Alibaba Cloud
Cloud Monitor

FAQ

Issue: 20190221

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.	 Notice: 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]*

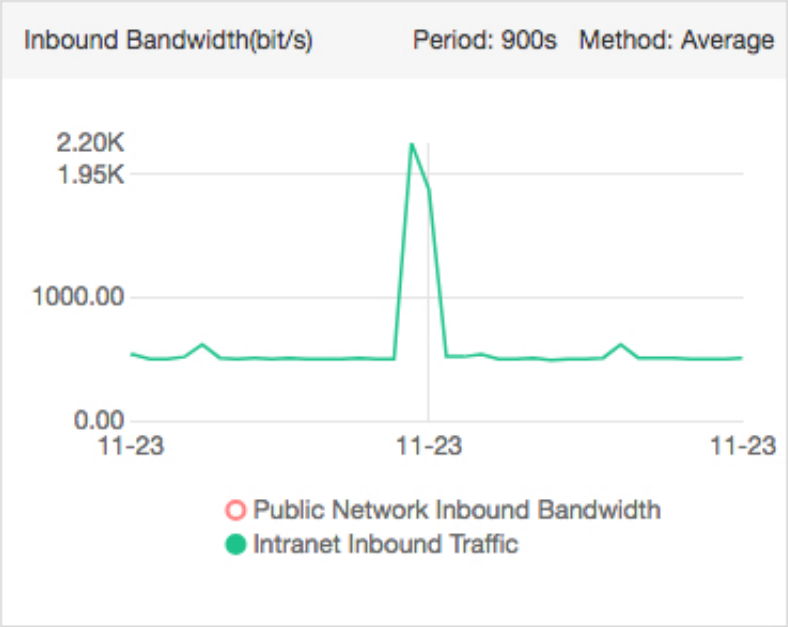
Style	Description	Example
{} or {a|b}	It indicates that it is a required value, and only one item can be selected.	`swich {stand | slave}`

Contents

1 Monitoring

1.1 Why does my inbound traffic on the intranet unexpectedly spike?

In CloudMonitor, you may encounter a sudden spike in inbound traffic over the intranet, as shown in the following figure.



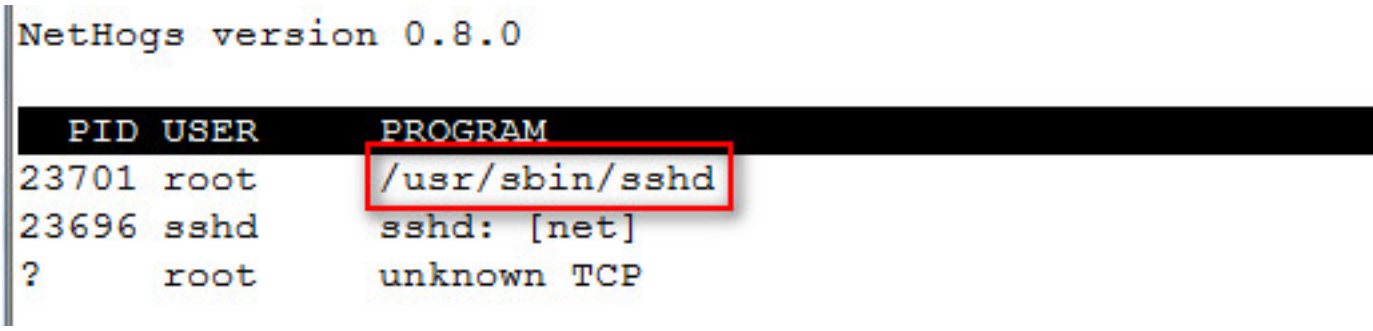
Generally, inbound traffic over the intranet tends to be relatively low, except for when SLB instances are used because SLB instances communicate with ECS instances over the intranet. Therefore, sudden spikes in intranet traffic are usually caused by ECS instances copying data over the intranet.

However, another common cause of intranet traffic spikes are virus attacks, which result in a large number of packet forwarding on the intranet. If a spike is caused by

this issue and you are running Linux OS on your instance, you can install NetHogs on the system to view the specific processes occupying traffic.

```
#yum install nethogs Install NetHogs.
```

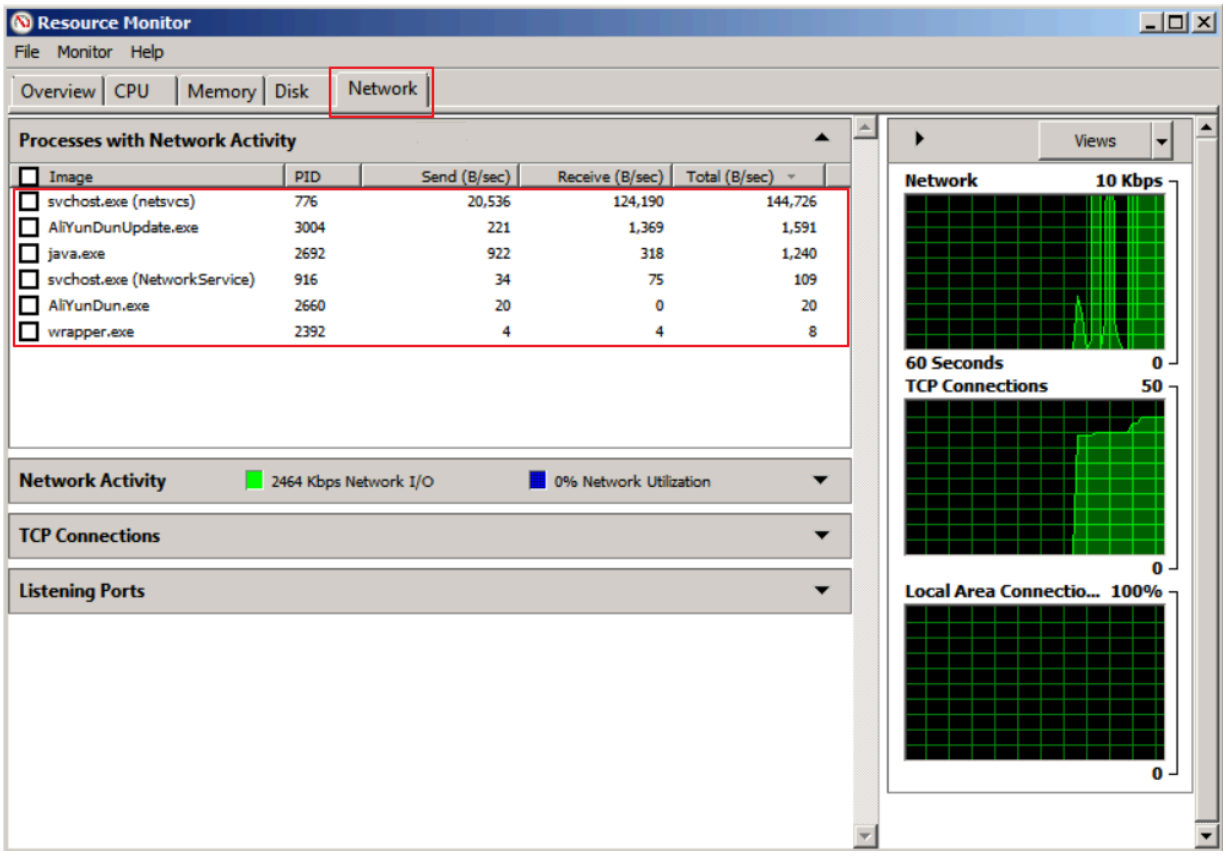
```
#nethogs eth0 View the specific traffic usage of the intranet NIC.
```



By using NetHogs, you can check intranet bandwidth usage and discover which processes are occupying the intranet bandwidth.

If you are running Windows Server 2008 or later on your instance, you can go to the Resource Monitor to see the processes that occupying the bandwidth.

Right-click on the instance's taskbar and select Start Task Manager. After that, you will see the specific processes that consume network traffic, as shown in the following figure.



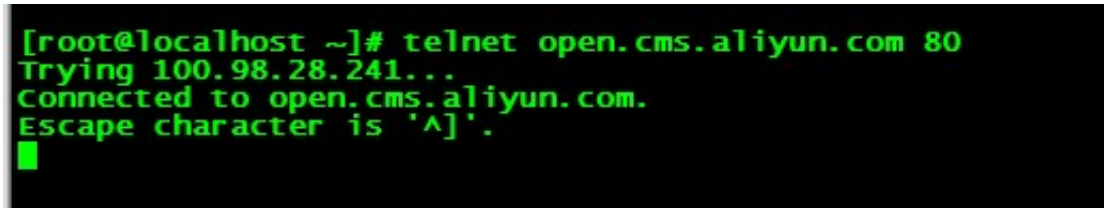
1.2 What are the custom monitoring SDKs?

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

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

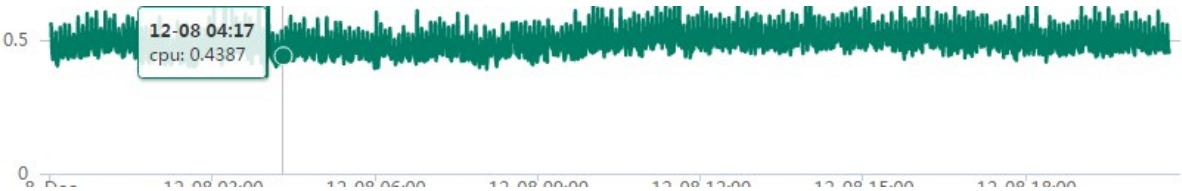
1.3 Why is CloudMonitor unavailable after the ECS intranet is disabled?

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



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

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



Instancesname/Host Name	Agent Status (All)	Agent Version	Region	IP	Network Type	CPU Usage	Memory Usage	Disk Usage	Actions
[redacted]	Running	2.1.53	China North 3 (Zhangjiakou)	[redacted]	VPC	0%	9.43%	53%	Monitoring Charts Alarm Rules
[redacted]	Running	2.1.53	China North 3 (Zhangjiakou)	[redacted]	VPC	0.17%	10.05%	32%	Monitoring Charts Alarm Rules

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

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

1.6 Why is the CPU monitoring value for my ECS Windows instances abnormal?

Internal damage to the Windows performance counter may cause the CPU monitoring value for your ECS Windows instances in the CloudMonitor to display as zero or a negative value even though actual CPU usage is a positive value and not at zero. This problem will only affect your Windows instances.

You can run the command, `typeperf \Processor(_Total)\% Processor Time`, to check whether the counter works properly. If the result is Error: no valid counter, then the counter has failed. You can run the command `lodctr /r`to fix the counter.

1.7 What should I do if a CloudMonitor agent is stopped?

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

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

The agent fails to communicate with the CloudMonitor instance

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

1. Log on to the ***CloudMonitor console***.
2. In the left-side navigation pane, select Host Monitoring.
3. Select the target host and click Install, or install the agent manually. For more information, see 云监控*Go*语言版本插件安装.

The CloudMonitor process has ended

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

1. **Check CloudMonitor logs.**
   - **Linux:** *`/usr/local/cloudmonitor/logs`*
   - **Windows:** *`C:/Program Files/Alibaba/cloudmonitor/logs`*
2. **Check the agent running status.**
   - **Linux:**

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

   - **Windows:**

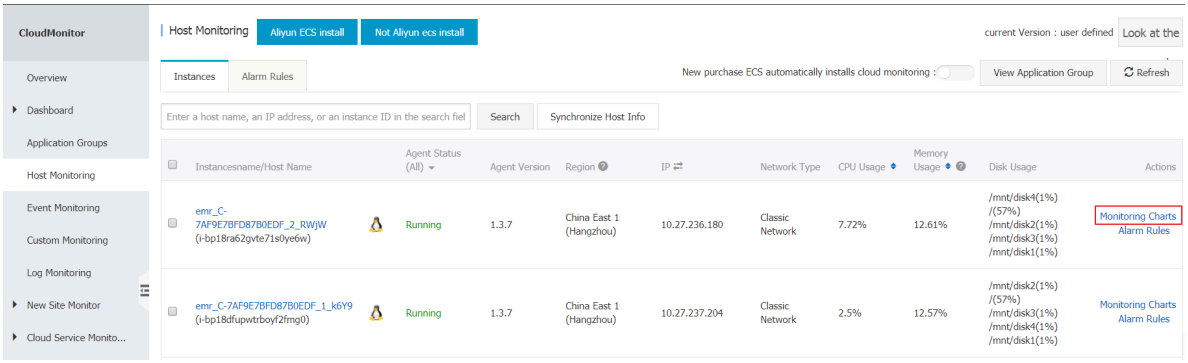
     ```
     C:\"Program Files (x86)"\Alibaba\cloudmonitor\wrapper\bin\
     AppCommand.bat status
     ```

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

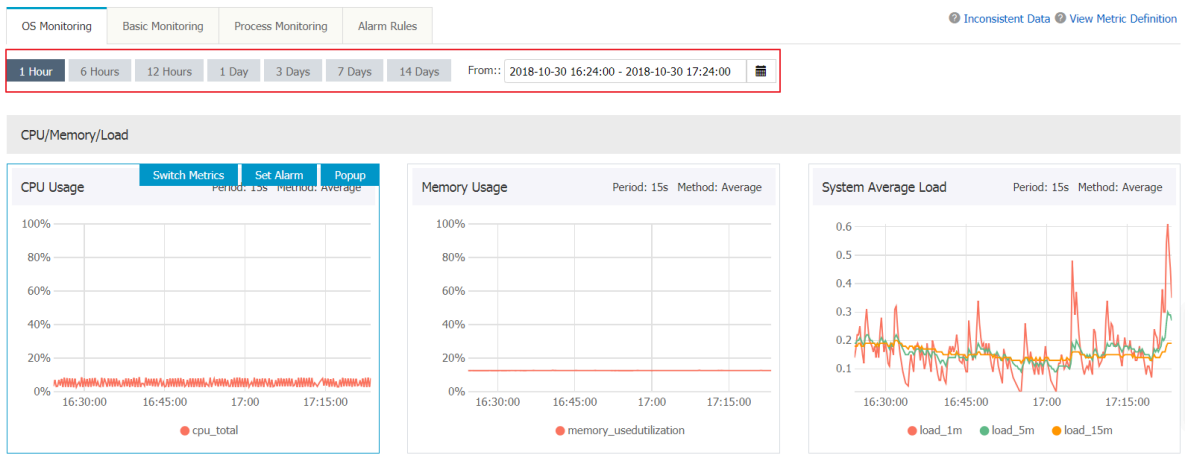
2 Operation

2.1 How do I view the monitoring data of a specified date in the CloudMonitor console?

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



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



Note:

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

2.2 What is the inode usage metric in CloudMonitor for?

Linux and Unix systems use inode numbers, instead of file names, to identify files. In other words, files names are simply aliases of inode numbers used for the convenienc

e of identification. When you open a file, the process involved in the system is as follows:

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

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

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

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

2.3 How has event monitoring been upgraded?

Upgrades

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

Upgrade details

1. Event alarms have now migrated to the Event Monitoring page of the console. Originally, event alarms were set on the Create Alarm Rule page. This change has the effect that you can no longer create the following event alarms by using alarm templates: CloudMonitor agent no heartbeat alarms; RDS, Redis, and Memcache faults; RDS, Redis, and Memcache master/slave switchover alarms; MongoDB and Container Service status and node exception alarms; RDS and Redis synchroniz ation exception alarms for disaster recovery.
2. Application groups support event alarm subscription notifications. When you create an application group, you can enable this function. After you enable this

feature, you will receive notifications for critical-level and warning-level events for the resources in your application group.

3. This upgrade does not affect any existing event alarm rules. However, you cannot modify these rules after upgrading. To make modifications, you need to create new alarm rules in the event monitoring console.

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

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