ALIBABA CLOUD

Alibaba Cloud

CloudMonitor

FAQ

Document Version: 20220428

Alibaba Cloud

Legal disclaimer

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

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

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

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

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

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

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

Document conventions

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

Table of Contents

1.Operations

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

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

Procedure

1. Prepare an Alibaba Cloud AccessKey pair.

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

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

2. Generate a signature string for an HTTP request.

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

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

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

Parameter	Description	Example
VERB	The HTTP method used to make the request.	PUT, GET, or POST
CONTENT-MD5	The MD5 value of the Body field in the HTTP request. **Note** The MD5 value must be a string consisting of uppercase letters and digits.	0B9BE351E56C90FED853B32524253E8B

Parameter	Description	Example
CONTENT-TYPE	The type of the HTTP request body.	application/json
DATE	The standard timestamp header of the HTTP request. **Note** This timestamp header follows the RFC 1123 time format and uses the GMT standard time.	Mon, 3 Jan 2010 08:33:47 GMT
CanonicalizedHeaders	The string constructed from the custom headers that are prefixed with `x-cms` and `x-acs` in the HTTP request.	○ x-cms-api-version:0.1.0 ○ x-cms-signature
CanonicalizedResource	The string constructed from the resources requested by the HTTP request.	/event/custom/upload

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

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

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

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

3. Generate a digital signature for the HTTP request.

Formula for generating a digital signature:

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

Sample signature string of an HTTP request:

```
SignString="POST" + "\n"
+"0B9BE351E56C90FED853B32524253E8B" + "\n"
+"application/json" + "\n"
+"Tue, 11 Dec 2018 21:05:51 +0800" + "\n"
+"x-cms-api-version:1.0" + "\n"
+"x-cms-ip:127.0.0.1" + "\n"
+"x-cms-signature:hmac-sha1" + "\n"
+"/metric/custom/upload"
accesskey="testkey"
accessSecret="testsecret" // The AccessKey secret used to sign the HTTP request.
```

Signature generated based on the preceding signature string:

```
1DC19ED63F755ACDE203614C8A1157EB1097E922
```

1.2. How do I use pssh to install the Cloud Monitor agent on multiple hosts at a time?

This topic describes how to use pssh to install the Cloud Monitor agent on multiple hosts at a time.

Introduction to pssh

pssh is a tool that allows you to perform operations on multiple hosts at the same time. pssh is written in Python and is suitable for performing repetitive operations on no more than 30 hosts at the same time. For example, you can use pssh to install software, stop a process, or download a file on multiple hosts at the same time.

Install the Cloud Monitor agent on a single host

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

Install the Cloud Monitor agent on multiple hosts at the same time by using pssh

- **Install pssh**
  i. Install Python 2.4 or a later version.
  ii. Install pssh.

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

- **Add the IP addresses and ports of the hosts where you want to install the Cloud Monitor agent to the ip.txt file**

i. Open the ip.txt file.

ii. Add the IP addresses and ports of the hosts to the ip.txt file in the format of user@ip:port. Each host occupies a row. The default port 22 is used if you do not specify the port for a host.

iii. Make sure that the user that you specify for a host in the ip.txt file has the sudo permissions on the host.

iv. Make sure that the same password is configured on the hosts. Alternatively, you can configure mutual trust between the host where you run the pssh tool and the hosts where you want to install the Cloud Monitor agent to allow password-free logons.

- **Run the pssh tool to install the Cloud Monitor agent on the specified hosts at the same time**

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

-h: the file that contains the IP addresses and ports of the hosts where you want to install the Cloud Monitor agent.

-A: the password used to log on to the hosts. You do not need to specify this parameter if you have configured mutual trust between the host where you run the pssh tool and the hosts where you want to install the Cloud Monitor agent.

-i: the command used to install the Cloud Monitor agent.

- **Check whether the Cloud Monitor agent is installed on the hosts**

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

1.3. Why is an error reported when I add a process to be monitored in Cloud Monitor?

This topic describes why an error is reported when you add a process to be monitored in Cloud Monitor.

Problem description: Cloud Monitor displays the **Add Task Error: add error** message when you add a process to be monitored in Cloud Monitor.

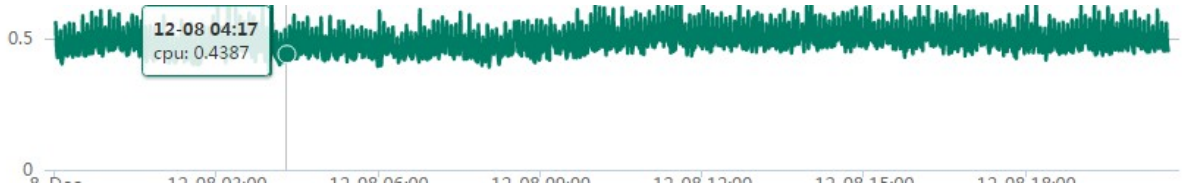
Cause: Server Guard is not installed on the server where the process resides.

Solution: Install Server Guard on the server.

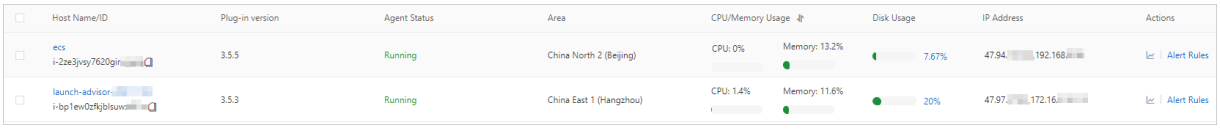
1.4. Why is the CPU utilization displayed as 0% in the Cloud Monitor console?

This topic describes why the CPU utilization is displayed as 0% in the Cloud Monitor console.

This issue is caused by low CPU utilization. The CPU utilization is around 0.5%, as shown in the following figure.



An Elastic Compute Service (ECS) instance reports the CPU utilization to Cloud Monitor once a minute. Cloud Monitor displays the average CPU utilization in the last five minutes in the console. If the average CPU utilization in the last five minutes is less than 0.5%, Cloud Monitor displays the CPU utilization as 0%.

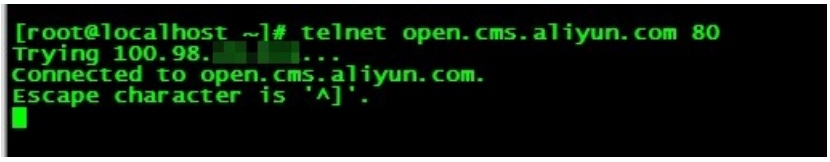


1.5. Why does Cloud Monitor fail to monitor my ECS instance after I disable the internal network access for the instance?

This topic describes why Cloud Monitor fails to monitor an ECS instance after you disable access to the internal network for the ECS instance.

If you want to use Cloud Monitor to monitor an ECS instance, make sure that the ECS instance can access the internal network of Alibaba Cloud.

An ECS instance communicates with Cloud Monitor by using the domain name open.cms.aliyun.com. This domain name can be resolved only on the internal network. Cloud Monitor collects monitoring data from an ECS instance by using the internal network. To allow Cloud Monitor to collect monitoring data from an ECS instance, make sure that the ECS instance can communicate with open.cms.aliyun.com by using port 80.



1.6. What does status code 610 mean?

This topic describes the meaning of status code 610 returned by Cloud Monitor.

Status code 610 indicates an HTTP connection timeout.

Cloud Monitor monitors the status of your site by sending HTTP requests to the site. After Cloud Monitor sends an HTTP request, Cloud Monitor determines that a connection timeout occurs if no response is received within 5 seconds. In this case, Cloud Monitor returns status code 610.

We recommend that you take measures, for example, increase the number of retry times and configure alerts based on combined conditions, to improve the alert accuracy.

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

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

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

2.Troubleshooting

2.1. How do I troubleshoot an abnormal stop of the Cloud Monitor agent?

This topic describes how to troubleshoot an abnormal stop of the Cloud Monitor agent.

Context

By default, the Cloud Monitor agent sends a heartbeat message to the Cloud Monitor server every 3 minutes. If the Cloud Monitor agent does not send heartbeat messages for 15 minutes, the host where the agent resides determines that the agent stops.

The Cloud Monitor agent may automatically stop due to the following causes:

- The Cloud Monitor agent cannot communicate with the Cloud Monitor server.
- The process of the Cloud Monitor agent exits.

Solution for the failure to communicate with the Cloud Monitor server

If the Cloud Monitor agent runs normally before it stops, you can reinstall the agent and start it again.

- Automatically install the Cloud Monitor agent

  For more information, see Automatically install the CloudMonitor agent for C++ (recommended).

- Manually install the Cloud Monitor agent

  For more information, see Manually install the CloudMonitor agent for C++ on an ECS instance or Manually install the CloudMonitor agent for C++ on a host that is not provided by Alibaba Cloud.

Solution for the exit of the agent process

You can view the status and logs of the Cloud Monitor agent to determine the cause of the exit. If the process of the Cloud Monitor agent exits, it may be caused by a bug of the Cloud Monitor agent. We recommend that you submit a ticket and do not perform troubleshooting until Alibaba Cloud engineers contact you.

- View logs of the Cloud Monitor agent
  - Windows

    a.

    b. Go to the *C:\Program Files\Alibaba\cloudmonitor\local_data\logs* directory that stores the logs of the Cloud Monitor agent.

    c. Open the log file *argusagent.log* or *argusagentd.log* in Notepad or WordPad.

    - *argusagentd.log*: stores the logs generated by the C++ agent about daemon processes. The logs contain information such as the startup and shutdown of monitoring processes.
    - *argusagent.log*: stores the operational logs of the C++ agent.

- Linux
  a. Log on to the host where the Cloud Monitor agent resides as the root user.
  b. Run the following commands to view the logs of the Cloud Monitor agent:

     cd /usr/local/cloudmonitor/local_data/logs

     cat argusagent.log

     cat argusagentd.log

     - *argusagentd.log*: stores the logs generated by the C++ agent about daemon processes. The logs contain information such as the startup and shutdown of monitoring processes.
     - *argusagent.log*: stores the operational logs of the C++ agent.

- View the status of the Cloud Monitor agent
  - Windows
    a. Log on to the host where the Cloud Monitor agent resides as the administrator.
    b. Open the **Services** window.

       Press *Win+R*. In the **Run** dialog box, enter **services.msc** and click **OK**.

    c. View the status of the **argusagent** service.
  - Linux
    a. Log on to the host where the Cloud Monitor agent resides as the root user.
    b. Run the following command to view the status of the Cloud Monitor agent:

       ps aux | grep argusagent | grep -v grep

2.2. How can I restart the CloudMonitor agent for C++?

After you install or configure the CloudMonitor agent, you must restart it to apply the configuration. This topic describes how to restart the CloudMonitor agent for C++ in Windows and Linux.

Windows

1. Use an administrator account to log on to the server on which the CloudMonitor agent resides.
2. Go to the *C:\Program Files\Alibaba\cloudmonitor* directory in which the CloudMonitor agent resides.
3. Double-click *stop.bat* to stop the CloudMonitor agent.
4. Double-click *start.bat* to start the CloudMonitor agent.

Linux

1. Use the root account to log on to the server on which the CloudMonitor agent resides.
2. Run the following command to go to the directory of the CloudMonitor agent:

   cd /usr/local/cloudmonitor
3. Run the following command to restart the CloudMonitor agent:

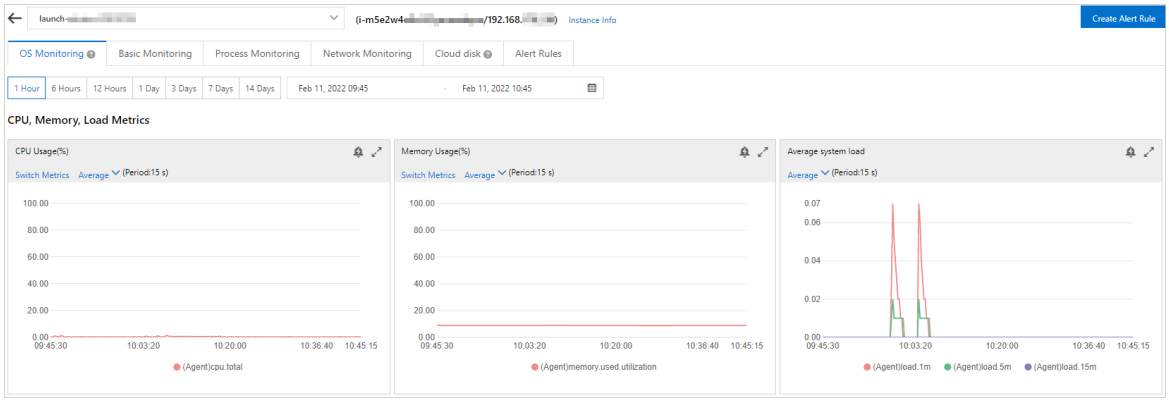
   ./cloudmonitorCtl.sh restart

2.3. How do I view the monitoring data within a specific period of time in the CloudMonitor console?

This topic describes how to view the monitoring data within a specific period of time in the CloudMonitor console.

Procedure

1.
2. In the left-side navigation pane, click **Host Monitoring**.
3. On the **Host Monitoring** page, find the host that you want to manage and click the icon in the **Actions** column.
4. Specify a period of time to view the monitoring data.



> **Note** You can view only the monitoring data of the last 30 days in the CloudMonitor console.

2.4. How do I report the monitoring data of hosts that are not provided by Alibaba Cloud to CloudMonitor by using an NGINX proxy server?

This topic describes how to report the monitoring data of hosts that are not provided by Alibaba Cloud to CloudMonitor by using an NGINX proxy server.

Step 1: Deploy an NGINX proxy server

> **Note** We recommend that you use a Linux server as your proxy server because CloudMonitor is deployed on a Linux server. In this example, a Linux server that runs CentOS is used.

1. Download the latest installation package of NGINX, for example, **nginx-1.19.6**.
   i. Go to the nginx: download page.
   ii. Click **nginx-1.19.6** to download the *nginx-1.19.6.tar.gz* package.
2. Download NGINX patch packages to the specified directory of the proxy server, for example, */opt*.

   > **Note** In this example, the *proxy_connect_1014.patch* patch package is installed.

   i. Log on to the proxy server as the root user.
   ii. Run the following commands to download NGINX patch packages:

   cd /opt

   yum install -y git

   git clone https://github.com/chobits/ngx_http_proxy_connect_module.git

   The following figure shows the downloaded patch packages.

```
proxy_connect.patch                    proxy_connect_rewrite_1015.patch
proxy_connect_1014.patch               proxy_connect_rewrite_101504.patch
proxy_connect_rewrite.patch            proxy_connect_rewrite_1018.patch
proxy_connect_rewrite_1014.patch
```

3. Run the following commands to install the sample NGINX patch package.

   yum install -y patch pcre pcre-devel

   patch -p1 < ngx_http_proxy_connect_module/patch/proxy_connect_1014.patch

4. Install NGINX.
   i. Upload the *nginx-1.19.6.tar.gz* package to the specified directory of the proxy server, for example, */usr/local*.
   ii. Log on to the proxy server as the root user.
   iii. Run the following commands to decompress the *nginx-1.19.6.tar.gz* package to the *nginx-1.19.6* directory:

   cd /usr/local

   tar zxvf nginx-1.19.6.tar.gz

   iv. Run the following commands to initialize NGINX:

   cd nginx-1.19.6

   ./configure --prefix=/usr/local/nginx-1.19.6 --with-http_stub_status_module --with-http_ssl_module --add-module=ngx_http_proxy_connect_module

   v. Run the following commands to install NGINX:

   make install

   make && make install

   vi. Run the following command to start NGINX:

   ./nginx

vii. Check whether NGINX is installed.

In the address bar of your browser, enter *IP address of the proxy server:80*. If the following output is displayed, the installation is successful.

5. Configure an NGINX proxy.

i. Run the following commands to create a directory named *conf.d*:

```
cd /usr/local/nginx-1.19.6/conf
mkdir conf.d
```

ii. Run the following commands to create a file named *forward.conf* in the *conf.d* directory.

```
cd conf.d
vi nginx.conf
```

iii. Configure a forward proxy or a reverse proxy in the *forward.conf* file.

- Forward proxy

  If you consider the Internet outside the LAN as a huge resource pool, the clients in the LAN need to access the Internet by using a forward proxy.

  Copy the following code to the *forward.conf* file. Set the `resolver` parameter to the IP address of the proxy server and do not change the default values of other parameters.

```
server {
     listen                          80;
     # dns resolver used by forward proxying
     resolver                        192.168.XX.XX;  # The IP address of the proxy
server.
     # forward proxy for CONNECT request
     proxy_connect;
     proxy_connect_allow             443;
     proxy_connect_connect_timeout   10s;
     proxy_connect_read_timeout      10s;
     proxy_connect_send_timeout      10s;
     # forward proxy for non-CONNECT request
     location / {
         proxy_pass http://$http_host$request_uri  # The protocol and request URI
of the proxy server. Do not change the default values.
         proxy_set_header Host $host;
     }
 }
```

  Note The forward proxy of NGINX does not support HTTPS.

- Reverse proxy

  If the LAN provides resources and services to the Internet, the clients on the Internet need to access resources in the LAN by using a reverse proxy.

  Copy the following code to the *forward.conf* file. Set the `server_name` parameter to the IP address of the proxy server. Set the `proxy_pass` parameter to the URL that the proxy server accesses. Set the `ssl_certificate` parameter to the Secure Sockets Layer (SSL) certificate. Set the `ssl_certificate_key` parameter to the key of the SSL certificate. Do not change the default values of other parameters.

```
server {
    listen              443 ssl;
    server_name         192.168.XX.XX; # The IP address of the proxy server.
    ssl_certificate     XXXX.pem; # The SSL certificate.
    ssl_certificate_key XXXX.key; # The key of the SSL certificate.
    location / {
        proxy_pass  https://www.aliyun.com; # The URL that the proxy server acces
ses.
        proxy_set_header Host $host;
        proxy_set_header X-Real-IP $remote_addr;
        proxy_set_header REMOTE-HOST $remote_addr;
        proxy_set_header X-Forward`ed-For $proxy_add_x_forwarded_for;
        }
}
```

  Note For more information about how to apply for an SSL certificate, see Apply for a certificate.

iv. Press the Esc key, enter *:wq*, and then press the Enter key to save and close the *forward.conf* file.

v. Run the following commands to open the *nginx.conf* file:

  cd ..

  vi nginx.conf

vi. Edit the *nginx.conf* file.

  Copy the following code to the *nginx.conf* file and set the `include` parameter to the path to the *forward.conf* file.

```
http {
.....
include /usr/local/nginx-1.19.6/conf/conf.d/forward.conf;
.....
}
```

vii. Press the Esc key, enter *:wq*, and then press the Enter key to save and close the *nginx.conf* file.

viii. Run the following command to restart the NGINX proxy server:

  nginx -s reload

ix. Check whether the NGINX proxy is configured.

- Forward proxy

  Run the following command to access a URL. If the URL can be accessed, the NGINX proxy is configured.

  curl -x *192.168.XX.XX (IP address of the proxy server)http://example.aliyundoc.com (Any URL)*

- Reverse proxy

  Run the following command. If you can access only the URL specified in the *nginx.conf* file, the NGINX proxy is configured.

  curl -x *192.168.XX.XX (IP address of the proxy server)https://example.aliyundoc.com (Any URL)*

Step 2: Install and configure the CloudMonitor agent

1. Install the CloudMonitor agent on a host that is not provided by Alibaba Cloud.

   For more information, see Install and uninstall the CloudMonitor agent for C++.

2. Configure the NGINX proxy server in the CloudMonitor agent.

   i. Log on to the host where the CloudMonitor agent resides as the root user.

   ii. Run the following commands to open the *agent.properties* file.

   cd /usr/local/cloudmonitor/conf

   vi agent.properties

   iii. Configure the NGINX proxy server in the configuration file of the CloudMonitor agent.

   The following code provides an example on how to configure an NGINX proxy server:

```
http.proxy.auto=false
# Manually configure the proxy server
http.proxy.host=192.168.XX.XX  # The IP address of the NGINX proxy server.
http.proxy.port=8080  # The port of the NGINX proxy server.
#http.proxy.user=user  # The NGINX proxy server does not require a username for HTTP authentication.
#http.proxy.password=password  # The NGINX proxy server does not require a password for HTTP authentication.
```

   iv. Press the Esc key, enter *:wq*, and then press the Enter key to save and close the *agent.properties* file.

   v. Run the following command to restart the CloudMonitor agent:

   ./cloudmonitorCtl.sh restart

Step 3: View the monitoring data of the host not provided by Alibaba Cloud

1.
2. In the left-side navigation pane, click **Host Monitoring**.
3. On the **Host Monitoring** page, click the host name or click the icon in the **Actions** column of the host.

View the monitoring data of the host not provided by Alibaba Cloud.

2.5. How do I uninstall the CloudMonitor agent?

This topic describes how to uninstall the CloudMonitor agent for Java, Go, or C++.

Windows

1. Log on to the host where the CloudMonitor agent resides as the administrator.
2. Create a *.ps1* file, such as the test.ps1 file.
3. Copy the following content to the *test.ps1* file:

```
if([System.Environment]::Is64BitOperatingSystem -eq $true)
{
    $CMS_ARCH="amd64"
    $ARGUS_ARCH="win64"
}else
{
    $CMS_ARCH="386"
    $ARGUS_ARCH="win32"
}
$dest_path_prefix="C:\Program Files\Alibaba"
$dest_path="$dest_path_prefix\cloudmonitor"
echo "the current arch is $CMS_ARCH"
$go_dest_file="CmsGoAgent.windows-$CMS_ARCH.exe"
$argus_dest_file="cloudmonitor_$ARGUS_ARCH.zip"
$downloadpath="Argus/$CMS_VERSION/$argus_dest_file"
if (Test-Path "$dest_path\wrapper\bin\AppCommand.bat")
{
   echo "old java cloudmonitor already installed - remove it..."
   & "$dest_path\wrapper\bin\AppCommand.bat" remove
   rm -Force -Recurse "$dest_path"
}
if (Test-Path "C:\Program Files (x86)\Alibaba\cloudmonitor\wrapper\bin\AppCommand.bat"
)
{
    echo "old java cloudmonitor already installed - remove it..."
    & "C:\Program Files (x86)\Alibaba\cloudmonitor\wrapper\bin\AppCommand.bat" remove
    rm -Force -Recurse "C:\Program Files (x86)\Alibaba\cloudmonitor"
}
if (Test-Path "$dest_path\$go_dest_file")
{
    "echo remove go-agent"
    & "$dest_path\$go_dest_file" stop
    & "$dest_path\$go_dest_file" uninstall
}
```

4. Save and close the *test.ps1* file.
5. Right-click the *test.ps1* file and select **Run with PowerShell**.

Linux

1. Log on to the host where the CloudMonitor agent resides as the root user.
2. Create a script file. For example, run the following command to create the test.sh file:

   touch test.sh
3. Run the following command to open the *test.sh* file:

   vi test.sh
4. Copy the following content to the *test.sh* file:

```
#!/bin/bash
if [ -z "${CMS_HOME}" ]; then
  CMS_HOME_PREFIX="/usr/local"
  if [ -f /etc/os-release -a ! -z "`egrep -i coreos /etc/os-release`" ];then
    CMS_HOME_PREFIX="/opt"
  fi
fi
CMS_HOME="${CMS_HOME_PREFIX}/cloudmonitor"
if [ `uname -m` = "x86_64" ]; then
    ARCH="amd64"
    ARGUS_ARCH="64"
else
    ARCH="386"
    ARGUS_ARCH="32"
fi
case `uname -s` in
  Linux)
    CMS_OS="linux"
    ;;
  *)
    echo "Unsupported OS: $(uname -s)"
    exit 1
    ;;
esac
DEST_START_FILE=${CMS_HOME}/cloudmonitorCtl.sh
# Uninstall the CloudMonitor agent for Java or Go.
GOAGENT_ELF_NAME=${CMS_HOME}/CmsGoAgent.${CMS_OS}-${ARCH}
if [ -d ${CMS_HOME} ] ; then
  if [ -f ${DEST_START_FILE} ];then
    ${DEST_START_FILE} stop
  fi
  if [ -f ${CMS_HOME}/wrapper/bin/cloudmonitor.sh ] ; then
    ${CMS_HOME}/wrapper/bin/cloudmonitor.sh remove;
    rm -rf ${CMS_HOME};
  fi
  if [ -f ${GOAGENT_ELF_NAME} ]; then
    ${GOAGENT_ELF_NAME} stop
    rm -rf ${CMS_HOME}
  fi
fi
```

5. Press the Esc key, enter *:wq*, and then press the Enter key to save and close the *test.sh* file.
6. Run the following command to run the *test.sh* file:

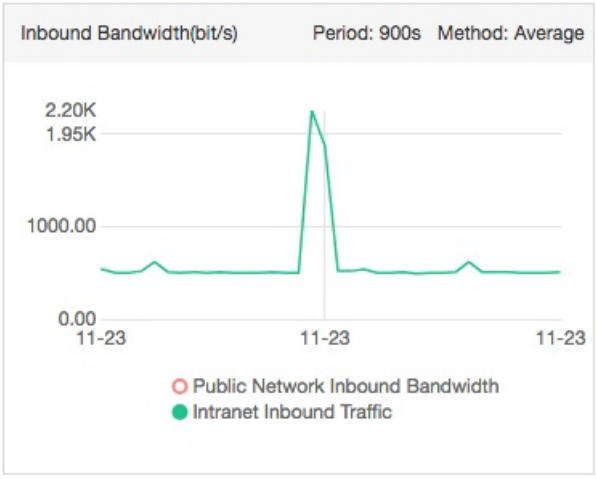
```
sh test.sh
```

2.6. How do I resolve the issue of unexpectedly high traffic over the internal network for ECS instances?

This topic describes how to resolve the issue of unexpectedly high traffic over the internal network for Elastic Compute Service (ECS) instances.

Problem description

On the **Host Monitoring** page of Cloud Monitor console, the inbound traffic over the internal network is unexpectedly high for an ECS instance, as shown in the following figure.



Cause

An ECS instance uses a public network interface controller (NIC) to provide services and uses the internal network only in a few cases. The traffic over the internal network is high for the current ECS instance when other ECS instances transmit large amounts of data to the ECS instance.

> **Note** The traffic over the internal network is high for the backend ECS instances of a Server Load Balancer (SLB) instance. This is because the SLB instance communicates with the backend ECS instances by using the internal network.

If no ECS instances transmit data to the ECS instance but the traffic over the internal network is high, the ECS instance may be infected with viruses, which cause the ECS instance to forward a large number of packets. For more information about how to resolve the issue in this case, see Solution.

Solution

This section describes the solution for ECS instances that run the Linux and Windows operating systems.

- Linux

> **Note** The NetHogs tool is an open source command line interface (CLI), which is similar to the top command in the Linux operating system. The NetHogs tool is used to analyze the real-time bandwidth usage of processes or applications.

i. Download the NetHogs tool.

ii. Run the following command to install the NetHogs tool:

yum install nethogs

iii. Run the following command to view the internal bandwidth usage of each process:

nethogs *eth0*

- Windows

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

i. On the ECS instance, right-click the taskbar and select **Task Manager**.

ii. On the **Process** tab of the **Task Manager** dialog box, view the internal bandwidth usage of processes.

2.7. How do I troubleshoot the automatic installation failure of the CloudMonitor agent on an Alibaba Cloud instance?

This topic describes how to resolve the issue in which the CloudMonitor agent fails to be automatically installed on an Alibaba Cloud Elastic Compute Service (ECS) instance.

Procedure

1. Log on to the ECS instance where the CloudMonitor agent fails to be installed as the root user.
2. Run the following command to check whether the region ID of the ECS instance can be obtained:

   curl http://100.100.100.200/latest/meta-data/region-id

   - Yes: Go to .
   - No: Manually install the CloudMonitor agent on the ECS instance. For more information, see Manually install the CloudMonitor agent for C++ on an ECS instance.
3. Run the following command to check whether the ECS instance can access Object Storage Service (OSS) over the network:

   ping cms-agent-${region-id}.oss-${region-id}.aliyuncs.com

In the command, replace `{region-id}` with the region ID of the ECS instance. For example, if the region ID is `cn-shenzhen`, run the **ping cms-agent-cn-shenzhen.oss-cn-shenzhen.aliyuncs.com** command.

- Yes: The network is normal. CloudMonitor may cause the issue. Contact CloudMonitor technical support by submitting a ticket.
- No: The network is abnormal. OSS may cause the issue. Contact OSS technical support by submitting a ticket.

2.8. What can I do if a site monitoring task expires?

This topic describes how to handle a site monitoring task after it expires.

CloudMonitor provides a free quota of 10 site monitoring tasks. The validity period of the free site monitoring tasks is 30 days. After your site monitoring task expires, you can delete the expired site monitoring task and create another site monitoring task. The validity period of the new site monitoring task is still 30 days. For more information, see Delete one or more site monitoring tasks and 创建站点监控任务.

2.9. How do I troubleshoot the heartbeat check failure that is reported by the CloudMonitor agent?

The CloudMonitor agent reports an error message that indicates a failed heartbeat check if a host failure, a network exception, or the downtime of the agent occurs. In this topic, an Elastic Compute Service (ECS) instance is used as an example to describe how to troubleshoot a failed heartbeat check.

Procedure

1. Check whether the ECS instance runs as expected. For more information, see View instance information.
   - If the ECS instance runs as expected, perform .
   - If the ECS instance does not run as expected, start or restart the ECS instance. For more information, see Start an instance or Restart an instance.

     > **Note** If you still receive this error message after you start o restart the ECS instance, read the related topics of ECS to check the cause. For more information, see Instance FAQ.

2. Check whether the CloudMonitor agent that is installed on the ECS instance runs as expected. For more information, see Install and uninstall the CloudMonitor agent for C++.
   - If the CloudMonitor agent runs as expected, perform .
   - If the CloudMonitor agent does not run as expected, restart the CloudMonitor agent. For more information, see How can I restart the CloudMonitor agent for C++?.
3. Ping the IP address that is used by CloudMonitor to receive heartbeat data on the ECS instance and check whether the network connection to the ECS instance is available.

For more information about how to obtain the IP address that is used by CloudMonitor to receive heartbeat data, see Configure the network.

- If the network connection is available, perform .
- If the network connection is not available, configure the network of the ECS instance. For more information, see Configure the network.

4. Collect logs that are stored in the */usr/local/cloudmonitor/local_data/logs* directory of the CloudMonitor agent and submit a ticket.

2.10. What can I do if CloudMonitor fails to identify multiple hosts that are deployed by using the same image?

If you use an image to deploy a host, a serial number is automatically generated for the host after the CloudMonitor plug-in is installed. If you use the same image to deploy multiple third-party hosts, CloudMonitor may fail to identify the hosts.

To resolve the issue, perform one of the following system-specific operations:

- Windows

  Delete the key-value pair *serial_number* in the *Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\cloudmonitor* directory of the registry.

- Linux

  Delete the *serial_number.properties* file in the */etc/cloudmonitor* directory.