unit": "kb/s", // units
        "Leveldescription": "alarm occurred", // alarm status,
contains "occurrence alarm" and "recovery alarm"
        "Time": 1451767500000, // alarm occurrence time
        "Metricproject": "acs_slb", // Product Name
        "Userid": "username ",//
        "Dimensions:" instanceid = instanceid, Port = 3306, VIP = maid
 ", // monitoring dimension
        "Collaborationcount": "3", // Number of Retries
        "Period": "15 minutes", // statistics cycle
        "Metricname": "amount of incoming data per second", // monitor
 Indicator Name
        "Alertname": "maid"

    "Type": 0/Reserve field, 0 indicates alarm notification,
occurrence and recovery, 1 Fault Notification, trigger an alarm once,
do not record the status.
```

10 RAM for CloudMonitor

CloudMonitor supports *RAM*. This allows you to control permissions for Cloud Service Monitoring metric data, alarm rule management, alarm contact and alarm contact group management through sub-accounts.

Note:

Currently, metric data queries are supported for the following cloud products:

- ECS
- RDS
- Server Load Balancer
- OSS
- CDN
- ApsaraDB for Memcache
- EIP
- ApsaraDB for Redis
- Message Service
- Log Service

Permission description

In RAM system permissions, the Read-only CloudMonitor access permission only authorizes the sub-account to view relevant data, such as metric data and alarm data.

Authentication type

In addition to basic sub-account permission control, RAM currently supports time, MFA, and IP authentication.

Resource description

Currently, RAM does not support fine-grained resource descriptions. Only the “*” wildcard is used for resource authorization.

Operation description

- Metric data

  Data query actions are divided into two groups: Product instance list display and CloudMonit or metric data queries. When authorizing a sub-account to log on to the CloudMonitor portal

and view metric data, you must also grant the sub-account permissions for the corresponding product's instance list and metric data query.

The corresponding actions are listed in the following table.

Product name	action
CMS	QuerMetricList
CMS	QueryMetricLast
ECS	DescribeInstances
RDS	DescribeDBInstances
SLB	DescribeLoadBalancer*
OSS	ListBuckets
OCS	DescribeInstances
EIP	DescribeEipAddresses
Aliyun Cloud for Redis	DescribeInstances
Message Service	ListQueue
CDN	DescribeUserDomains

- Alarm management

  Alarm management includes alarm rule management, alarm contact and alarm contact group management, and event subscription.

  The query-related actions are listed in the following table.

Action	Meaning
QueryAlarm	Query the alarm rule
QueryAlarmHistory	Query the alarm history
QueryContactGroup	Query the contact group
QueryContact	Query the contact
QuerySms	Query the number of SMSs used
QueryMns	Querying the event subscription configuration

  The management-related actions are listed in the following table.

Action	Meaning
UpdateAlarm	Modify the alarm rule
CreateAlarm	Create the alarm rule
DeleteAlarm	Delete the alarm rule
DisableAlarm	Disable the alarm rule
EnableAlarm	Enable the alarm rule
CreateContact	Create the contact
DeleteContact	Delete the contact
UpdateContact	Modify the contact
SendEmail	Send the email authentication code
SendSms	Send the SMS verification code
CheckEmail	Check the mail verification code
CheckSms	Check the SMS verification code
CreateGroup	Create the contact group
DeleteGroup	Delete the contact group
UpdateGroup	Modify the contact group
CreateMns	Create the event subscription
DeleteMns	Delete the event subscription
UpdateMns	Modify the event subscription

11 Dashboard

11.1 Dashboard

With the launch of the dashboard function in the CloudMonitor, Alibaba Cloud offers you a one-stop metric visualization solution.

It allows you to view detailed metrics for troubleshooting and provides a quick view of the realtime services.

For example, if one of your applications is deployed on multiple ECS instances, you can add metric data of these ECS instances to the same metric chart to view the change trend of the metric data of multiple machines. For example, the CPU usage of multiple ECS instances can be displayed in the time sequence in one chart.

Display the ordering of instance resource consumption

For example, a metric chart can display multiple metrics of an ECS instance, including CPU usage , memory usage, and disk usage.

Display the ordering of instance resource consumption

For example, if you have 20 instances you can view all these instances in descending order in the table. This gives you a quick understanding about resource consumption, how to use resources rationally and avoid unnecessary cost.

Display the realtime metric data distribution of multiple instances

For example, the CPU usage distribution of an ECS instance group can be displayed in a heat map. This helps to What is the level of usage compared to other machines. You can click a color block to view the metric data trend of the corresponding machine in a specified period of time.

Display the aggregated data of a particular metric of multiple instances

For example, you can view the average aggregation value of the CPU usage of multiple ECS instances in one chart, to know about the overall CPU usage and check whether the resource usage of each instance is balanced.

Full-screen display

The dashboard supports full-screen display and automatic data refresh. You can add various product metrics to the dashboard and can view them in a full-screen mode.

11.2 Management Dashboards

Users can create a dashboard, modify a dashboard, delete a dashboard, view a chart in a dashboard.

View dashboards

Dashboard in CloudMonitor provides a custom view of monitoring data. You can view metric data on a monitoring dashboard across many products and instances in a centralized manner.

Note:

- CloudMonitor initializes ECS monitoring dashboards for you and displays ECS metric data.
- Data of one hour, three hours, and six hours can be automatically refreshed. However, data of more than six hours cannot be automatically refreshed.

Procedure

1. Log on to the CloudMonitor console.
2. Click the "Dashboard" option in the left menu to access the "Dashboard" page.
3. By default, the ECS Global Monitor tray is displayed, and you can select another monitor tray in the drop-down list.
4. Click "Full screen" in the top-right corner of the page to view the monitoring dashboard in full screen.
5. Select time range: Click the Time Selection button above the monitor and control page, you can quickly select the monitoring data time range shown in the chart on the large panel. The scope of Time Selection is to monitor the full range of charts on the disk.
6. Automatic Refresh: After you click automatic refresh, when you select a query time span of 1 hour, 3 hours, and so on, you can turn on the automatic refresh function, which can be refreshed once a minute.
7. The units of the monitor are displayed in parentheses for the chart name.
8. The mouse follows a monitor value that displays all charts for the same time.

Create a Dashboard

You can create a new monitoring dashboard and customize the display charts, when your business operations are complex and the default ECS monitoring dashboards does not meet monitoring visualization requirements.

.

Note:
Create up to 20 charts per monitor tray.

操作步骤

1. Log on to the CloudMonitor console.
2. Click **Dashboard** in the navigation pane.
3. In the upper-right corner of the page, click **Create Monitoring Dashboard**.
4. Enter the name of the monitoring dashboard, and click Create to complete the action.
5. The page is automatically redirected to the new monitoring dashboard page where you can add various metric charts as required.
6. The mouse hangs on the monitor tray name, the right hand side changes the name, click to modify the disk name.

Delete a dashboard

You can delete a monitoring dashboard if you do not need it as your business changes.

Note:
When you delete a monitoring dashboard, all monitoring charts that are added to the dashboards are deleted.

操作步骤

1. Log on to the CloudMonitor console.
2. Click the "Dashboard" option in the left menu to access the "Dashboard" page.
3. In the top-right corner of the page, click "Delete Current Monitoring Dashboard" button to delete the dashboard.

11.3 Add a chart

CloudMonitor initializes the ECS monitor tray for your user dimension, if you need to view it, additional data can be set by adding charts.

Note:

- Cloud monitoring will initialize the ECS monitor tray for you by default. Shows CPU usage, network inflows, network inflows, system disks BPS, system Disks Iops, network in traffic, network out traffic 7 monitoring charts.

- Limit on line chart view: 1 line chart can display up to 15 lines.
- Area map display limit: 1 area map can show up to 10 blocks of area.
- Tabular Data restrictions: displays the sorting results of up to 1000 pieces of data.
- Thermal attempt display limit: A thermal attempt shows a maximum of 1000 color blocks.

Interface parameter descriptions

- Graph type
  - Line diagram: displays monitoring data in a time series. Multiple metric items can be added.
  - Area chart: It displays metric data by time sequence. Multiple metric items can be added.
  - Topn table: real-time display of monitor data values sorted from large to small. Displays a maximum of 1000 entries in positive order or 1000 data in inverted order. For example, a table can display the CPU usage of all machines in an ECS group in a descending order. Only one monitoring item can be added.
  - Heat map: It displays the real-time data of metric items. It is used to display distribution and comparison of real-time metric data of a specific metric item of multiple instances. For example, a heat map can display the distribution of the CPU usage of multiple instances. Only one metric item can be added.
  - Pie chart: It displays the real-time data of metric items. Often used in the comparison of data . Only one monitoring item can be added.
- Cloud product monitoring: the monitoring of each cloud product in ALI cloud.
- Log monitoring: a monitor that is added by the user through log monitoring.
- Monitoring item: the name of the monitoring metric that needs to be viewed, such as CPU usage, memory usage, and so on.
- Statistical methods: the common statistical methods for monitoring items are maximum, minimum, and average. That is, how metric data is aggregated within the statistical period.
- Resources: monitoring data for which resources need to be viewed by applying grouping or instance filtering.

操作步骤

1. Log on to the *CloudMonitor console*.
2. Click **Dashboard** in the navigation pane.
3. Click on the Add chart in the upper right corner of the monitor tray To Go To The add page.
4. Select the display type for the chart.

5. Select the cloud product you want to view and name the chart.
6. Select the monitoring metrics and statistics you want to view.
   - Select the monitoring item that you want to view.
   - Select the way metric data is aggregated, for example, by maximum value, minimum value or average value.
7. If you need to add a monitor item, click Add monitor item, repeat Step 6th.
8. Click "Publish" to generate a chart in Monitor Dashboard.
9. Drag the right border, bottom border or the bottom-right corner of the chart, to resize the chart (if required).

11.4 Add business metric monitoring

Add Business Metric Monitoring function can be used when you want to upgrade from custom monitoring to business metric monitoring.

Note:

- Limit on line chart view: 1 line chart can display up to 15 lines.
- Limit on area chart view: 1 area chart may display up to 15 areas.
- Table data limit: the ordered results can be displayed for a maximum of 1,000 data entries.
- Thermal attempt display limit: A thermal attempt shows a maximum of 1000 color blocks.

Interface parameter descriptions

- Chart title: it is the title of the metric chart. It displays the name of a metric, by default.
- Metric (required): the name of metric for which data is submitted via APIs/SDKs
- Filter (optional): equivalent to the 'Where' statement in SQL. If the filtering criteria are left blank, it means all the data will be processed.
  - Line chart: this chart displays metric data by time sequence.
  - Area chart: this chart displays metric data by time sequence.
  - Heat map: this map displays the real-time metric data. It is usually used to display distribution and comparison of metric data that is grouped by dimension and aggregated.
  - Pie chart: this chart displays the real-time metric data, Often used in the comparison of data .
  - Topn table: displays the real-time metric data.

操作步骤

1. Log on to the *CloudMonitor console*.
2. Click the "Dashboard" option in the left menu to access the "Dashboard" page.
3. Click Add log monitor in the upper right corner of the monitor tray To Go To The add page.
4. Define the Chart name, Metric name and Chart type.
5. Define the Chart name, Metric name and Chart type.
6. Click "Publish" to generate a chart in Monitor Dashboard.
7. Drag the right border, bottom border or the bottom-right corner of the chart, to resize the chart (if required).

12 Application Groups

12.1 Create application groups

Scenarios

Alibaba Cloud depth users who have purchased a variety of cloud products, add resources such as the same business-related server, database, object store, cache, and so on by applying grouping capabilities into the same application grouping. Managing alarm rules in a Grouped dimension and viewing monitoring data can greatly reduce administrative complexity, improve operational efficiency.

Note:

- Add up to 1000 resource instances per grouping.
- When you create a grouping, if the initialization alarm rule is checked, cloud monitoring is based on the type of resource in your group, check if the average of 5 minutes exceeds the threshold and is notified by mail and Wangwang, the notification object is the alarm contact group that was selected when the apply grouping was created.

Operation Steps

1. Log on to the *CloudMonitor console*.
2. Select Apply grouping on the left-hand menu of the page to enter the apply grouping page.
3. Click Create group in the upper-right corner of the page to enter the Edit page.
4. Fill in the grouping name.
5. Select the product you want to add.
   - Default initialization for ECs and RDS Product, you can select the range of products for this grouping by adding a product, removing this product button
   - Select the instances that need to be grouped in the product's list of corresponding instances .
6. Select the notification object that receives the Alert Notification.
7. Select whether to initialize alarm rules for grouping.
8. Click the confirm button to save the apply grouping settings.

12.2 Managing Alarm Rules

Alarm rules feature helps you to create, view, modify, enable, disable, and delete alarm rules in the application groups.

Note:

When you request alarm rules in the application group dimension, the system displays only the alarm rules applied to the specific application group. The alarm rules applied to the instances or all resources would not be displayed.

Create an alarm rule

1. Log on to the *CloudMonitor console*.
2. Select **Application Groups** in the navigation pane.
3. Select the group for which you want to create an alarm rule, and click the group name or click **Manage** to go to the group details page.
4. Click **Create Alarm Rule** from the options available.
5. Click Confirm to complete the action.

Delete alarm rules

1. Log on to the *CloudMonitor console*.
2. Select **Application Groups** in the navigation pane.
3. Select the group for which you want to delete the alarm rule, and click the group name or click **Manage** to go to the group details page.
4. Click **Alarm Rules** from the options available to go to the alarm rules page of the group.
5. Click Delete next to the alarm rule under the **Actions** column to delete this rule. To delete multiple alarm rules at the same time, select rules to be deleted and click **Delete** from the options in the list.

Modify an alarm rule

1. Log on to the *CloudMonitor console*.
2. Select **Application Groups** in the navigation pane.
3. Select the group for which you want to create an alarm rule, and click the group name or click **Manage** to go to the group details page.
4. Click **Create Alarm Rule** from the options available.
5. Click **Modify** next to an alarm rule under the **Actions** column to modify the rule.

Enable or Disable group alarm rules

When you are required to stop a service or perform application maintenance, or an upgrade, you can disable all alarm rules of the group involved, to avoid reception of many unwanted alarm notifications due to manual changes. Once the changes are completed, you can reinstate the alarm rules.

- Disable all alarm rules of a group
  1. Log on to the *CloudMonitor console*.
  2. Click **Application Groups**in the navigation pane.
  3. Select a group name and click **More** from the **Actions** column.
  4. Select **Disable All Alarm Rules** to disable all alarm rules of the selected group.
- Enable all alarm rules of a group
  1. Log on to the *CloudMonitor console*.
  2. Click **Application Groups**in the navigation pane.
  3. Select a group name and click **More** from the **Actions** column.
  4. Select **Enable All Alarm Rules**.
- Disable partial alarm rules of a group
  1. Log on to the *CloudMonitor console*.
  2. Click **Application Groups**in the navigation pane.
  3. Select a group with an alarm, and click the group name or click **Manage** to go to the group details page.
  4. Click **Alarm Rules** from the options available.
  5. Click **Disable** next to Alarm Rules under the **Actions** column. If you want to disable multiple alarm rules collectively, select the rules and click **Disable** from the options in the list.
- Enable partial alarm rules of an application group
  1. Log on to the *CloudMonitor console*.
  2. Click **Application Groups**in the navigation pane.
  3. Select a group with an alarm, and click the group name or click **Manage** to go to the group details page.
  4. Click **Alarm Rules** from the options available.

5. Click **Enable**next to Alarm Rules under the **Actions** column. If you want to enable multiple alarm rules all at the same time, select the rules and click **Enable** from the options in the list.

12.3 Check groups

The group details page includes the fault list, alarm history, alarm rules, group resources, events, and group resource metric data.

Group list

The group list displays all the groups on the CloudMonitor. You can also view the resources and health condition of each group.

Parameters

- **`Group name`**: The name of a group.
- **`Health condition`**: The alarm status of any group resource. The group is healthy when add, modify, and no active alarms for any group resource. The group is said to be unhealthy when any of the resources has active alarms.
- **`VM count`**: VM count is the total number of servers (ECS servers and other servers) in the group.
- **`Resource count`**: The total number of resource types in the group. For example, if the group has ECS, ApsaraDB for RDS, and Server Load Balancer instances, then the total number of resource count is three.
- **`Unhealthy Count`**: The total number of instances with active alarms in the group. For example, if two ECS instances and one ApsaraDB for RDS instance have active alarms, the number of unhealthy instances is three.
- **`Creation time`**: The time when the group is created.
- **`Actions`**: Four types of operations are supported namely copy this group and create a new group, enable all the alarm rules and disable all the alarm rules, and delete groups.

Fault list

The fault list shows the resources with active alarms in your group. This allows you to quickly view all the unhealthy instances and troubleshoot faults in time.

Note:

- When multiple metrics of a resource have active alarms all at the same time, the fault list displays the resource multiple times. Each row of the list shows one metric with an active alarm.
- Once you disable the rule hit by active alarms, the resources and metrics associated with the rule disappears from the fault list.

Parameters

- Faulty resource: A resource with an active alarm.
- Start time: Time when the first alarm is generated.
- Status: Displays a message indicating that a resource has an active alarm.
- Duration: The time duration when a faulty resource is in the alarm state.
- Alarm rule name: The name of the alarm rule applied to a faulty resource.
- Actions: Click Expand to view the metric trends of a faulty resource with an active alarm for past six hours, and compare the metric data with the alarm threshold value.

Alarm history

Alarm history provides the account of all the alarm rules applied to a group.

Note:
You can request for the alarm data history of the past three days. If the interval between the query start-time and end-time exceeds three days, the system prompts you to re-select the time range.

Parameters

- **`Faulty resource`**: Resource with an active alarm.
- **`Duration`**: The time during which a faulty resource is in the alarm state.
- **`Occurrence time`**: The time when the alarm is generated.
- **`Alarm rule name`**: The name of the alarm rule applied to a faulty resource.
- **`Notification method`**: Method by which alarm notifications are sent. These notifications are sent through SMS, email, or TradeManager.
- **`Product type`**: The product type where the faulty resource belongs to.
- **`Status`**: The status of the alarm rule such as the alarm state, cleared state, and channel silence state.
- **`Notification object`**: A group of contacts who receive alarm notifications.

Alarm rules

Alarm rules display the list of all the alarm rules applied to a group. You can select the preferred alarm rule from the list and can enable, disable, and/or modify the rules as per the requirement.

Note:

The alarm rules list only displays the alarm rules applied to a specific group. It does not show the alarm rules with Resource Range set to the All Resources or an Instance.

Parameters

- Policy name: Name of an alarm rule (policy) specified when the policy is created.
- Status: Displays whether or not, the resources associated with the alarm rules have active alarms.
  - Normal state: All resources associated with the alarm rules are normal.
  - Alarm state: At least one instance associated with the alarm rule has an active alarm.
  - Insufficient data: At least one instance associated with the alarm rule has insufficient data and no instance has an active alarm.
- Enable: Enables the alarm rule.
- Product name: Name of the product which group resources belongs to.
- Policy description: A brief description of alarm rules setting.
- Actions: The optional operations include Modify, Enable, Disable, Delete, and Alarm History.
  - Modify: You can click Modify to make changes in the alarm rule.
  - Disable: Click Disable to disable the alarm rule. Once the alarm rule is disabled, the alarm service does not check whether metric data exceeds the threshold value.
  - Enable: Click Enable to enable the alarm rule. Once you enable a previously disabled alarm rule, the alarm service checks the metric data and determines whether to trigger an alarm based on the alarm rule.
  - Delete: Click Delete to delete the alarm rule.
  - Alarm History: Click to view the alarm history of the alarm rule.

Group resources

Display all the resources of a group and health condition of the resource.

Parameters

- Instance name: Instance name or ID of a resource.

- Health condition: The alarm status of any group resource. The resource is healthy if no alarm is generated according to the corresponding alarm policy. The resource is unhealthy if it has an active alarm.

Event

Currently, the alarm rule (policy) provides the alarm history and records alarm policy operation events (add, modify, and delete), allowing you to trace any operation performed on a specific alarm rule.

Note:
You can query event information over last 90 days.

Parameters

- Occurrence time: The time when any event occurs.
- Event name: The event names such as alarm generated, alarm cleared, create alarm rule, modify alarm rule, or delete alarm rule.
- Event type: Events are classified into system events and alarm events. System events include create alarm rule, delete alarm rule, and modify alarm rule. Alarm events include alarm generated and alarm cleared.
- Event details: Provide details of an event.

Metric chart

The lower section of the group details page displays the monitoring details of group resources. By default, CloudMonitor initializes frequently used metric data. If you want to display more metric data or change the chart type, modify the charts and customize metric data and/or the chart type.

Note:
To obtain the OS metrics of ECS, you must install the CloudMonitor agent.

Initialized metric data

The following group data is initialized by default. If you want to view more metric data, click Add Metric Chart to add more metrics to the data.

Product category	Metric	Chart type	Description
ECS	CPU usage and Internet outbound bandwidth	Line chart	Displays the aggregate data of all servers in the group.

Product category	Metric	Chart type	Description
ApsaraDB for RDS	CPU usage, disk usage, IOPS usage, connection usage	Line chart	Displays the data of a single database instance.
Server Load Balancer	Outbound bandwidth and inbound bandwidth	Line chart	Displays the data of a single Server Load Balancer instance.
OSS	Storage size and GET/PUT request count	Line chart	Displays the data of a single bucket.
CDN	Downstream bandwidth and hit rate	Line chart	Displays the data of a single domain name.
EIP	Internet outbound bandwidth	Line chart	Displays the data of a single instance.
ApsaraDB for Redis	Memory usage, connection usage, and QPS usage	Line chart	Displays the data of a single instance.
ApsaraDB for MongoDB	CPU usage, memory usage, IOPS usage, and connection usage	Line chart	Displays the data of a single instance.

12.4 Modify an application group

Scenarios

You need to modify the resources in your application group when your applications use more cloud products to meet the requirements of service resizing or technical architecture improvement.

You need to modify the alarm notification objects of your application group when the application O&M and development personnel is changed.

Note:

- When the application O&M and development personnel changes, you must modify the alarm rule notification contacts of your group.
- After an instance is added to a group, the instance automatically gets associated with the alarm rule configured in the group dimension. You do not need to create an alarm rule for the instance.

Procedure

1. Log on to the *CloudMonitor Console*.
2. Select **Application Groups** from the navigation pane.
3. Select a group you want to edit from the group list and go to the group details page.
4. Click **Modify Group** in the upper-right corner of the page.
5. Edit the group content.
6. Click **OK** to save the changes.

12.5 Copy a group

Scenarios

You can quickly create groups with the same alarm rules and monitor charts through the ability to copy groups. Simplifies the process of configuring grouping. Lets you avoid repeatedly configuring the same alarm rules and monitoring charts for different groups.

Procedure

1. Log on to the *CloudMonitor console*.
2. Select **Application Groups** from the left-side navigation pane.
3. Select a group to be duplicated on the group list page. That is, select **Actions** > **More** > **Copy Group**.
4. Add instances and notification contacts for the new group in a pop-up window. After this, a duplicate group with the same alarm rules and metric charts will be created.

12.6 Application groups

The application group feature of the CloudMonitor allows you to manage cloud product resources by group across products and regions and can centrally manage service-related resources. With the help of this feature, service-related resources such as servers, databases, load balance, and storage can be managed from the service perspective. You can manage alarm rules and view metric data from the service perspective and this can help to improve O&M efficiency.

Scenarios

If you have puchased multiple Alibaba Cloud products, you can use the group feature to add resources (such as servers, databases, object storage, and cache) related to the same service to the same group. You can manage alarm rules and view metric data in the group dimension. This reduces management complexities and improves cloud monitoring efficiency.

Note:

- A single cloud account can create up to 100 groups.
- Up to 1,000 resource instances can be added to one group.