Tencent Cloud Observability Platform

Troubleshooting

Product Documentation

©2013-2022 Tencent Cloud. All rights reserved.

Copyright Notice

©2013-2024 Tencent Cloud. All rights reserved.

Copyright in this document is exclusively owned by Tencent Cloud. You must not reproduce, modify, copy or distribute in any way, in whole or in part, the contents of this document without Tencent Cloud's the prior written consent.

Trademark Notice

Tencent Cloud

All trademarks associated with Tencent Cloud and its services are owned by Tencent Cloud Computing (Beijing) Company Limited and its affiliated companies. Trademarks of third parties referred to in this document are owned by their respective proprietors.

Service Statement

This document is intended to provide users with general information about Tencent Cloud's products and services only and does not form part of Tencent Cloud's terms and conditions. Tencent Cloud's products or services are subject to change. Specific products and services and the standards applicable to them are exclusively provided for in Tencent Cloud's applicable terms and conditions.

Contents

Troubleshooting
- CVM CPU/Memory Usage Is Too High
- CVM Login Failure
- CVM Bandwidth Utilization Is Too High
- CVM Has No Monitoring Data
- No Alarm Is Received

©2013-2022 Tencent Cloud. All rights reserved.

Troubleshooting
CVM CPU/Memory Usage Is Too High

Last updated：2024-01-27 17:35:59

Overview

This document describes how to troubleshoot and solve the problem of not being able to log in to Windows and Linux CVM instances due to the instances' overly high CPU or memory usage.

Troubleshooting Approaches

1. Log in to the instance and identify the process that is causing high CPU or memory usage.
2. Analyze the process.
If the process has an exception, the exception may be caused by a virus or a trojan. In this case, terminate the process or use an antivirus application to scan your system.
If the process is a service process, check whether the high CPU or memory usage is caused by an access volume change and whether it can be optimized.
If the process is a Tencent Cloud component process, submit a ticket and we will help you locate and troubleshoot the problem.

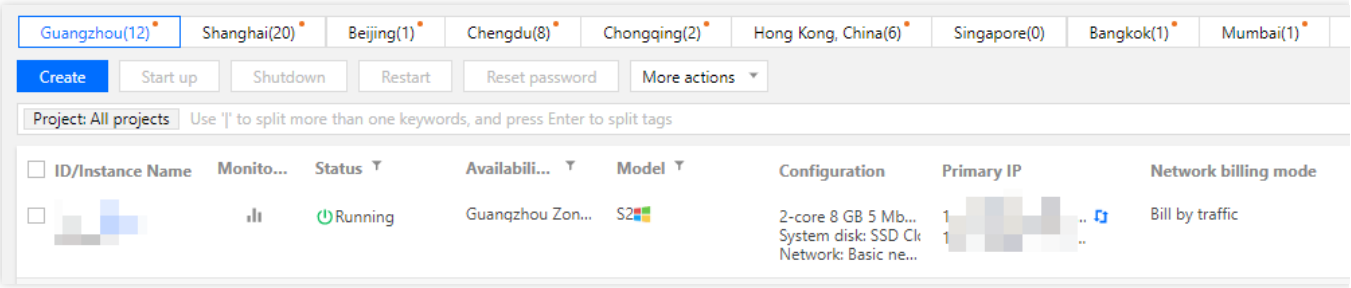
Locating and Troubleshooting the Problem

Windows CVM instances

Logging in to a CVM instance via VNC

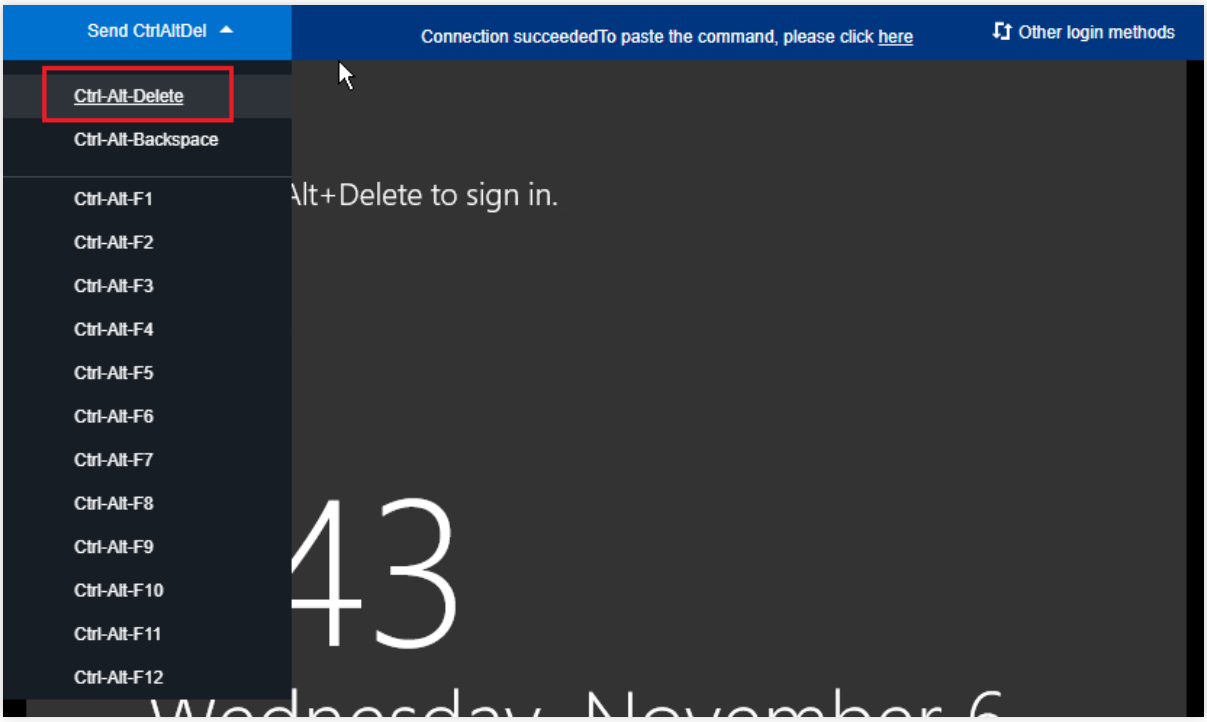
Note:
If you cannot establish a remote connection with your CVM instance due to high CPU or memory load, see Logging in to a Windows Instance via VNC.
1. Log in to the CVM Console.
2. On the instance management page, locate the target CVM instance and click **Log In**, as shown in the following figure:

©2013-2022 Tencent Cloud. All rights reserved.



3. On the **Log in to Windows instance** page that appears, click **Log In Now** under **Alternative login methods (VNC)** to log in to the CVM instance.

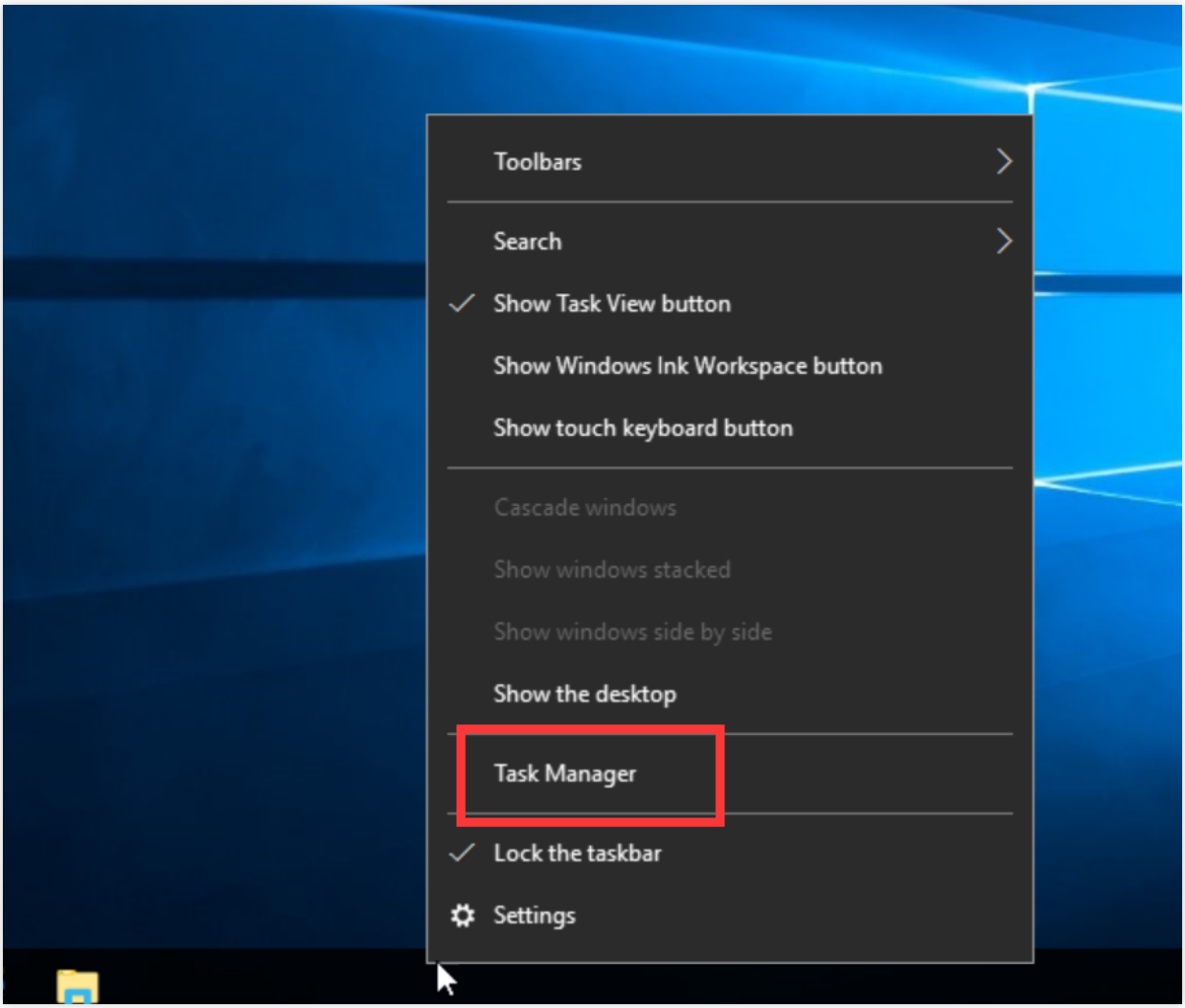
4. On the login page that appears, select **Send CtrlAltDel** in the upper-left corner and click **Ctrl-Alt-Delete** to access the system login page, as shown in the following figure:



Viewing the resource usage of processes

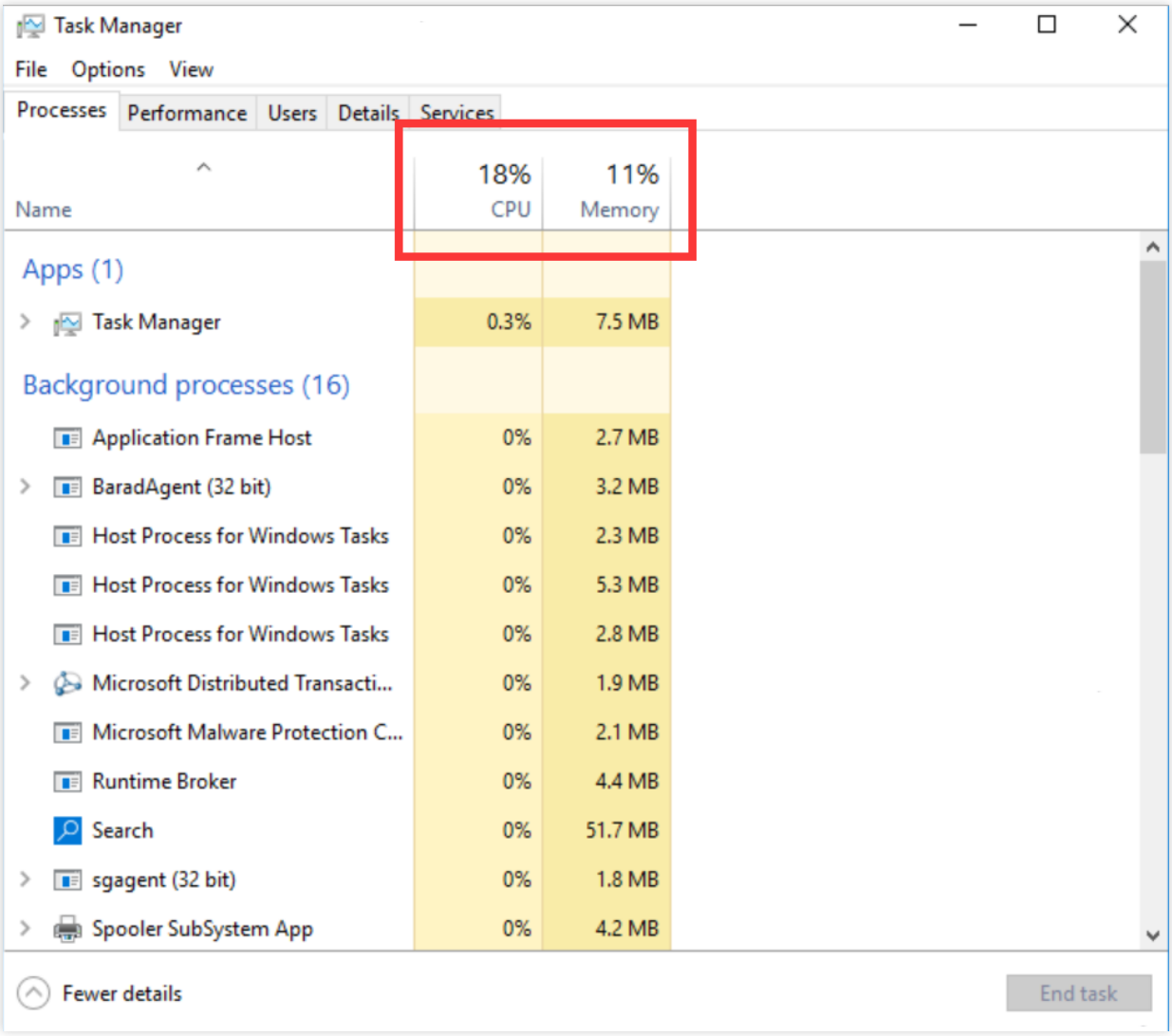
1. In the CVM instance, right-click the taskbar and select **Task Manager**, as shown in the following figure:

©2013-2022 Tencent Cloud. All rights reserved.



2. In "Task Manager", you can view the resource usage, as shown in the following figure:

©2013-2022 Tencent Cloud. All rights reserved.



Note:

You can sort the processes in ascending or descending order by clicking **CPU** or **Memory**.

Analyzing the processes

Analyze the processes on the **Task Manager** page to troubleshoot and solve the problem.

The problem is caused by a system process

If a system process is occupying too many CPU or memory resources, complete the following steps:

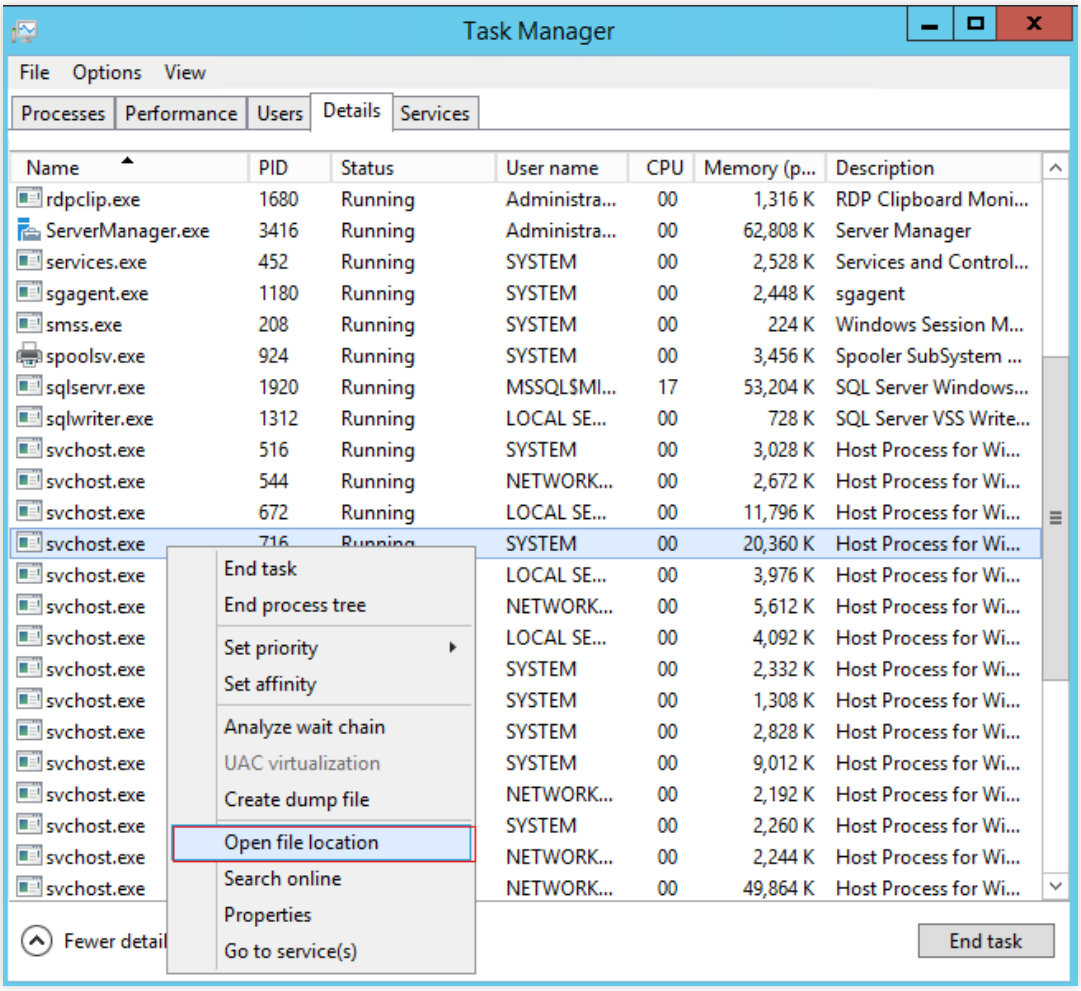
1. Verify the name of the process.

Several viruses use names that are very similar to system processes, such as svch0st.exe, explore.exe, and iexplorer.exe.

2. Locate the executable file that corresponds to the process.

System processes are usually located in `C:\\Windows\\System32` and have valid digital signatures and descriptions. To locate the corresponding executable file such as `svchost.exe`, select the process on the **Task Manager** page, right-click the process, and choose **Open file location**, as shown in the following figure:

©2013-2022 Tencent Cloud. All rights reserved.



If the executable file is not in `C:\\Windows\\System32` , it is likely that your CVM instance has a virus. Kill the virus manually or by using an antivirus application.

If the executable file is in `C:\\Windows\\System32` , restart your CVM instance or end safe but unnecessary processes.

The following describes typical system processes:

System Idle Process: a process that displays the percentage of time that the processor is idle for

system: a memory management process

explorer: the desktop and file management process

iexplore: the Microsoft Internet Explorer process

csrss: the Microsoft client/server runtime subsystem

svchost: a system process that is used to execute DLLs

Taskmgr: the task manager process

lsass: the local security permission service

The problem is caused by processes with exceptions

If you find that high CPU and memory usage is caused by processes with strange names such as xmr64.exe (a cryptocurrency mining malware), your CVM instance may be infected with viruses or trojans. In this case, use a search engine to verify whether the processes are in fact viruses or trojans.

©2013-2022 Tencent Cloud. All rights reserved.

Use an antivirus application to remove the virus or trojan. Then, back up the data and reinstall the operating system when necessary.

If the process is not a virus or a trojan, restart your CVM instance or end safe but unnecessary processes.

The problem is caused by a service process

If you find that the problem is caused by a service process such as IIS, HTTPD, PHP, or Java, further analyze the problem.

For example, check whether your business volume is high.

If yes, we recommend that you upgrade your CVM instance. If you do not upgrade your CVM instance, optimize your service processes.

If no, use service error logs to further analyze the problem. For example, check whether the resources are wasted due to incorrect parameter settings.

The problem is caused by a Tencent Cloud component process

If the problem is caused by a Tencent Cloud component process, submit a ticket, and we will help you locate and troubleshoot the problem.

Linux CVM instances

Logging in to the CVM instance

Select a CVM login method based on your actual needs.

Log in to the Linux CVM remotely via third party software.

Note:

If the Linux CVM has a high CPU load, you may fail to log in to the CVM.

Log in to a Linux instance via VNC.

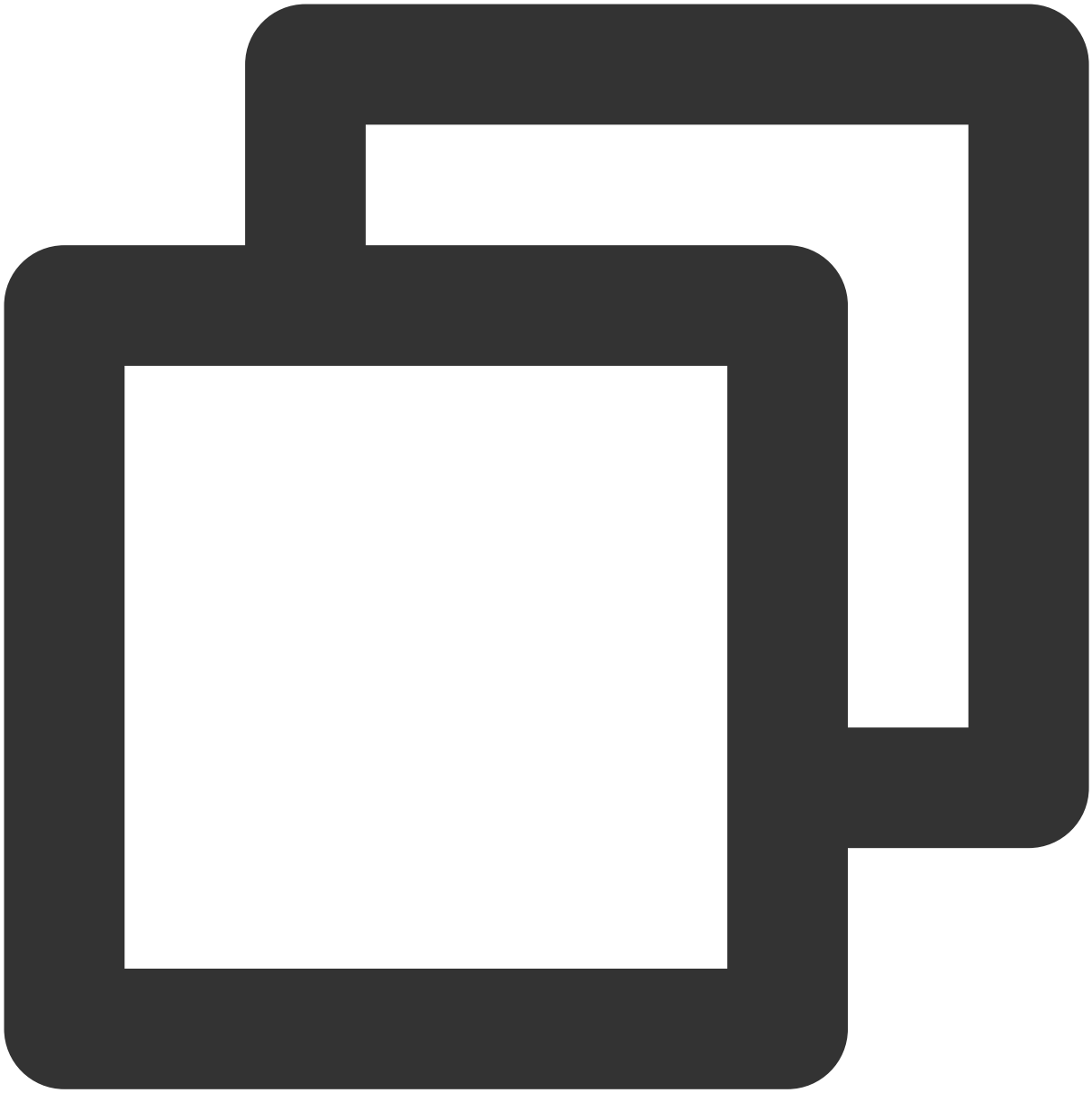
Note:

If the Linux CVM has a high CPU load, you can log in normally via the Console.

Viewing the resource usage of processes

Run the following command to view the system load. View the **%CPU** and **%MEM** columns and identify which processes consume more resources.

©2013-2022 Tencent Cloud. All rights reserved.



```
top
```

Analyzing processes

Analyze the processes on the **Task Manager** page to troubleshoot and solve the problem.

If the problem is caused by a service process, analyze whether the service process can be optimized and accordingly optimize the process or upgrade the CVM configuration.

If the problem is caused by a process with an exception, the instance may have a virus. In this case, you can terminate the process or use an antivirus application to kill the virus. When necessary, back up the data and reinstall the

©2013-2022 Tencent Cloud. All rights reserved.

operating system.

If the problem is caused by a Tencent Cloud component process, submit a ticket and we will help you locate and troubleshoot the problem.

Common Tencent Cloud components include:

sap00x: a security component

Barad_agent: a monitoring component

secu-tcs-agent: a security component

Terminating processes

1. Compare the resource consumption of different processes and record the PID of the process that needs to be terminated.
2. Enter `k` .
3. Enter the PID of the process that needs to be terminated and press the **Enter** key to terminate it, as shown in the following figure:

Suppose you need to terminate a process whose PID is 23.

```
top - 09:50:45 up 51 min,  1 user,  load average: 0.00, 0.01, 0.05
Tasks: 351 total,   1 running, 350 sleeping,   0 stopped,   0 zombie
%Cpu(s):  0.0 us,  0.1 sy,  0.0 ni, 99.9 id,  0.0 wa,  0.0 hi,  0.0 si,  0.0 st
KiB Mem :  1870516 total,  1441292 free,   127068 used,   302156 buff/cache
KiB Swap:  2097148 total,  2097148 free,        0 used.  1537932 avail Mem
PID to signal/kill [default pid = 2931] 23
  PID USER      PR  NI    VIRT    RES    SHR S  %CPU %MEM     TIME+ COMMAND
  293 root      20   0       0      0      0 S   0.2  0.0   0:03.24 kworker/2:1
  524 root      20   0       0      0      0 S   0.1  0.0   0:03.53 kworker/0:2
  137 root      20   0       0      0      0 S   0.1  0.0   0:02.70 rcu_sched
  141 root      20   0       0      0      0 S   0.0  0.0   0:00.73 rcuos/3
15672 root      20   0  130156   2028   1260 R   0.0  0.1   0:04.61 top
    1 root      20   0   57592   7436   2612 S   0.0  0.4   0:03.44 systemd
  310 root      20   0       0      0      0 S   0.0  0.0   0:00.64 kworker/u256:1
  333 root      20   0       0      0      0 S   0.0  0.0   0:00.26 kworker/3:1
  540 root      20   0       0      0      0 S   0.0  0.0   0:00.11 jbd2/sda2-8
  619 root      20   0   43016   2876   2564 S   0.0  0.2   0:00.33 systemd-journal
  738 root      20   0  329592  23192   6252 S   0.0  1.2   0:01.02 firewalld
  745 root      20   0   19284   1236    944 S   0.0  0.1   0:00.67 irqbalance
  754 dbus      20   0   34880   1904   1420 S   0.0  0.1   0:00.27 dbus-daemon
  853 root      20   0  509040   9620   5956 S   0.0  0.5   0:00.30 NetworkManager
  901 polkitd   20   0  514364  12260   4568 S   0.0  0.7   0:00.17 polkitd
 1816 root      20   0   91064   2064   1064 S   0.0  0.1   0:00.09 master
15681 root      20   0       0      0      0 S   0.0  0.0   0:00.06 kworker/1:1
15699 root      20   0       0      0      0 S   0.0  0.0   0:00.01 kworker/1:0
    2 root      20   0       0      0      0 S   0.0  0.0   0:00.09 kthreadd
```

Note:

If `kill PID 23 with signal [15]:` appears after you press **Enter**, press **Enter** again to keep the default settings.

4. If the operation is successful, the message `Send PID 23 signal [15/sigterm]` will appear. Press **Enter** to confirm the termination.

Other related problems

CPU usage is low but load average is high

Problem

©2013-2022 Tencent Cloud. All rights reserved.

The load average is an indicator of CPU load. The higher the load average, the longer the queue of pending processes is.

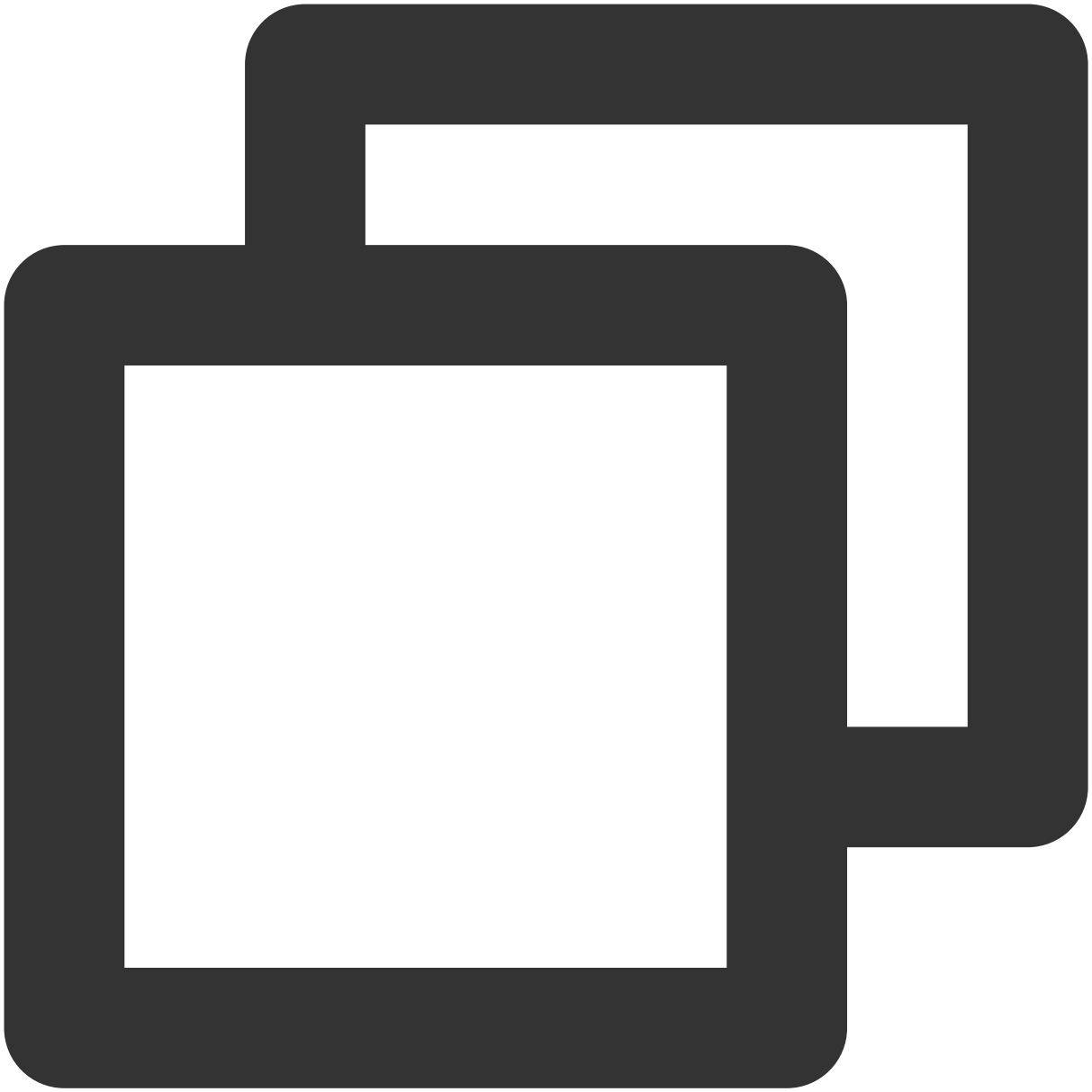
After the `top` command is executed, information similar to the following is returned, indicating that the CPU usage is low but the load average is very high.

```
    1   516   516   516 ?           -1 Ss       0   0:00 /sbin/iprinit --daemon
    1   569   569   569 ?           -1 Ss       0   0:00 /sbin/iprdump --daemon
    1   863   863   863 ?           -1 D+      38   0:16 /usr/sbin/ntpd -u ntp:ntp -g
    1   874   874   874 ?           -1 Ss       0   0:01 /usr/sbin/sshd -D
  874  8823  8823  8823 ?           -1 Ss       0   0:03  \_ sshd: root@pts/0
 8823  8825  8825  8825 pts/0     9006 Ss       0   0:00      \_ -bash
 8825  9006  9006  8825 pts/0     9006 D+       0   0:00          \_ ps -axjf
```

Solution

Run the following command to view the process states and check whether any process is in the D state, as shown in the following figure:

©2013-2022 Tencent Cloud. All rights reserved.



```
ps -axjf
```

©2013-2022 Tencent Cloud. All rights reserved.

```
    1   516   516   516 ?           -1 Ss       0   0:00 /sbin/iprinit --daemon
    1   569   569   569 ?           -1 Ss       0   0:00 /sbin/iprdump --daemon
    1   863   863   863 ?           -1 D+      38   0:16 /usr/sbin/ntpd -u ntp:ntp -g
    1   874   874   874 ?           -1 Ss       0   0:01 /usr/sbin/sshd -D
  874  8823  8823  8823 ?           -1 Ss       0   0:03  \_ sshd: root@pts/0
 8823  8825  8825  8825 pts/0     9006 Ss       0   0:00      \_ -bash
 8825  9006  9006  8825 pts/0     9006 D+       0   0:00          \_ ps -axjf
```

Note:

The D state refers to the uninterrupted sleep state. A process in this state cannot be terminated nor can it be exited by itself.

If there are many processes in the D state, restore the resources on which the processes depend or restart the operating system.

CPU usage of the kswapd0 process is high

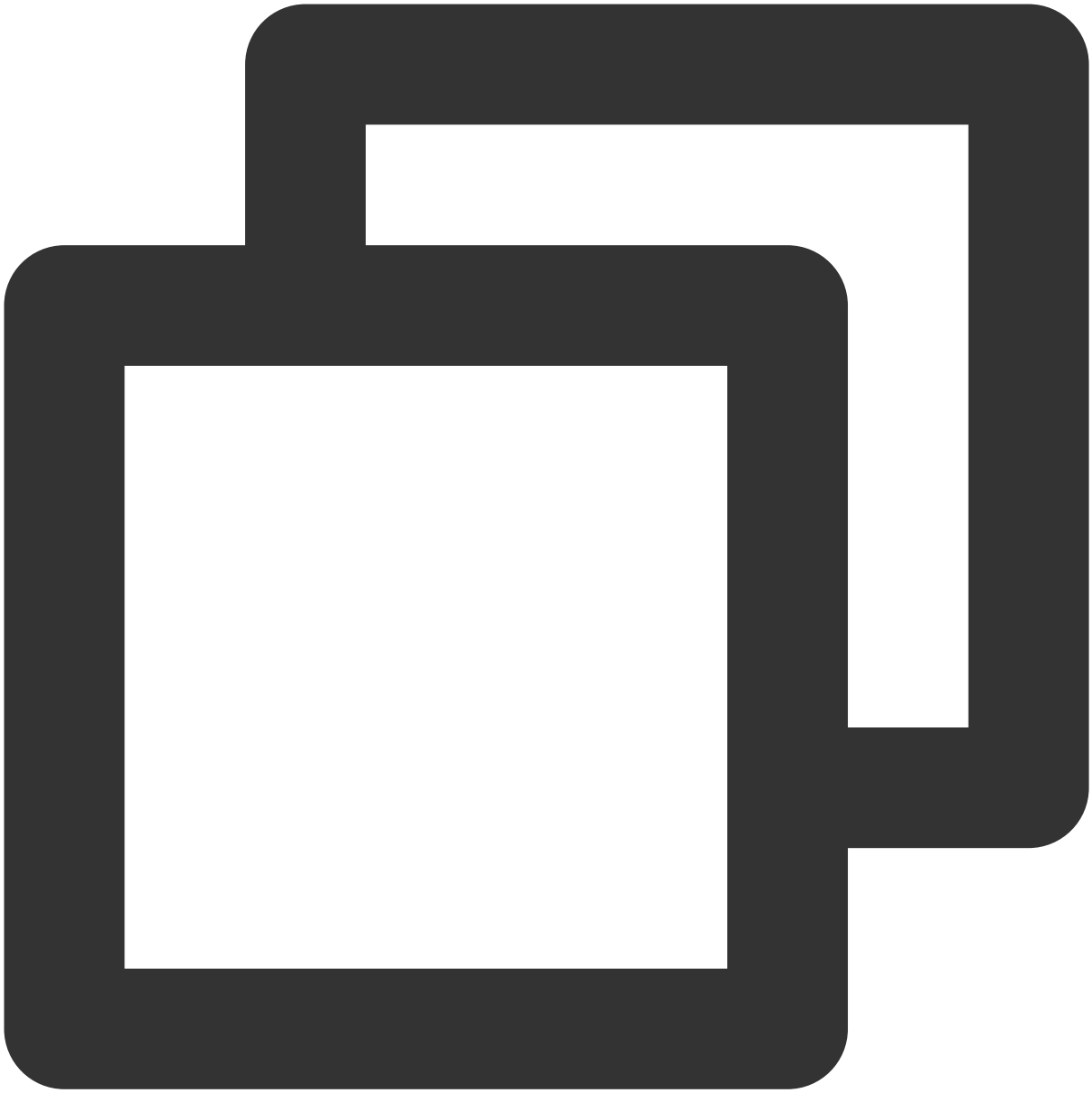
Problem

Linux manages memory by using the pagination mechanism and sets aside a portion of the disk as virtual memory. kswapd0 is the process responsible for page replacement in the virtual memory management of the Linux system. When system memory becomes insufficient, kswapd0 will frequently replace pages, which will result in high CPU usage.

Solution

1. Run the following command and find the kswapd0 process.

©2013-2022 Tencent Cloud. All rights reserved.



```
top
```

2. Check the state of the kswapd0 process.

If the process is not in the D state and has been running for a long time and consuming too many CPU resources, perform step 3 to check the memory usage.

3.

Run commands such as `vmstat` , `free` , and `ps` to check how much memory is being consumed by processes in the system.

©2013-2022 Tencent Cloud. All rights reserved.

Based on the memory usage, restart the system or terminate safe but unnecessary processes. If the si and so values are also high, pages are frequently replaced in the system. If the physical memory of the current system can no longer meet your requirements, please consider upgrading your system memory.

©2013-2022 Tencent Cloud. All rights reserved.

CVM Login Failure

Last updated：2024-01-27 17:35:59

Overview

Many causes can lead to CVM login failure. Causes that can be monitored by Tencent Cloud Observability Platform include overly high CVM bandwidth usage and overly high CVM CPU/memory usage. This document describes how to troubleshoot these two causes.

Problem Analysis

The following causes of CVM login failure can be detected by Tencent Cloud Observability Platform:
CVM bandwidth utilization is too high
CVM CPU/memory usage is too high
Note:
Before troubleshooting, check whether the login attempt failed because the entered password was incorrect, you forgot the password, or the password failed to reset.
If yes, reset the password.

Solutions

CVM bandwidth utilization is too high

Problem: the self-diagnosis tool shows that bandwidth utilization is too high.
Solutions:
1. Log in to the CVM instance via VNC.
Log in to a Windows instance via VNC.
Log in to a Linux instance via VNC.
2. Check the bandwidth utilization of the instance and troubleshoot accordingly. For more information, see CVM Bandwidth Utilization Is Too High.

CVM CPU/memory usage is too high

Problem: the self-diagnosis tool or Tencent Cloud Observability Platform shows that the CPU/memory usage of the CVM instance is too high, and therefore the system cannot establish a remote connection or the connectivity is poor.
Possible causes: viruses, trojans, third-party anti-virus software, application exceptions, driver exceptions, and

©2013-2022 Tencent Cloud. All rights reserved.

automatic software backend updates may lead to high CPU usage, resulting in CVM login failure or slow access.

Solutions:

1. Log in to the CVM instance via VNC.

Log in to a Windows instance via VNC.

Log in to a Linux instance via VNC.

2. Refer to CVM CPU/Memory Usage Is Too High to identify the process with a high load on the **Task Manager** page.

Note:

Many causes may lead to CVM login failure. For more information on other causes, see Windows Instance Login Failures or Linux Instance Login Failures.

©2013-2022 Tencent Cloud. All rights reserved.

CVM Bandwidth Utilization Is Too High

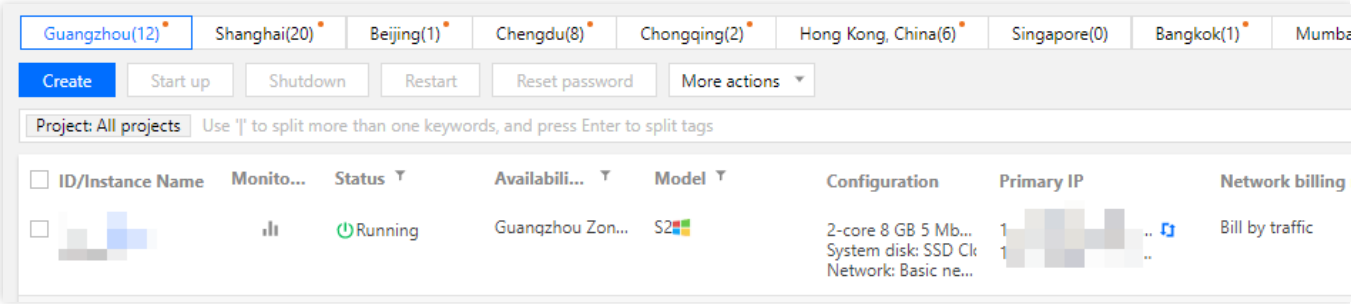
Last updated：2024-01-27 17:35:59

Overview

This document describes how to troubleshoot and solve the problem of Linux or Windows CVM login failure caused by overly high bandwidth utilization.

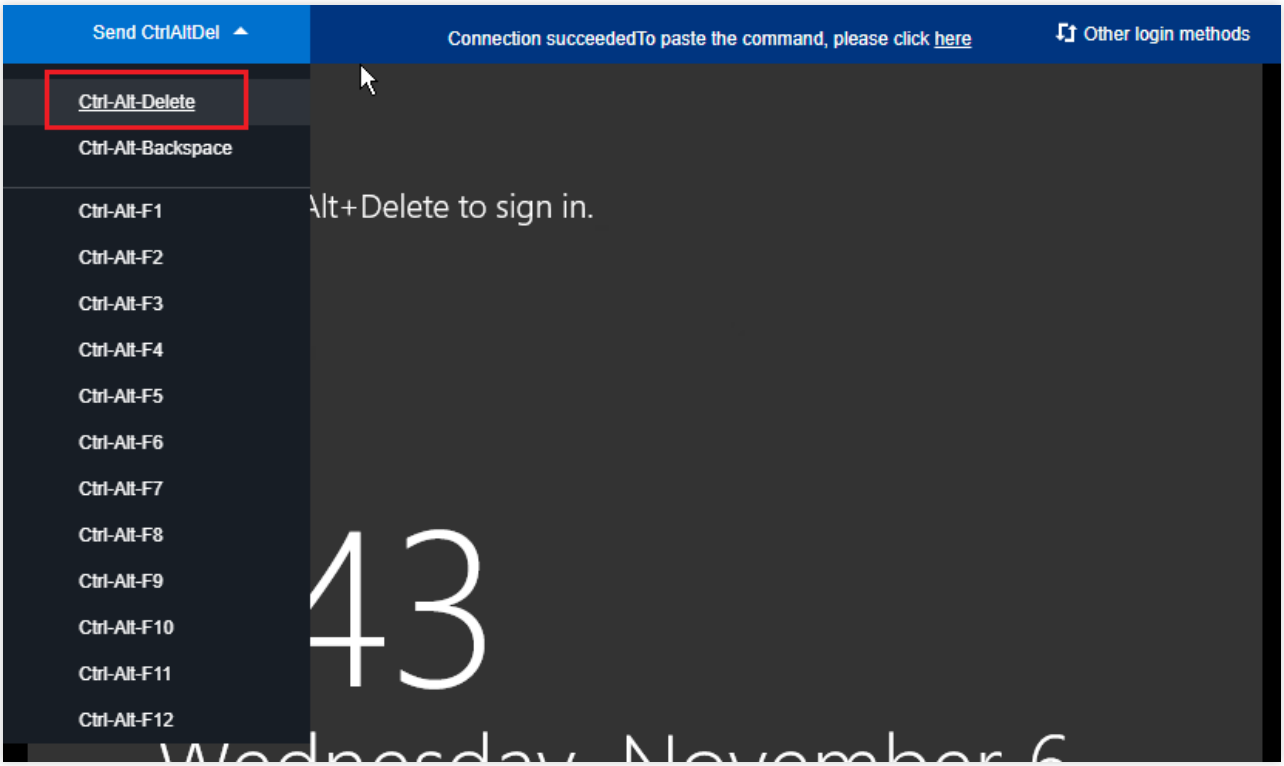
Locating and Troubleshooting the Problem

1. Log in to the CVM Console.
2. Select the target CVM instance and click **Log In**, as shown in the following figure:



3. On the **Log in to Windows/Linux instance** window that pops up, click **Log In Now** under **Alternative login methods (VNC)** to log in to the CVM instance.
4. On the login page that appears, select **Send CtrlAltDel** in the upper-left corner and click **Ctrl-Alt-Delete** to access the system login page, as shown in the following figure:

©2013-2022 Tencent Cloud. All rights reserved.



Windows CVM instances

After logging in to the Windows CVM instance via VNC, perform the following operations:

Note:

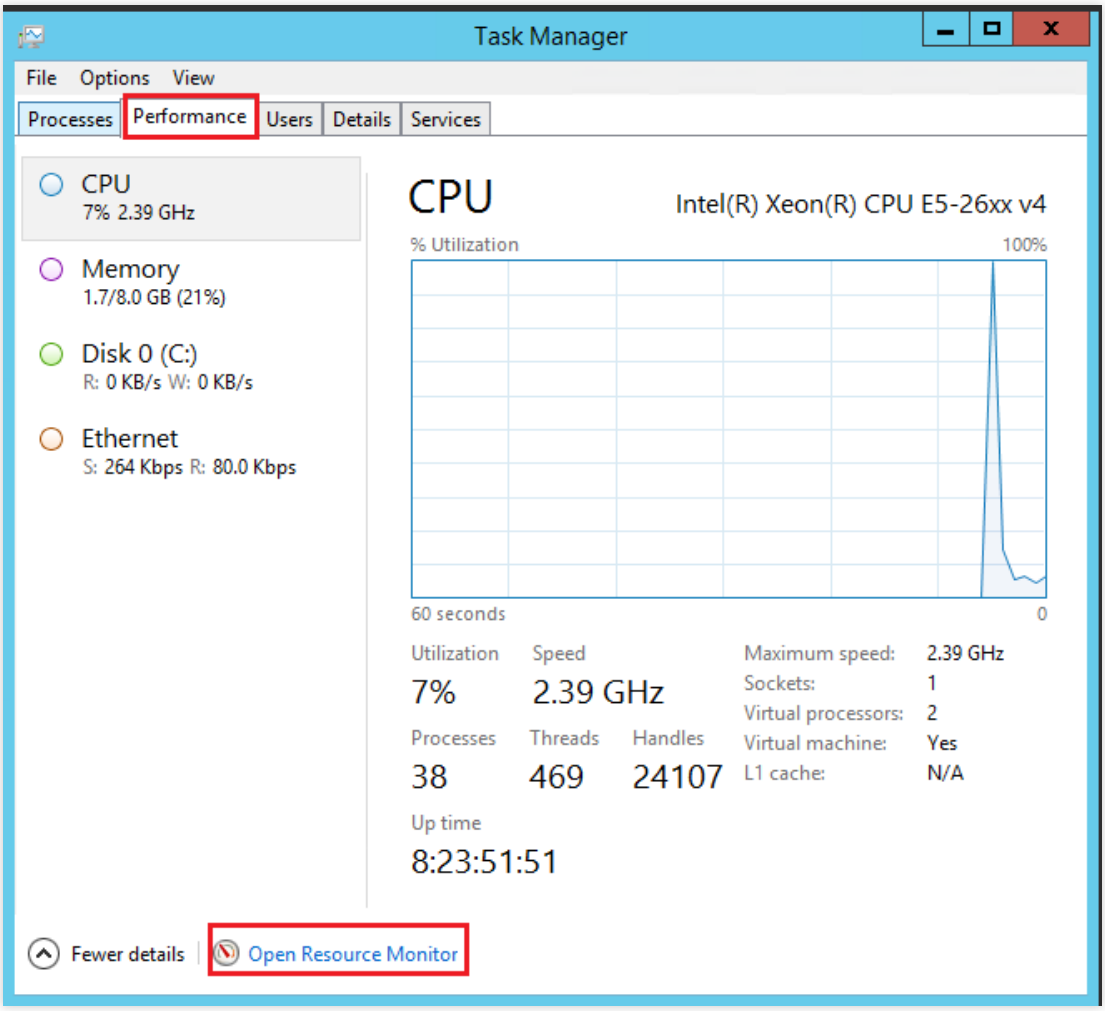
The following operations use a CVM instance running in the Windows Server 2012 operating system as an example.

1. In the CVM instance, click

. Select **Task Manager** to open the **Task Manager** page.

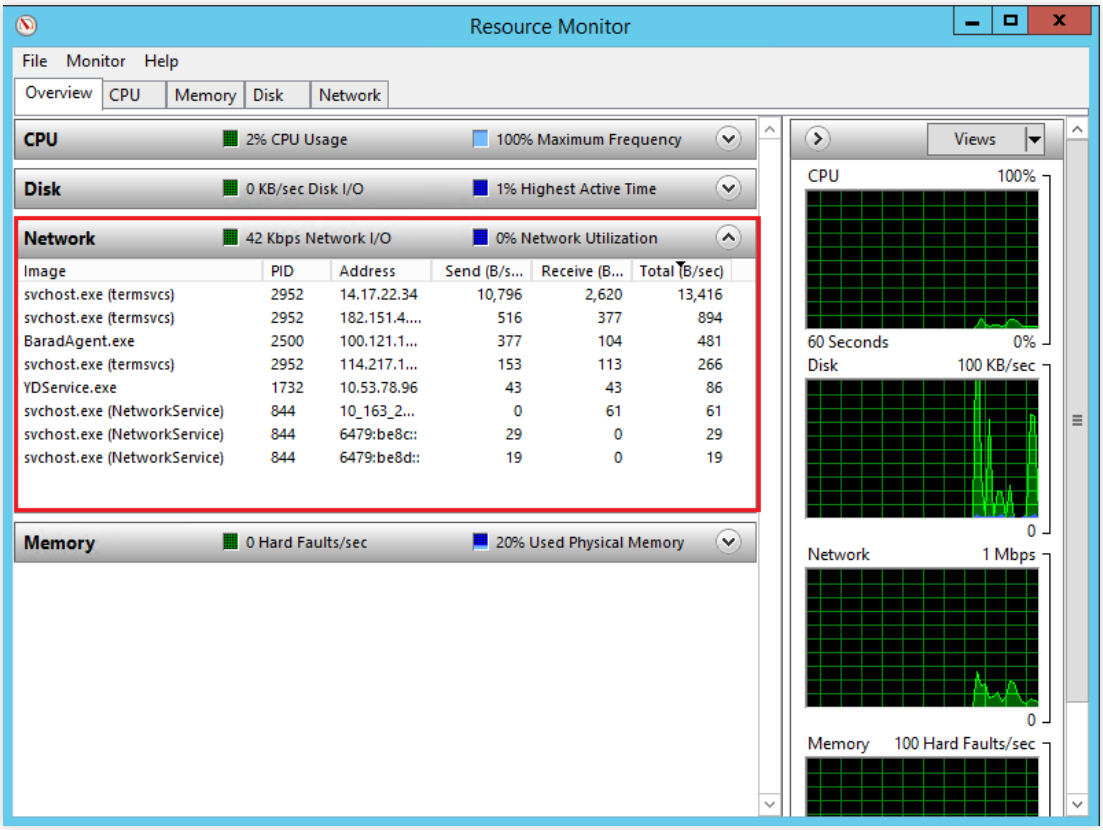
2. Click the **Performance** tab and then click **Open Resource Monitor**, as shown in the following figure:

©2013-2022 Tencent Cloud. All rights reserved.



3. On the **Resource Monitor** page, identify the process that consumes a lot of bandwidth. Based on your actual business, determine whether the process is normal, as shown in the following figure:

©2013-2022 Tencent Cloud. All rights reserved.



If this process is a service process, check whether the high bandwidth utilization is caused by changes in access traffic and whether you need to optimize the capacity or upgrade the CVM configuration.

If this process has an exception, the high bandwidth utilization may be caused by a virus or a trojan. If so, you can manually terminate the process or use security software to kill the virus. You can also back up data and then reinstall the operating system.

Note:

In Windows, many virus processes can disguise themselves as system processes. You can select **Task Manager** > **Processes** to check the process information and preliminarily identify the virus.

Normal system processes have complete signatures and descriptions, and most of them are located in the `C:\\Windows\\System32` directory. While virus programs may have the same names as system processes, they lack signatures and descriptions. In addition, their locations are often abnormal.

If this process is a Tencent Cloud component process, please submit a ticket, and we will help you locate and troubleshoot the problem.

Linux CVM instances

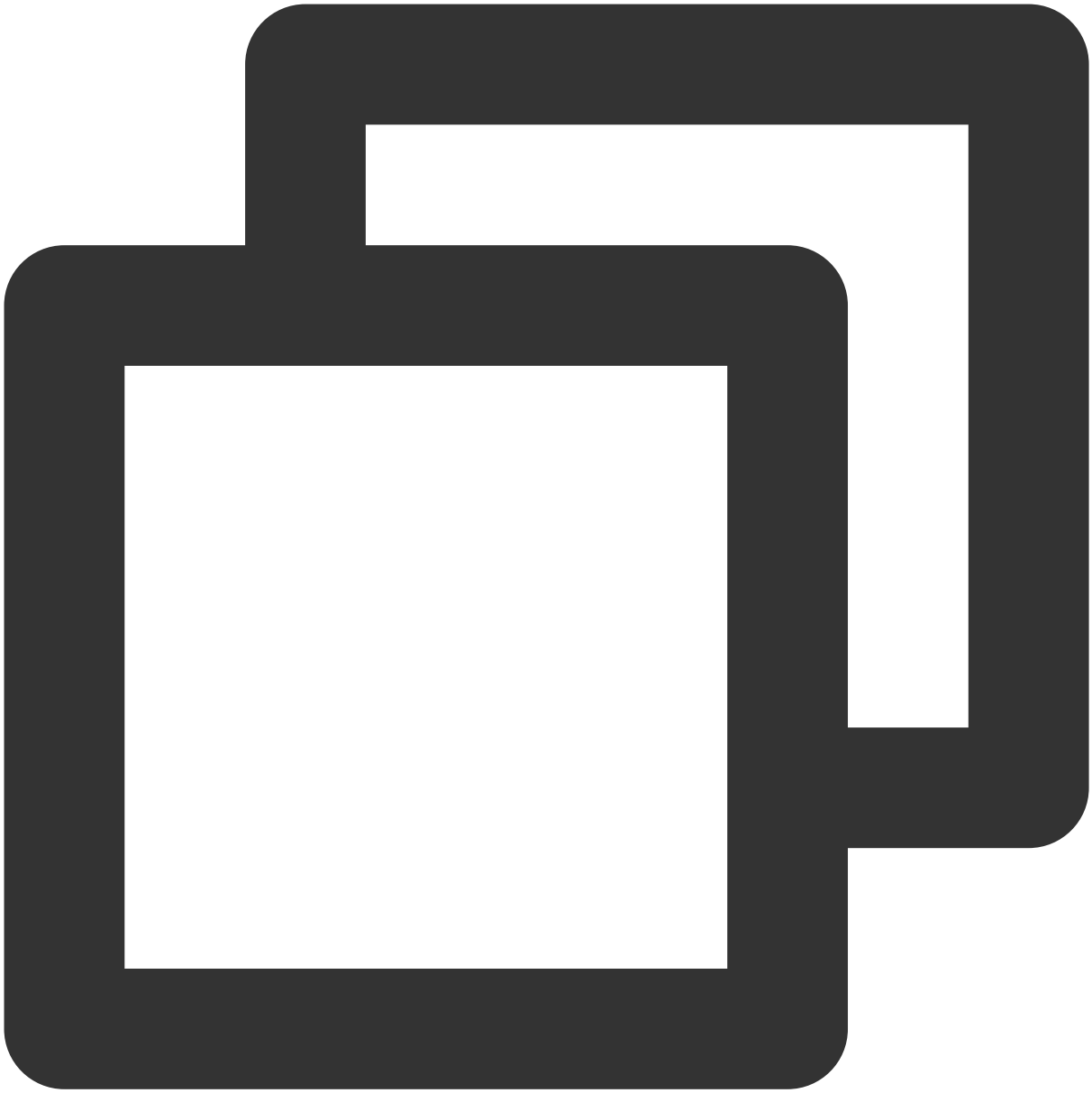
After logging in to the Linux CVM instance via VNC, perform the following operations:

Note:

The following operations use a CVM instance with the CentOS 7.6 operating system as an example.

1. Run the following command to install the iftop tool. This tool monitors traffic for Linux CVM instances.

©2013-2022 Tencent Cloud. All rights reserved.



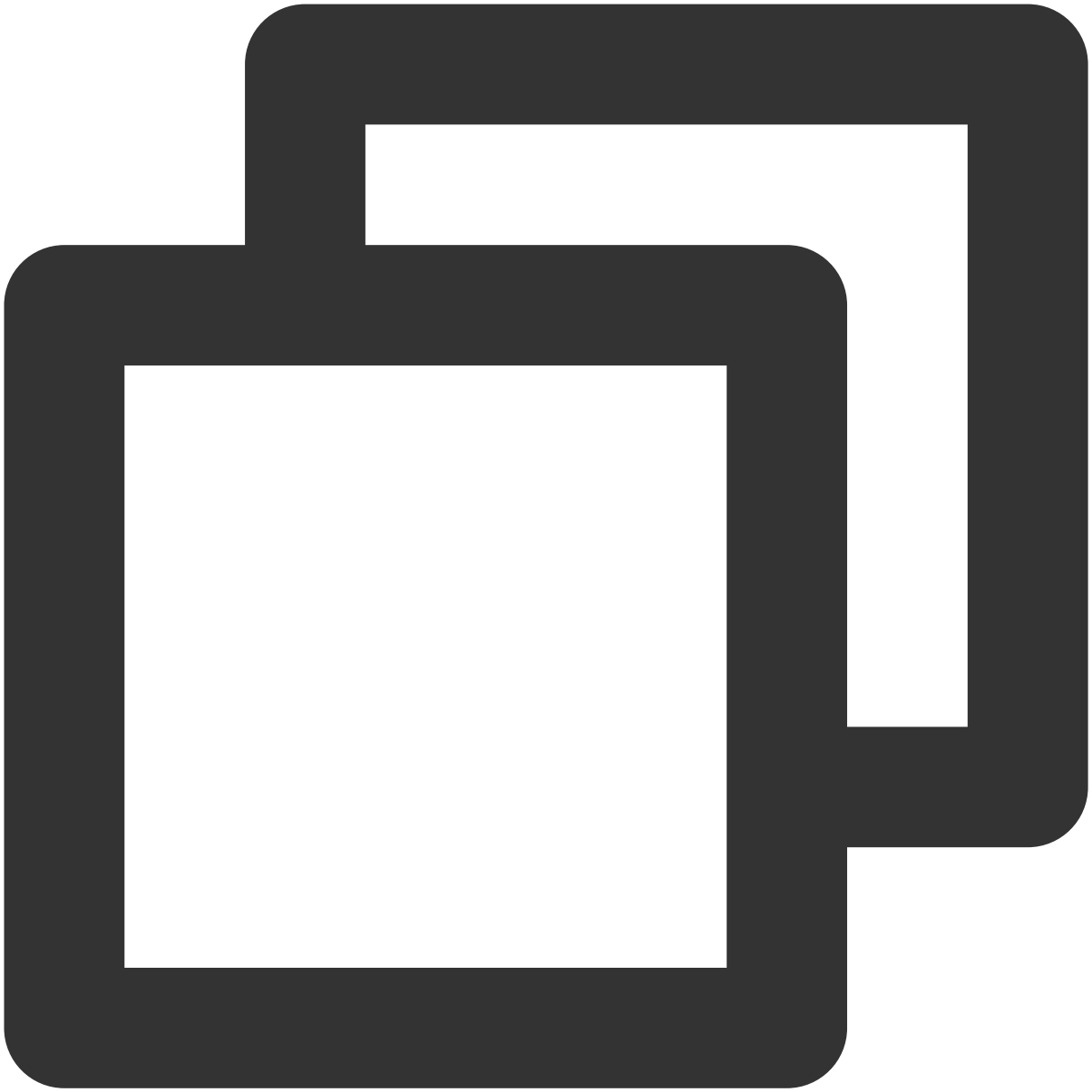
```
yum install iftop -y
```

Note:

For a CVM instance with the Ubuntu operating system, run the `apt-get install iftop -y` command.

2. Run the following command to install lsof.

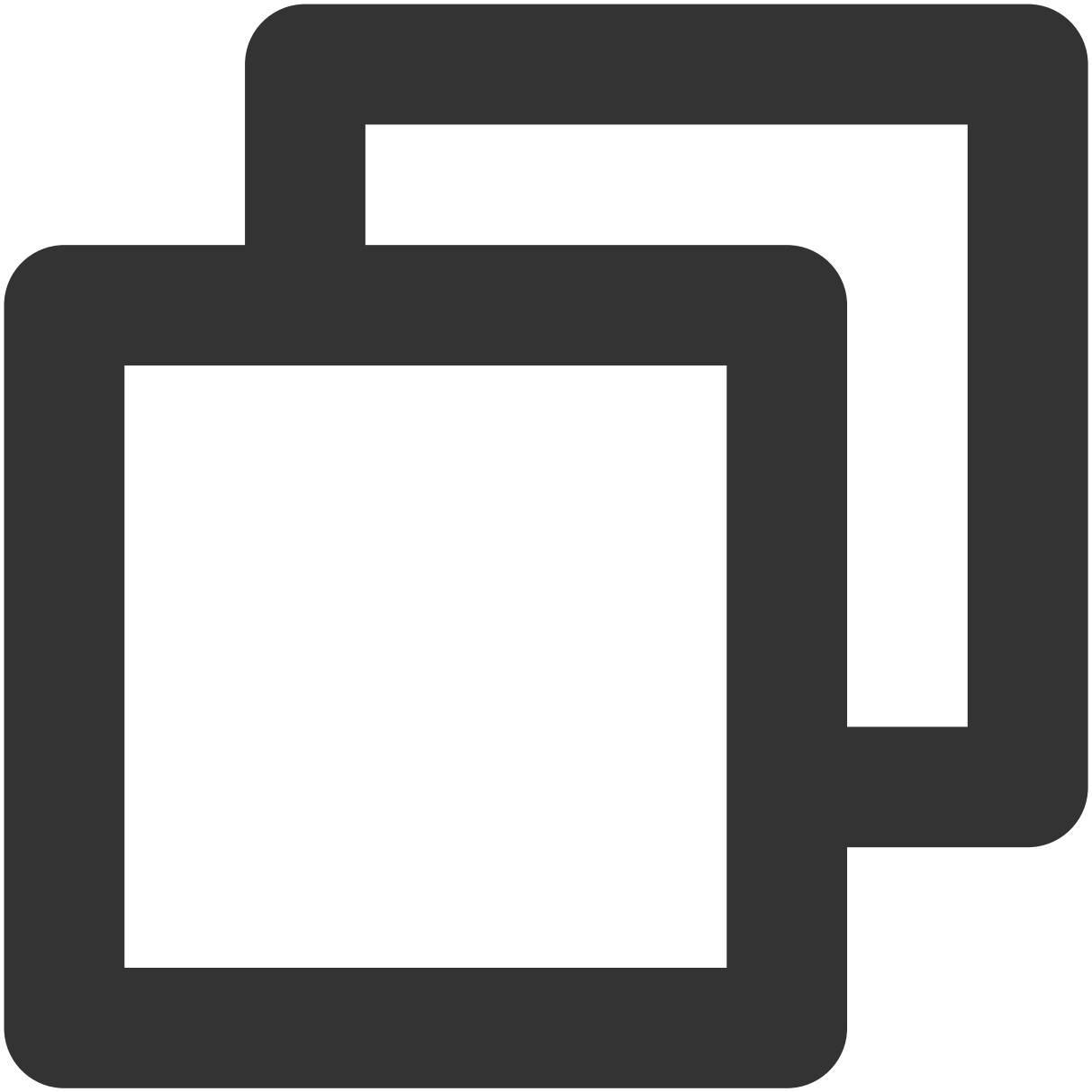
©2013-2022 Tencent Cloud. All rights reserved.



```
yum install lsof -y
```

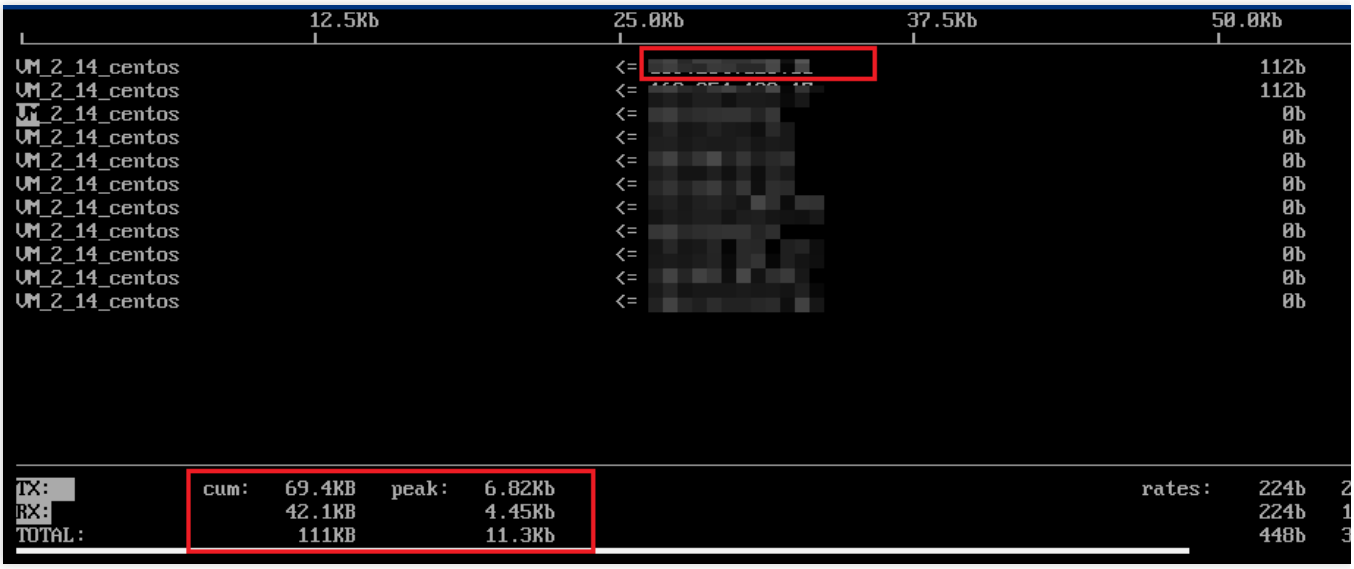
3. Run the following command to run iftop, as shown in the following figure:

©2013-2022 Tencent Cloud. All rights reserved.



```
iftop
```

©2013-2022 Tencent Cloud. All rights reserved.



`<=` and `=>` indicate the direction of the traffic.

"TX" indicates the traffic is outbound.

"RX" indicates the traffic is inbound.

"TOTAL" indicates the total traffic.

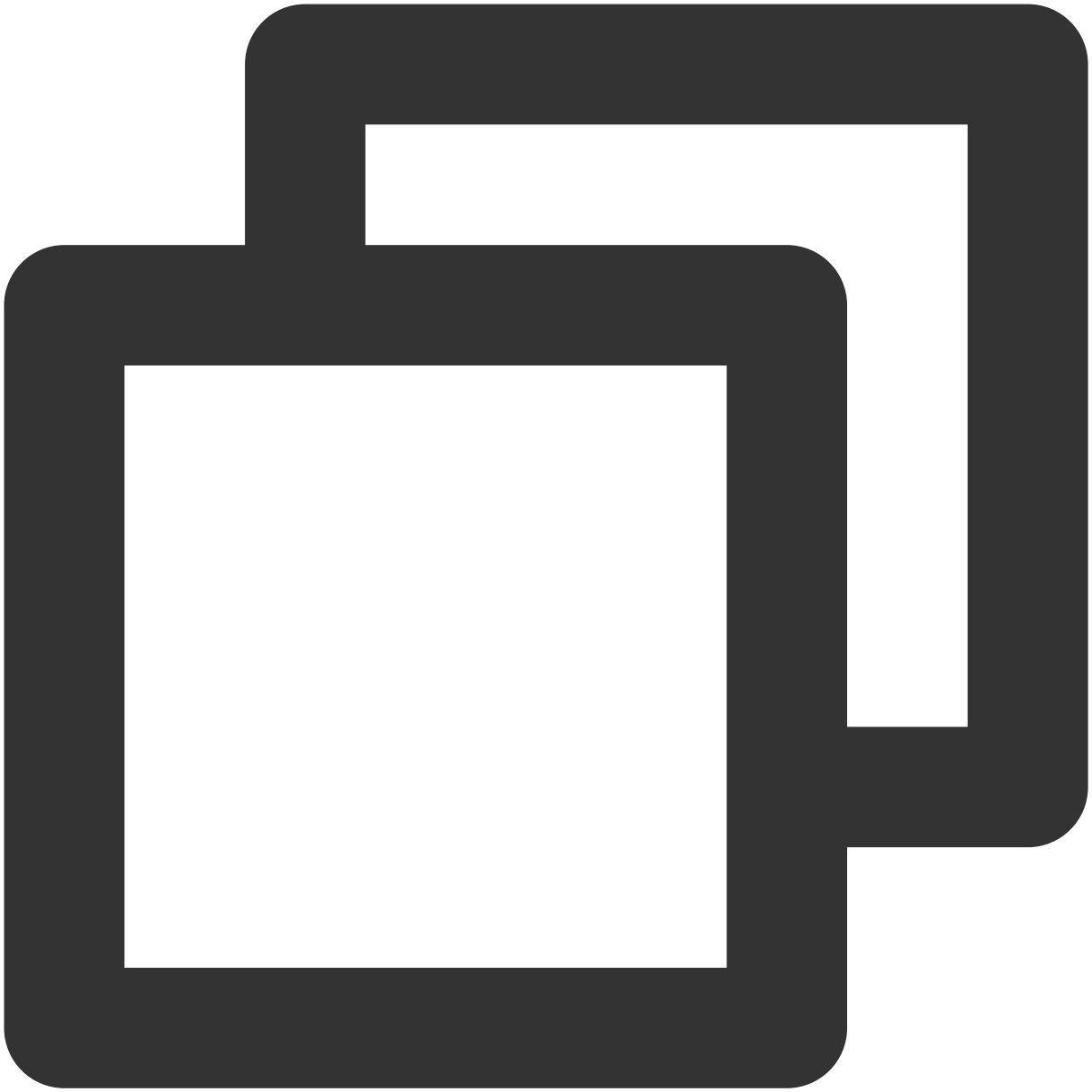
"Cum" indicates the total traffic from the moment iftop started to run until now.

"peak" indicates the traffic peak.

"rates" indicates the average traffic over the last 2, 10, and 40 seconds.

4. Based on the IP address of the consumed traffic in iftop, run the following command to check the process connected to this IP address.

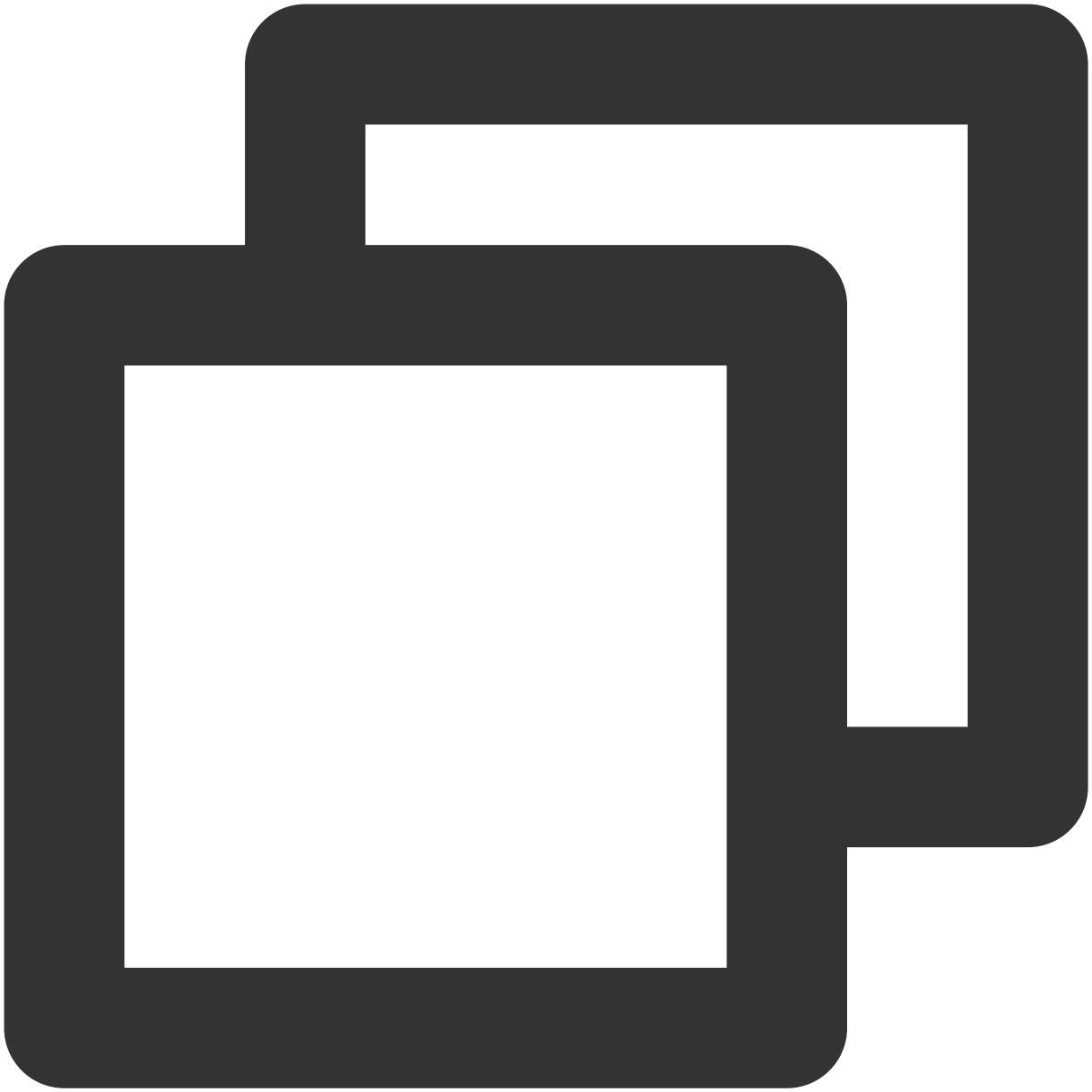
©2013-2022 Tencent Cloud. All rights reserved.



```
lsof -i | grep IP
```

For example, if the IP address of the consumed traffic is 201.205.141.123, run the following command:

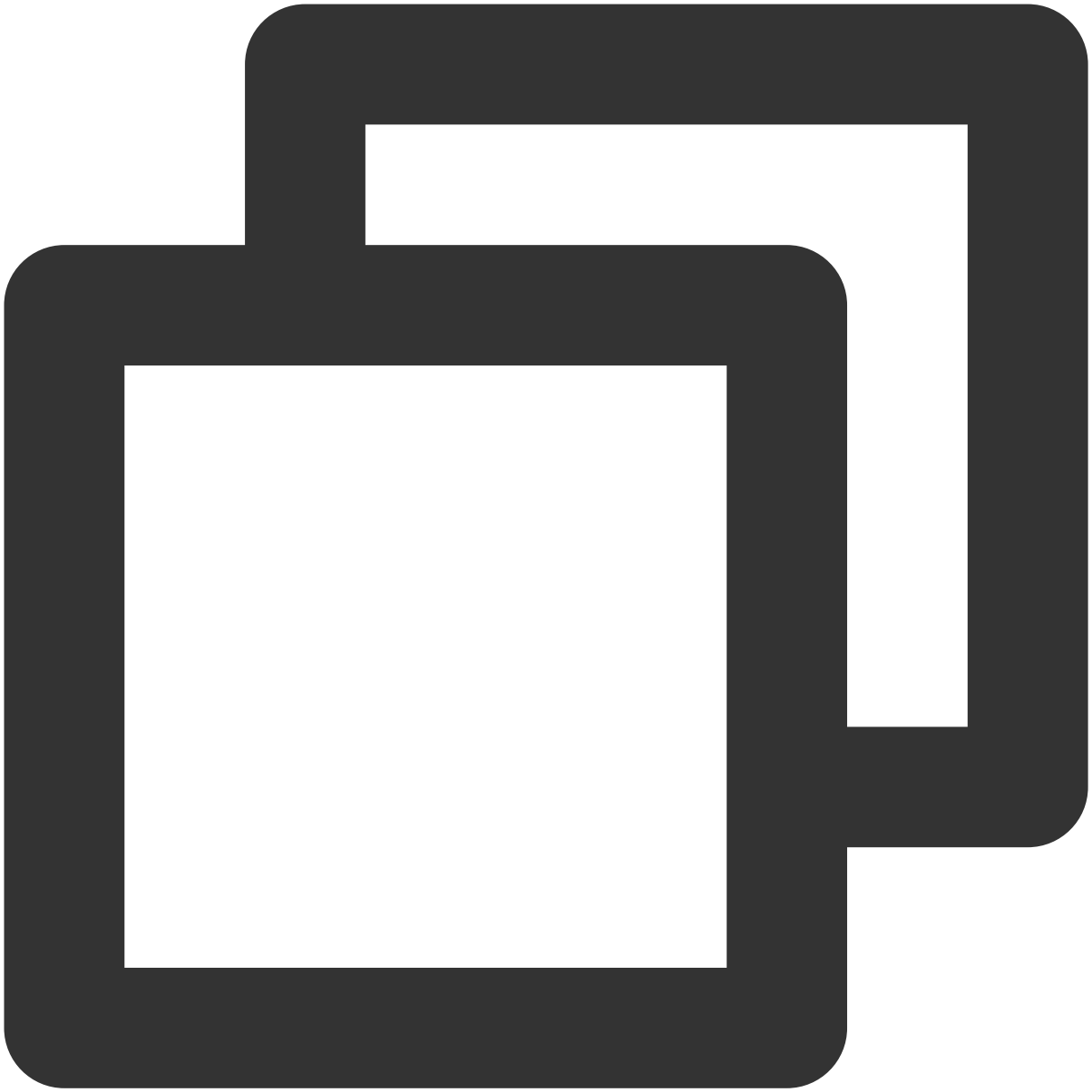
©2013-2022 Tencent Cloud. All rights reserved.



```
lsof -i | grep 201.205.141.123
```

If the following result is returned, the majority of the CVM bandwidth is consumed by the SSH process.

©2013-2022 Tencent Cloud. All rights reserved.



```
sshd       12145    root    3u  IPV4  3294018       0t0   TCP 10.144.90.86:ssh->203
sshd       12179  ubuntu    3u  IPV4  3294018       0t0   TCP 10.144.90.86:ssh->203
```

5. View the process that consumes a lot of bandwidth and check whether the process is normal.

If this process is a service process, check whether the high bandwidth utilization is caused by changes in access traffic and whether you need to optimize the capacity or upgrade the CVM configuration.

If this process has an exception, the high bandwidth utilization may be caused by a virus or a trojan. If so, you can manually terminate the process or use security software to kill the virus. You can also back up data and then reinstall the operating system.

©2013-2022 Tencent Cloud. All rights reserved.

If this process is a Tencent Cloud component process, please submit a ticket, and we will help you locate and troubleshoot the problem.

We recommend that you check the location of the destination IP address on WhatIsMyIPAddress.com. If the destination IP address is located in another country or region, the security risk is higher.

©2013-2022 Tencent Cloud. All rights reserved.

CVM Has No Monitoring Data

Last updated：2024-01-27 17:35:59

Overview

The CVM instance must have the monitoring component agents installed to collect CVM metric data. If you cannot get the monitoring metric data, refer to this document to troubleshoot this problem.
We recommend you reinstall the agents first as instructed in Installing CVM Agents and wait 3 minutes before checking again whether the monitoring data is restored. If an error occurs during the reinstallation or the monitoring data is not restored, troubleshoot the problem as detailed below.

Causes and Solutions

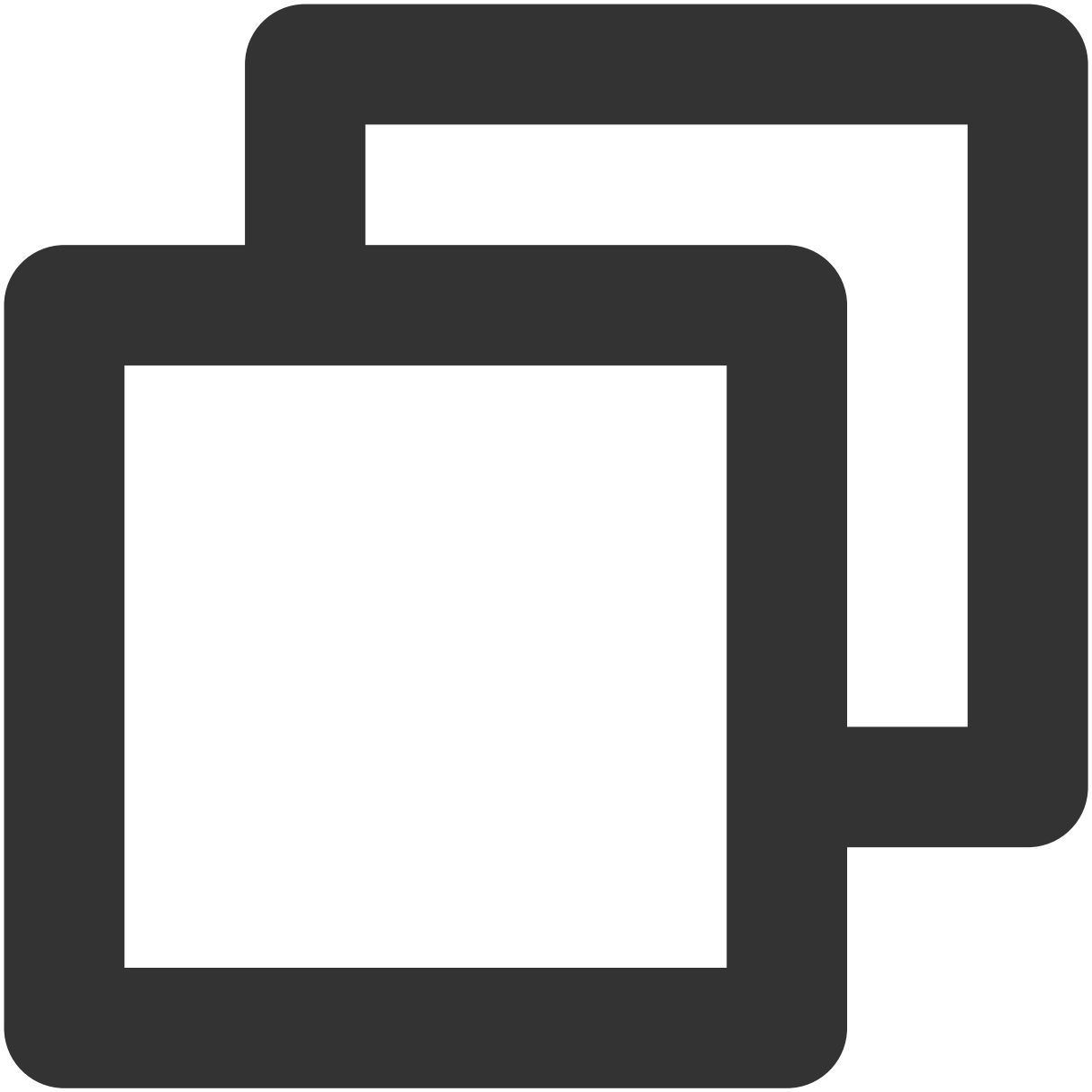
Cause	Solution
The agents are not installed/started	Troubleshoot by referring to Step 1
The reporting domains cannot be resolved	Troubleshoot by referring to Step 2
The agents failed to get the UUID	Troubleshoot by referring to Step 3
The CVM instance is shut down or being restarted	Troubleshoot by referring to Step 4
The CVM instance is under high load	Troubleshoot by referring to Step 5

Troubleshooting Procedure

Step 1. Check whether the agents have been installed or started

The troubleshooting procedures for Linux and Windows are different. You can refer to a procedure as needed.
Linux
Windows
1. Run the following command to check whether the agents have been installed successfully.

©2013-2022 Tencent Cloud. All rights reserved.



```
crontab -l |grep stargate
```

If the following message is displayed, the agents have been installed:

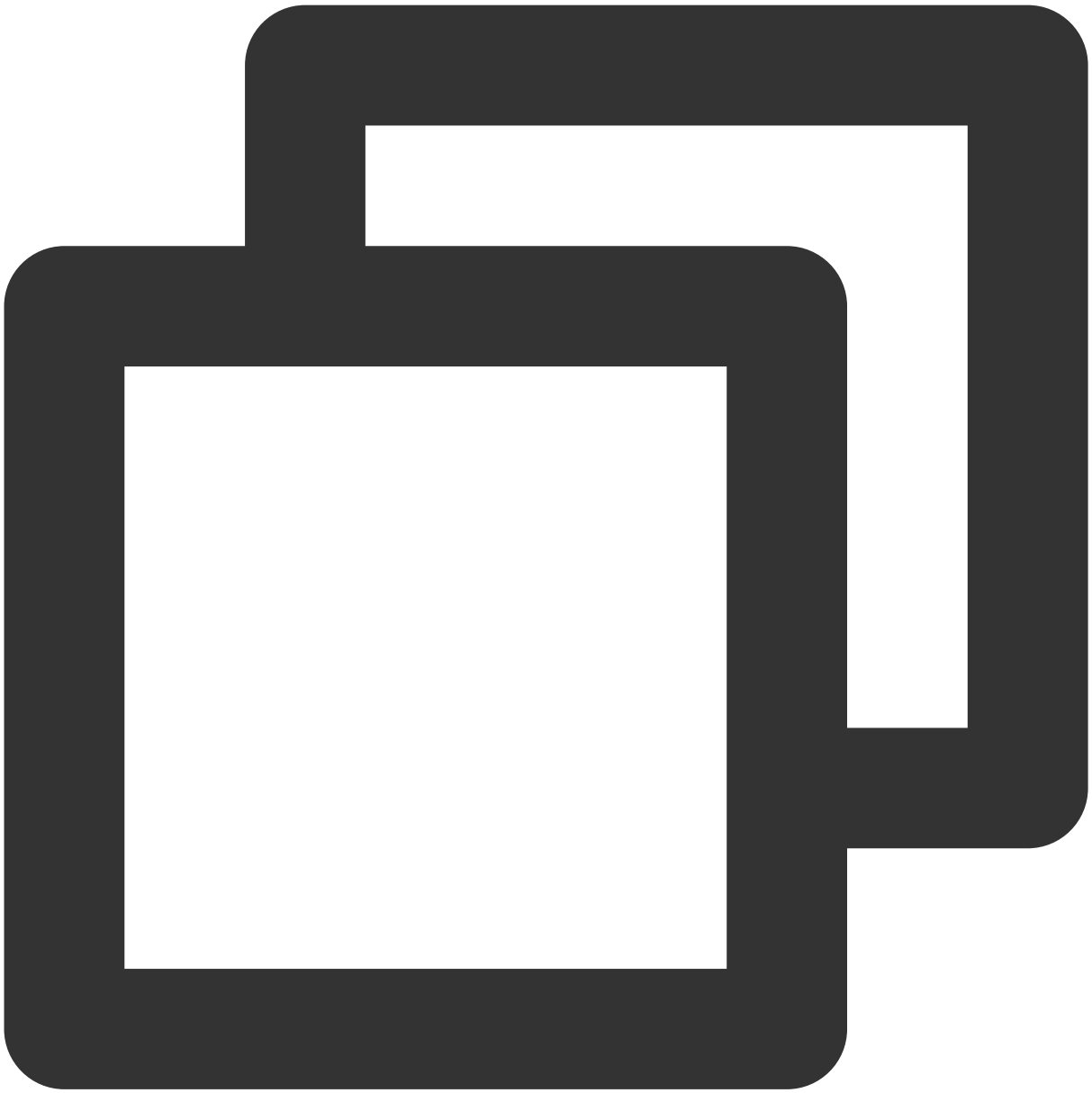
```
[r[redacted]]# crontab -l |grep stargate
*/1 * * * * flock -xn /tmp/stargate.lock -c '/usr/local/qcloud/stargate/ad
```

If not, install the agents as instructed in Installing CVM Agents.

©2013-2022 Tencent Cloud. All rights reserved.

2. Check whether the agents run properly.

Run the following commands to check whether the agents run properly:



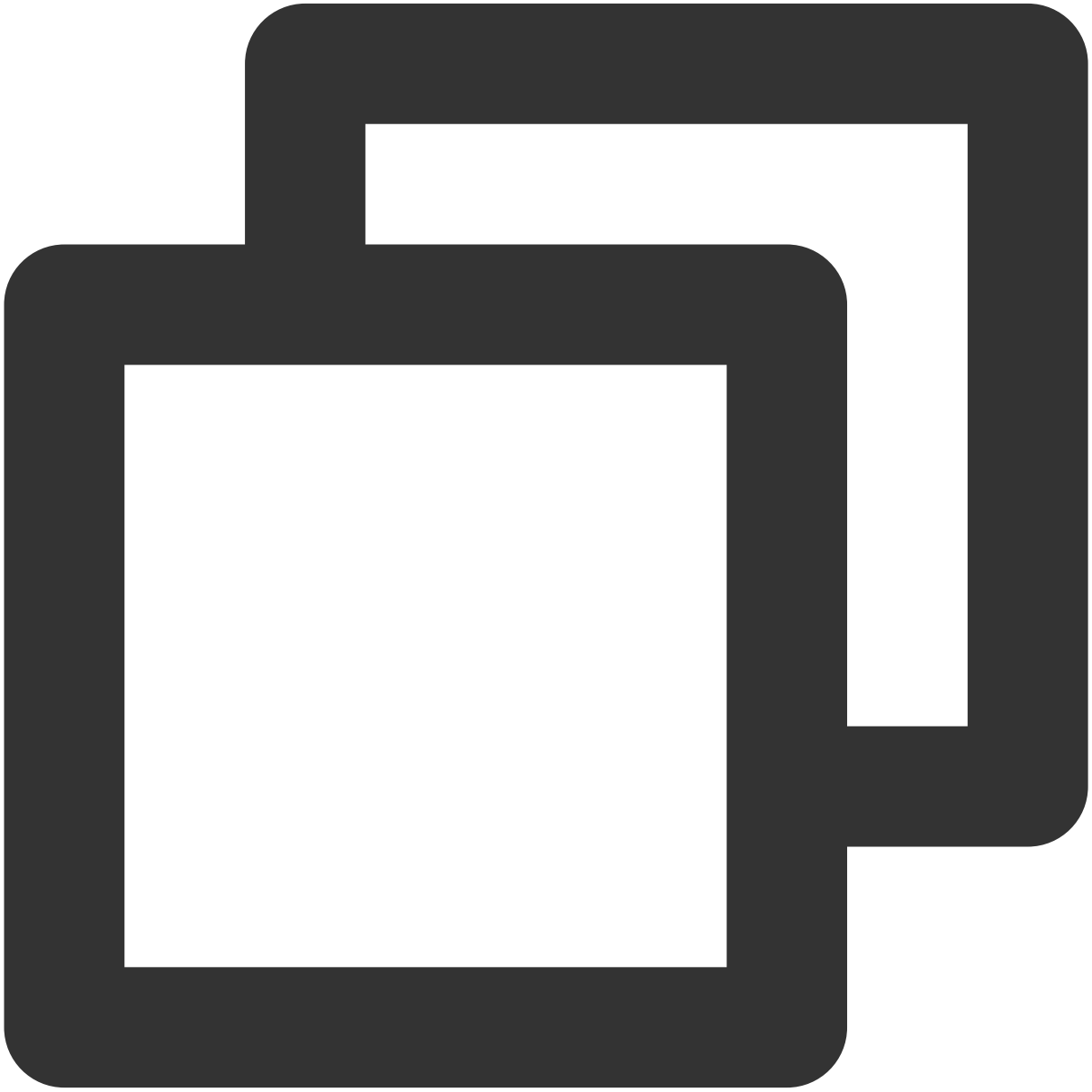
```
ps ax | grep sgagent
ps ax | grep barad_agent
```

If the output is as shown below, the agents run normally (note that the number of `barad_agent` processes is 3):

©2013-2022 Tencent Cloud. All rights reserved.

```
root@[redacted]:~# ps ax | grep barad_agent
15286 pts/0    S+     0:00 grep --color=auto barad_agent
22515 ?        S      0:06 barad_agent
22530 ?        S      1:04 barad_agent
22531 ?        Sl    10:16 barad_agent
```

If there is no output or the number of processes is incorrect, the agents are abnormal. In this case, run the following commands as the root account to start the agents. If the messages `stargate agent run succ` and `barad_agent run succ` are displayed, the agents have been restarted successfully.



```
cd /usr/local/qcloud/stargate/admin
```

©2013-2022 Tencent Cloud. All rights reserved.

```
./restart.sh
cd /usr/local/qcloud/monitor/barad/admin
./stop.sh
./trystart.sh
```

Note:

After the agents are started, wait 3 minutes and then check whether there is monitoring data in the CVM console.

Run `services.msc` to check whether the agents are installed and started. If the status of QCloud BaradAgent Monitor or QCloud Stargate Manager is not `Running`, the service is not started. In this case, click the name of the corresponding service and start it.

Note:

If the agents are already started but there is still no monitoring data, you can proceed with the troubleshooting.

If the agents have not been installed, your CVM instance cannot be monitored and you will not receive a notification when the CVM instance runs abnormally, which can pose a high risk. For more information on the installations of agents, see Installing CVM Agents.

Step 2. Check reporting domains

The following 4 domains need to be resolved for the agents to run properly:

update2.agent.tencentyun.com

receiver.barad.tencentyun.com

custom.message.tencentyun.com

metadata.tencentyun.com

The procedures for checking and fixing the reporting domains are different for Linux and Windows. You can refer to a procedure as needed.

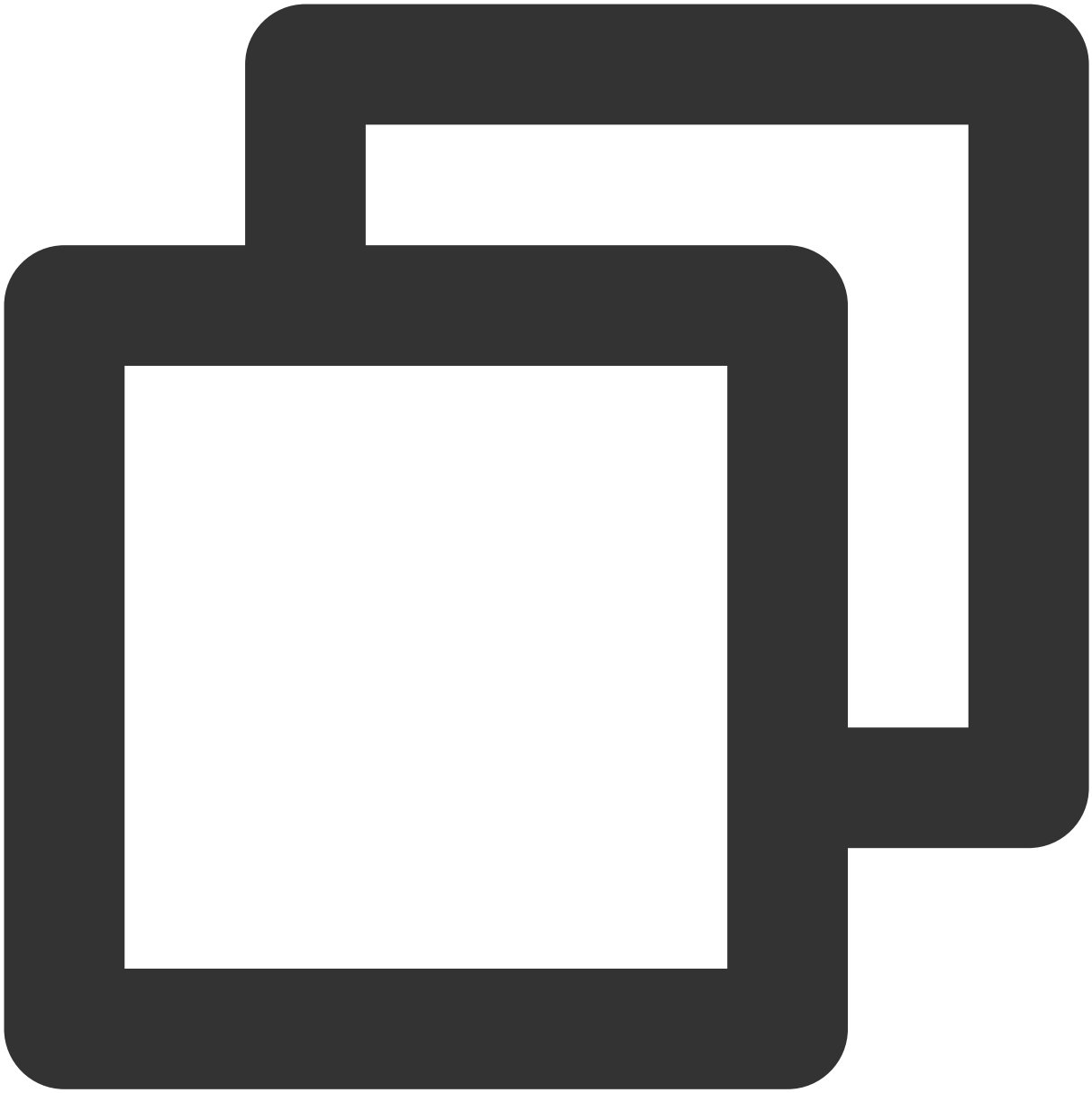
Linux

Windows

1. Check whether the reporting domains can be resolved properly.

Run the following commands to check whether these 4 domains can be resolved properly:

©2013-2022 Tencent Cloud. All rights reserved.



```
ping -c 1 update2.agent.tencentyun.com
ping -c 1 receiver.barad.tencentyun.com
ping -c 1 custom.message.tencentyun.com
ping -c 1 metadata.tencentyun.com
```

In normal cases, these 4 domains can be resolved on the CVM instance. If `unknown host` is displayed, the domains fail to be resolved. You can proceed to the next step to fix it.

2. Fix DNS resolution.

Tencent Cloud provides reliable private network DNS servers in different regions. We recommend you not overwrite the default DNS configurations. If you need to modify them, fix the resolution for the 4 domains above as follows:

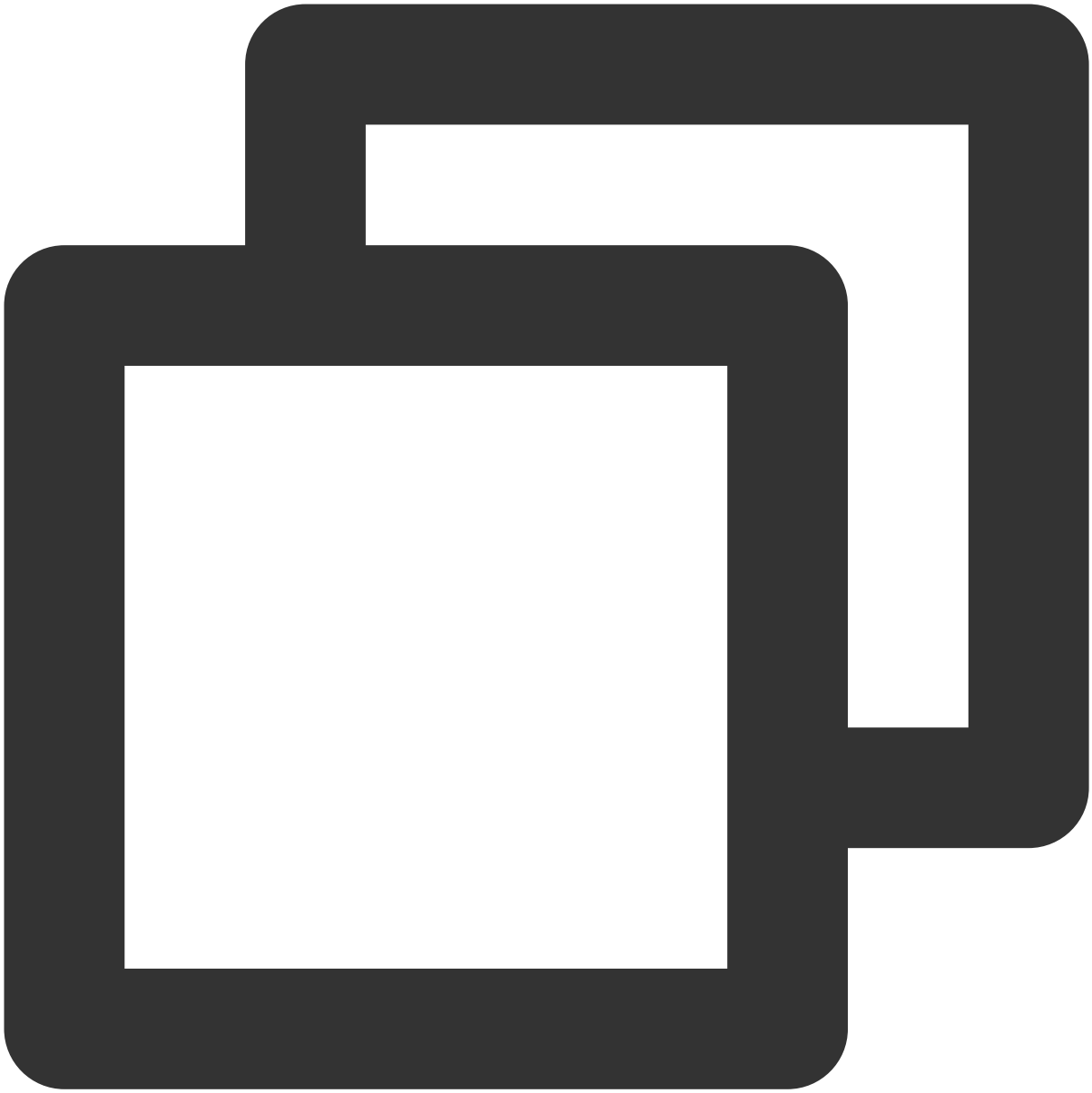
©2013-2022 Tencent Cloud. All rights reserved.

1. If you use a self-built/third-party DNS service, we recommend you not add the private network DNS provided by Tencent Cloud in `/etc/resolv.conf`. For more information, see Private Network Access.
2. If you use a self-built DNS service, you can also add the 4 domains above to your DNS. The domain and IP mappings are as follows:

Domain Name	IP
update2.agent.tencentyun.com	169.254.0.15
receiver.barad.tencentyun.com	169.254.0.4
custom.message.tencentyun.com	169.254.0.5
metadata.tencentyun.com	169.254.10.10

3. If the two methods above cannot work, you can add the following configuration to the `/etc/hosts` file on the server:

©2013-2022 Tencent Cloud. All rights reserved.



```
169.254.0.15 update2.agent.tencentyun.com
169.254.0.4 receiver.barad.tencentyun.com
169.254.0.5 custom.message.tencentyun.com
169.254.10.10 metadata.tencentyun.com
```

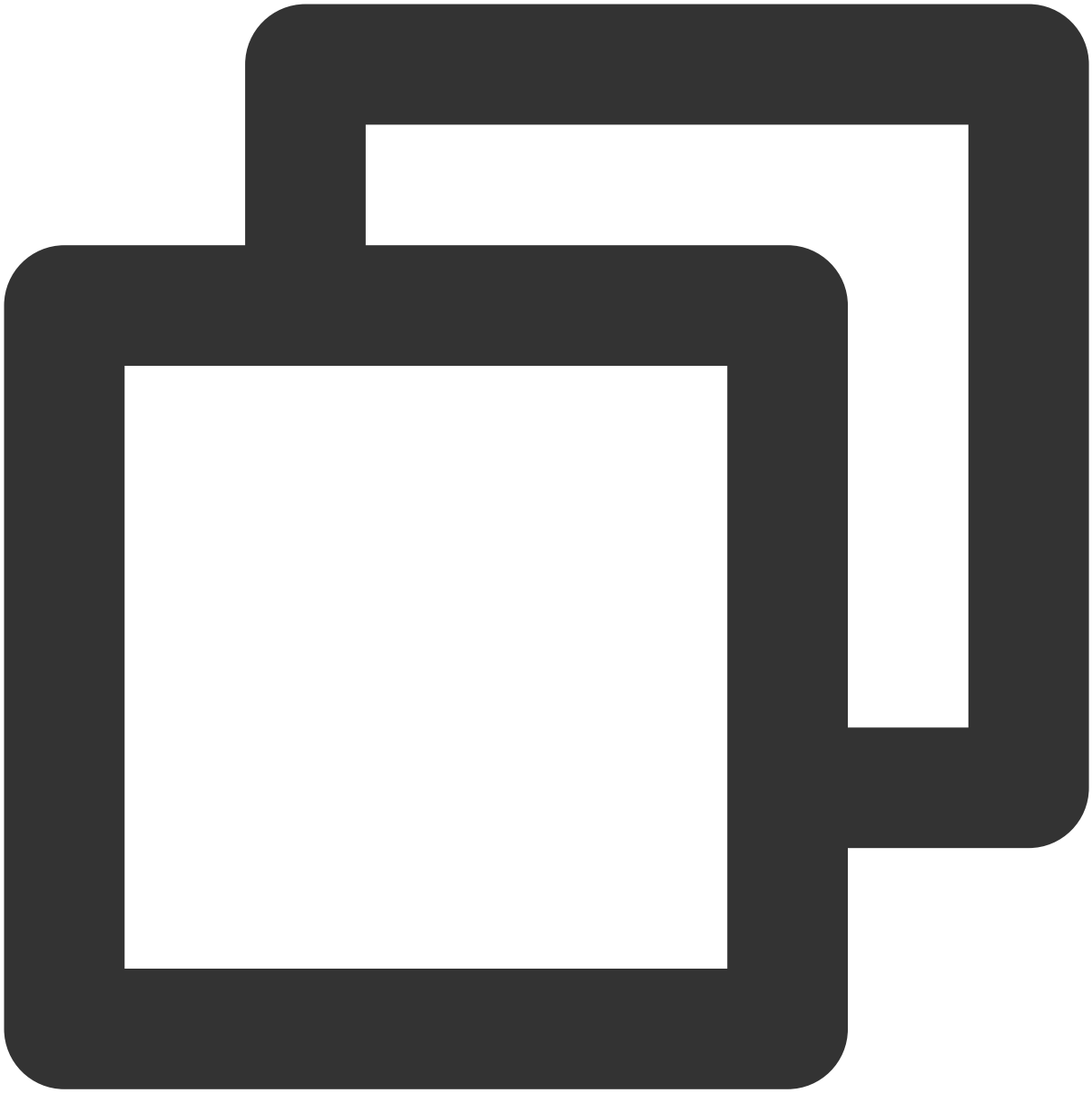
Note:

After the domain resolution issue is fixed, check whether the domains can be resolved properly. If yes, wait 3 minutes and then go to the CVM console to confirm whether there is monitoring data.

1. Check whether the reporting domains can be resolved properly.

Run the following commands to check whether these 4 domains can be resolved properly:

©2013-2022 Tencent Cloud. All rights reserved.



```
ping -n 1 update2.agent.tencentyun.com
ping -n 1 receiver.barad.tencentyun.com
ping -n 1 custom.message.tencentyun.com
ping -n 1 metadata.tencentyun.com
```

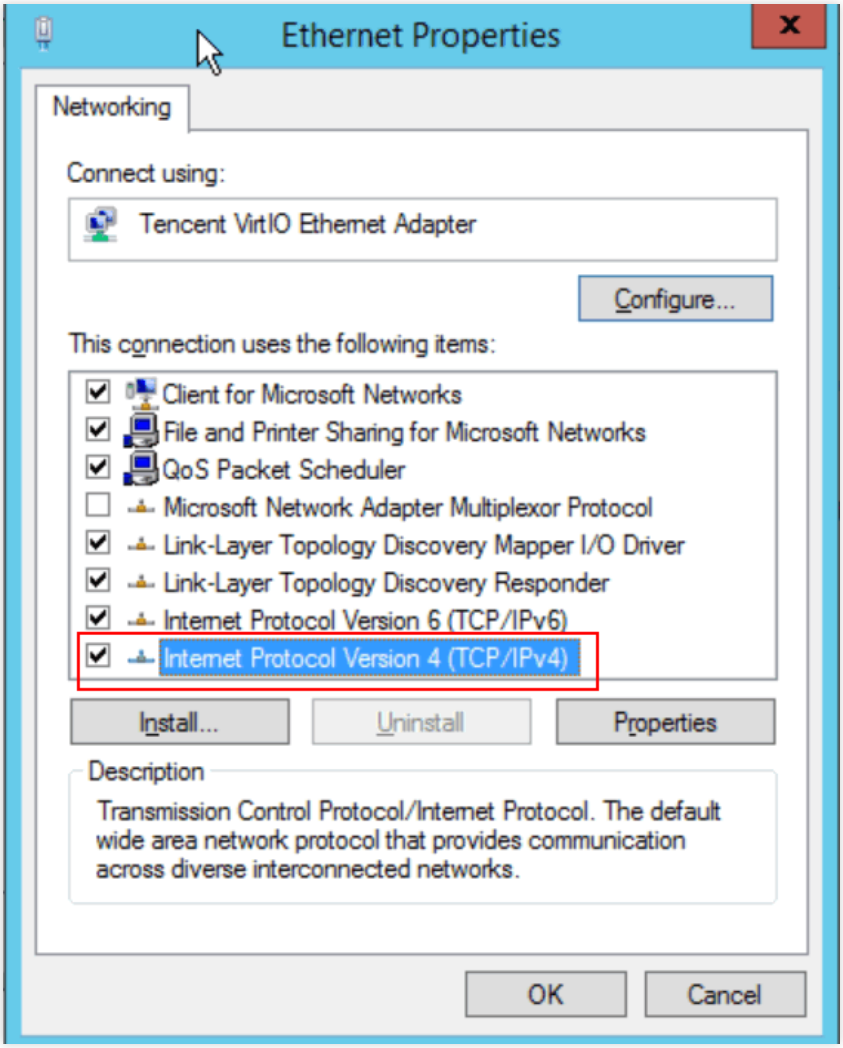
In normal cases, these 4 domains can be resolved on the CVM instance. If "host not found" is displayed, the domain resolution fails. In this way, you can fix the resolution as follows:

2. Fix DNS resolution.

Tencent Cloud provides reliable private network DNS servers in different regions. We recommend you not overwrite the default DNS configurations. If you need to modify them, fix the resolution for the 4 domains above as follows:

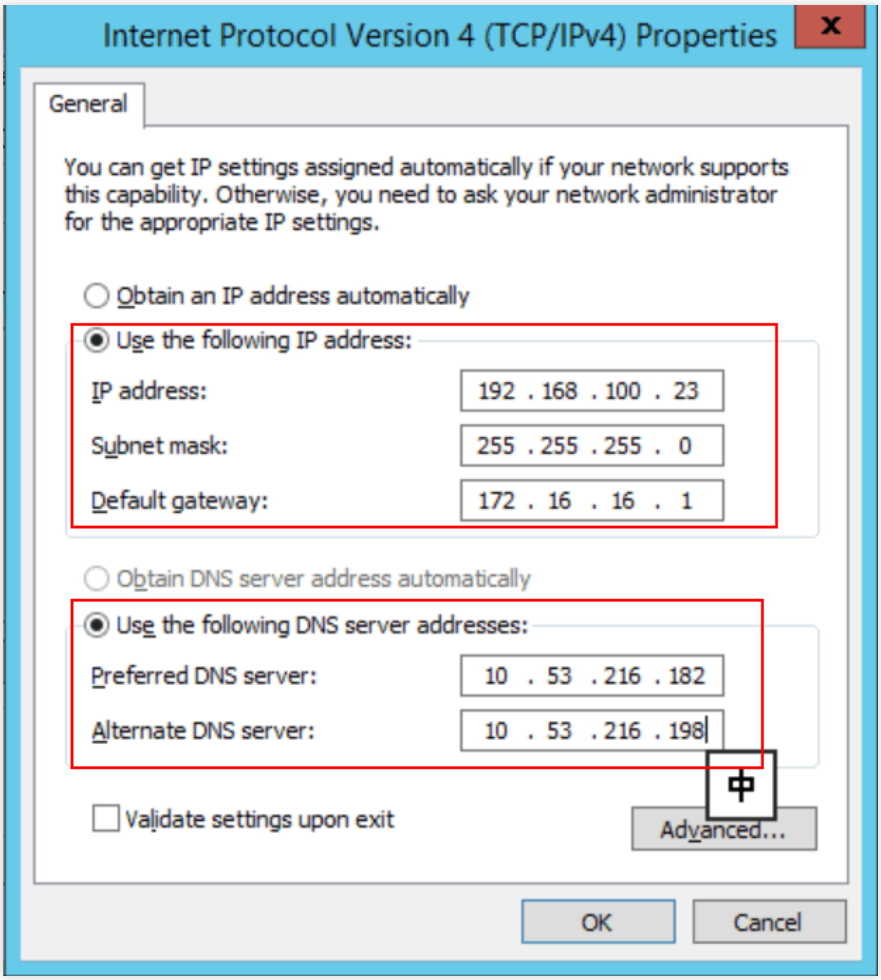
©2013-2022 Tencent Cloud. All rights reserved.

1. Log in to the Windows CVM instance.
2. On the operating system UI, open **Control Panel** > **Network and Sharing Center** > **Change adapter settings**.
3. Right-click **Ethernet** and select **Properties** to open the **Ethernet Properties** window.
4. In the **Ethernet Properties** window, double-click **Internet Protocol Version 4 (TCP/IPv4)** as shown below:



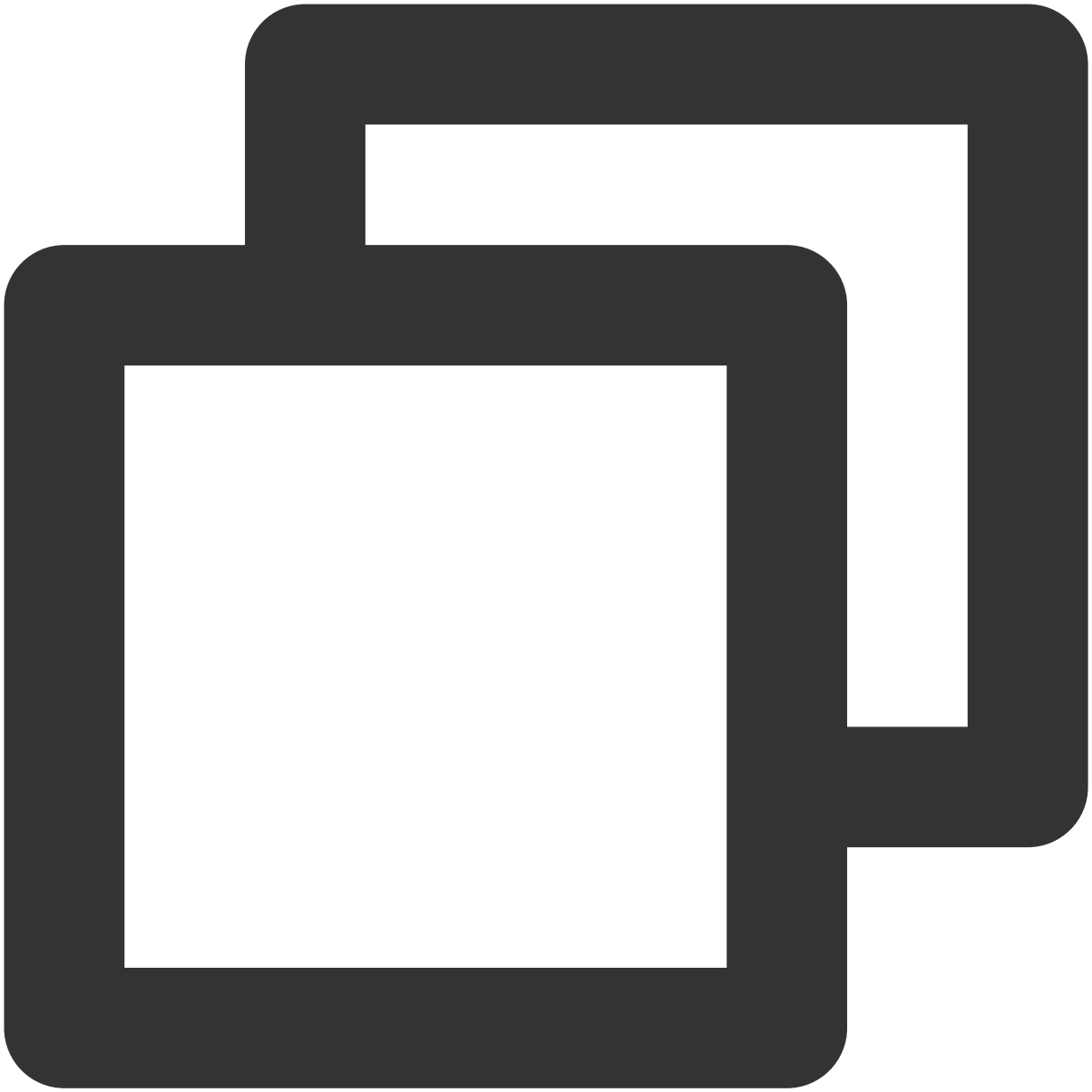
5. Select **Use the following DNS server addresses** and modify the DNS IP based on the corresponding region in the Private Network Access > Private Network DNS list. After the modification, click **OK**.

©2013-2022 Tencent Cloud. All rights reserved.



6. If the method above does not work, you can add the following configuration to the `C:\\Windows\\System32\\drivers\\etc\\hosts` file:

©2013-2022 Tencent Cloud. All rights reserved.



```
169.254.0.15 update2.agent.tencentyun.com
169.254.0.4 receiver.barad.tencentyun.com
169.254.0.5 custom.message.tencentyun.com
169.254.10.10 metadata.tencentyun.com
```

7. Run `services.msc` . Then, right-click the QCloud BaradAgent Monitor and QCloud Stargate Manager services and click **Restart the service**.

©2013-2022 Tencent Cloud. All rights reserved.

Note:

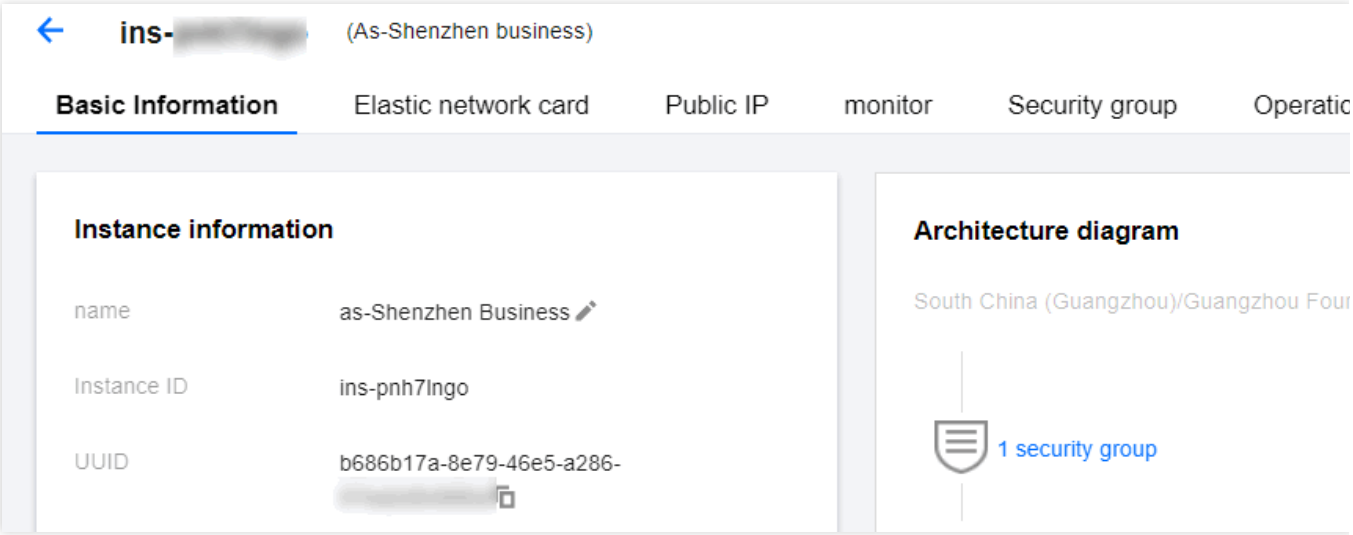
After fixing the UUID, wait 3 minutes and then go to the CVM console to confirm whether there is monitoring data.

If there is still no monitoring data after the restart, uninstall and reinstall the agents as instructed in Installing CVM Agents.

Step 3. Check whether the UUID is correct

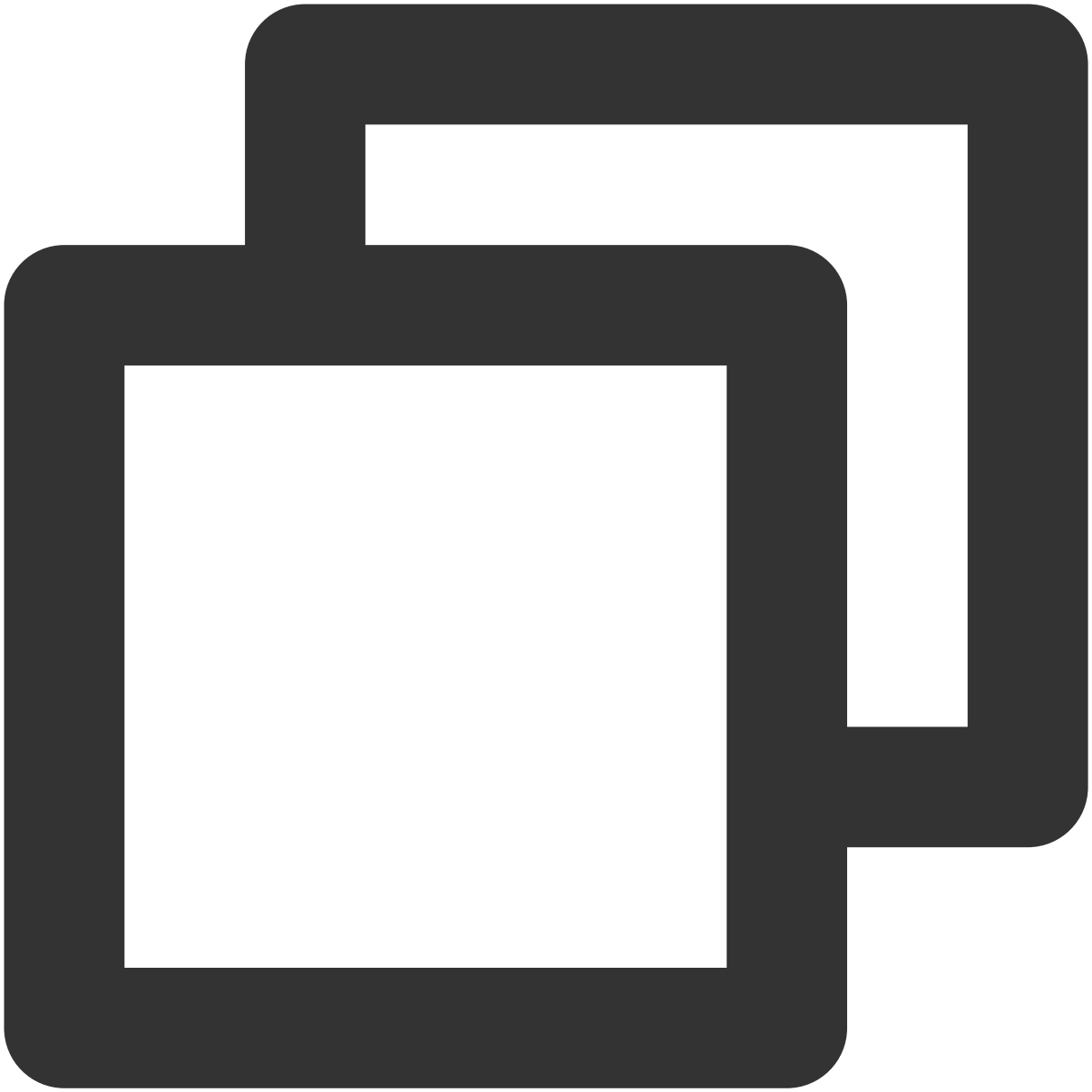
Currently, the incorrect UUID configuration issue occurs only in Linux OS. For details, see the following directions.

1. Log in to the CVM console and go to the instance detail page to view the UUID.



2. Log in to the CVM instance and run the following command to view the UUID:

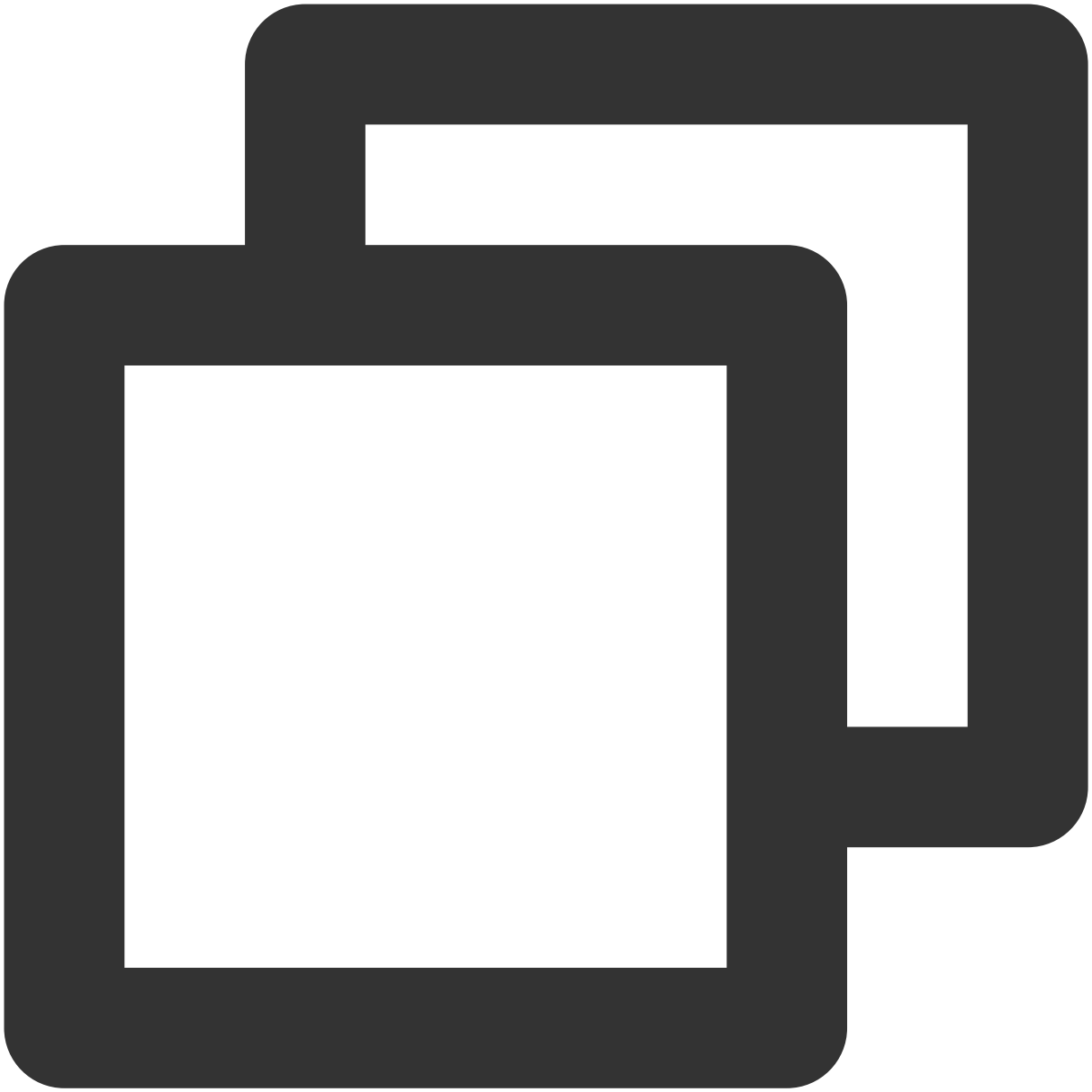
©2013-2022 Tencent Cloud. All rights reserved.



```
cat /sys/class/dmi/id/product_serial
```

If the UUID on the server is different from that displayed in the CVM console, run the following command as the root account to fix the UUID and restart the agents:

©2013-2022 Tencent Cloud. All rights reserved.



```
echo `cat /etc/uuid |awk -F '= ' '{print $NF}'` > /etc/uuid_to_serial; mount --bind
cd /usr/local/qcloud/stargate/admin
./restart.sh
cd /usr/local/qcloud/monitor/barad/admin
./stop.sh
./trystart.sh
```

Note:

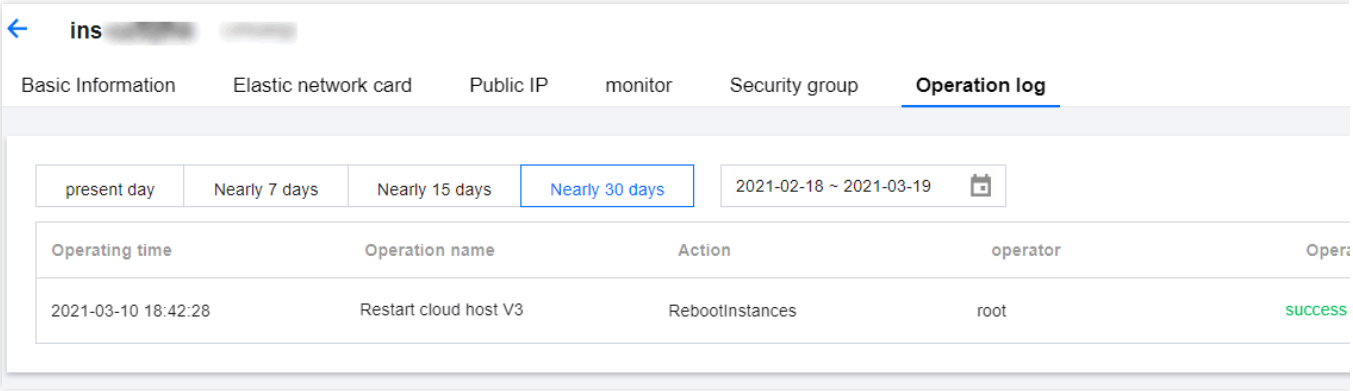
After fixing the UUID, wait 3 minutes and then go to the CVM console to confirm whether there is monitoring data.

©2013-2022 Tencent Cloud. All rights reserved.

Step 4. Check the CVM instance log

After the CVM instance is shut down, the instance's agents will be taken offline and thus no data will be reported. When you perform CVM Ops operations such as restart, upgrade, reinstallation, or image creation through the CVM console or through logging in to the CVM instance, the reporting of the CVM monitoring data may time out and the agents will be taken offline.

Troubleshooting: You can access the detail page of the CVM instance and view the operation logs to determine whether any relevant Ops operations were performed on the CVM instance at that time.



Step 5. Check the CVM instance load

The agents may fail to report data if the CPU usage, memory usage, or bandwidth utilization of the CVM instance is too high.

Troubleshooting methods:

High CPU usage: For detailed troubleshooting directions, see CVM CPU/Memory Usage Is Too High.

High memory usage: You can log in to the CVM instance or view the monitoring charts to check whether the CPU usage reaches 100%. If yes, upgrade the CVM configuration as needed.

High bandwidth utilization: For detailed troubleshooting directions, see CVM Bandwidth Utilization Is Too High.

©2013-2022 Tencent Cloud. All rights reserved.

No Alarm Is Received

Last updated：2024-01-27 17:35:59

This document introduces how to troubleshoot and resolve situations in which no alarms can be received.

Reasons for this Problem

Reason	Solution
The alarm policy has not been enabled	See Step 1 to enable the alarm policy
The alarm notification channel has not been configured or verified	See Step 2 to troubleshoot and enable or verify the alarm notification channel
No user has been added to the receiving group	See Step 3 to troubleshoot and add users to the receiving group
The alarm trigger conditions have not been met	See Step 4 to troubleshoot and check whether the alarm trigger conditions have been met

Troubleshooting

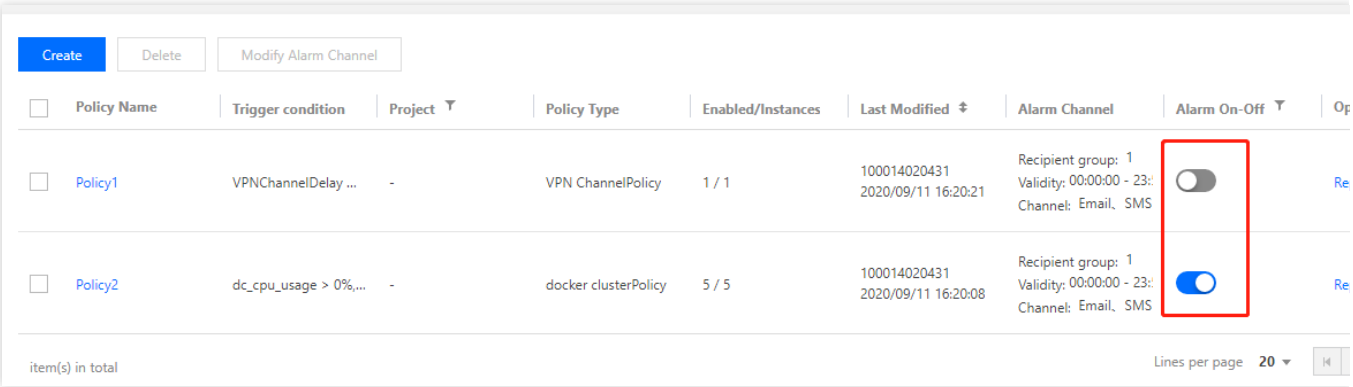
Step 1: Check whether the alarm policy is enabled

1. Access the Alarm Policy page in the Tencent Cloud Observability Platform console.
2. Check whether the alarm policy is enabled.

The alarm enable/disable button for policy 1 is gray in the figure below, indicating that the alarm policy has not been enabled yet. Click the gray button and then click **OK** to enable the policy.

The alarm enable/disable button for policy 2 is blue in the figure below, indicating that the alarm policy is enabled. Proceed to the steps below to continue troubleshooting.

©2013-2022 Tencent Cloud. All rights reserved.

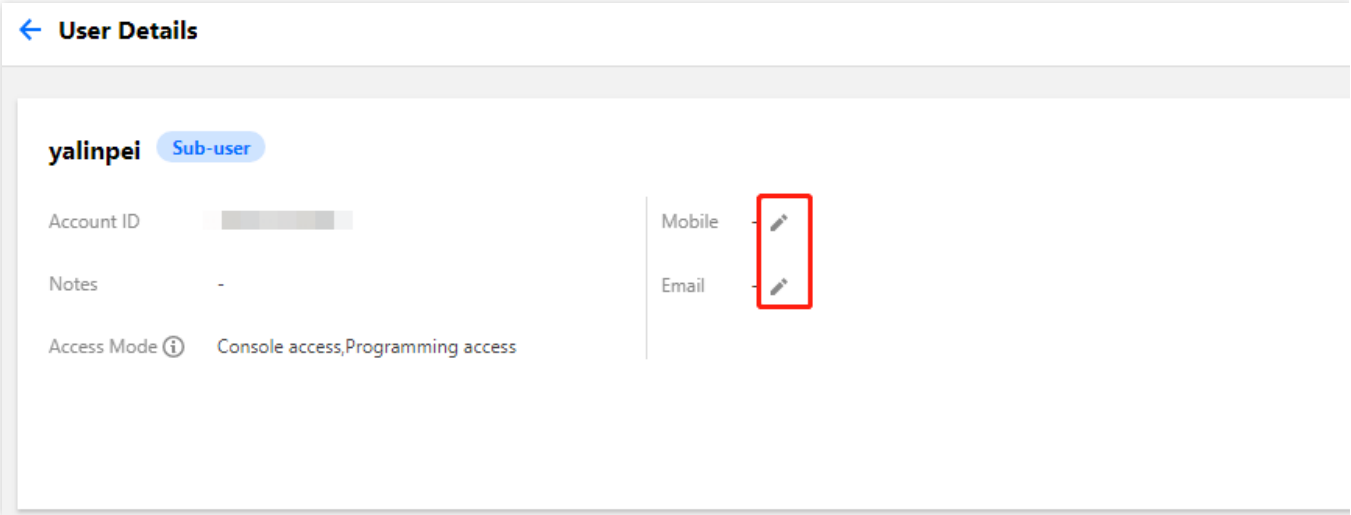


Step 2: Check whether the alarm channel has been configured/verified

1. Log in to the CAM console.
2. Click the corresponding user name in the user list to go to the user details page.

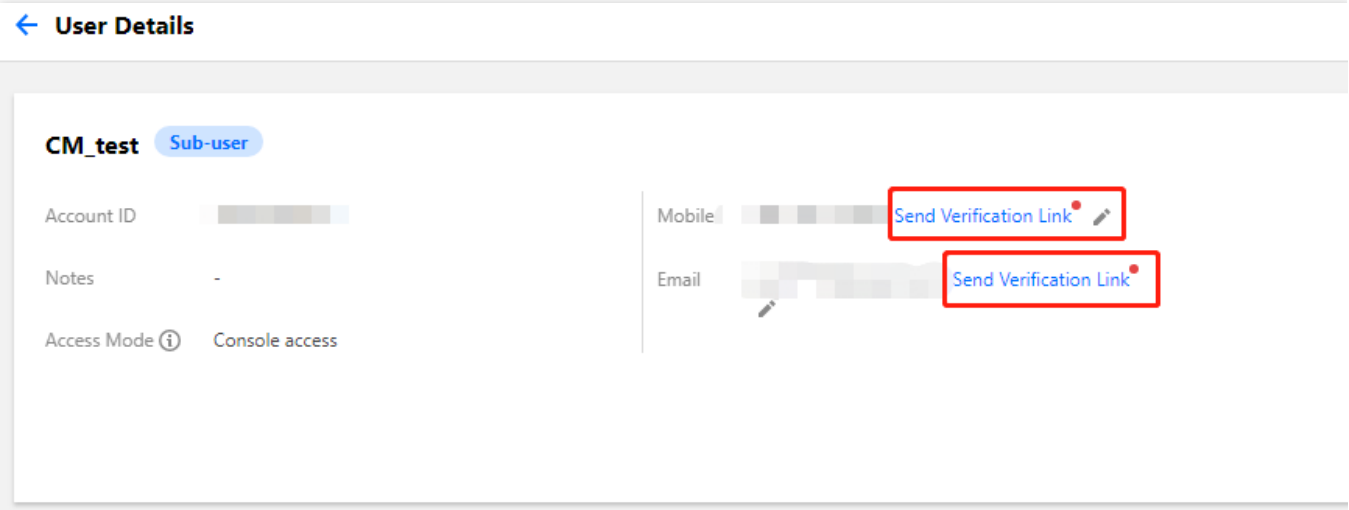
The alarm channel has not been configured: if the case shown in the figure below occurs, the alarm channel has not been configured. In this case, click

to configure a channel. After completing the configuration, verify the channel by referring to **The alarm channel has not been verified** below.



The alarm channel has not been verified: if the case shown in the figure below occurs, the alarm channel has not been verified. In this case, click the verification button.

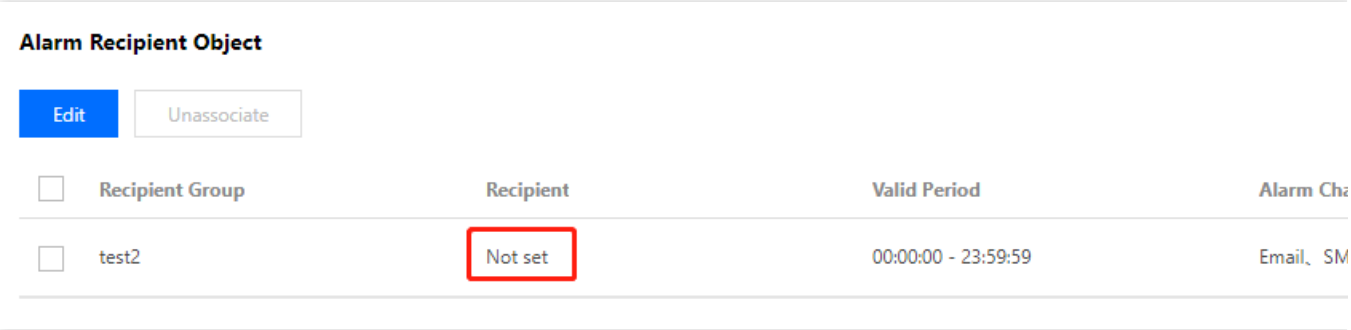
©2013-2022 Tencent Cloud. All rights reserved.



After the verification message or email is sent, go to the corresponding channel to complete the verification.
SMS verification: check the SMS inbox on your mobile phone and click the link in the received message to complete the verification.
Email verification: log in to your inbox and click the link in the received email to complete the verification.

Step 3: Check whether you have added users to the alarm receiving group

1. Go to the Alarm Policy page in the Tencent Cloud Observability Platform console.
2. Find the target alarm policy and click its name to go to the alarm policy management page.
3. Check whether the alarm recipients contain the user who has not received alarm notifications. If the alarm receiving group is "not configured" or does not contain the user, see Creating Alarm Recipient Groups to add the user to the alarm receiving group.



Step 4: Check whether the alarm trigger conditions have been met

Checking whether the metric alarm trigger conditions have been met

For example, if the metric is `CPU utilization` , the comparison operator is `>` , the threshold is `80%` , the measurement period is `5 minutes` , and the duration is `2 periods` , it means that the CPU utilization information is collected every 5 minutes. If the CPU utilization of a CVM is measured as above 80% **for 3**

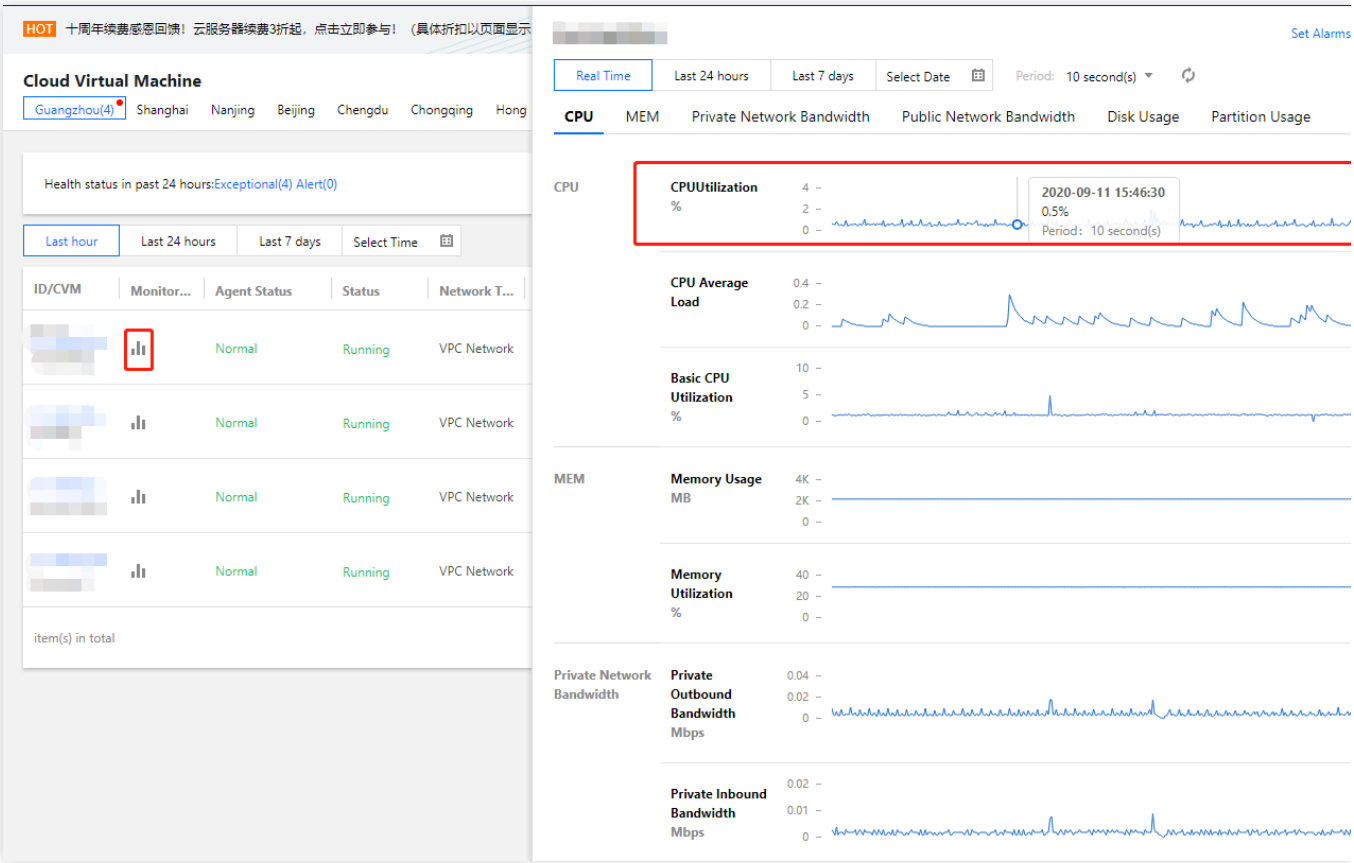
©2013-2022 Tencent Cloud. All rights reserved.

consecutive periods, an alarm will be triggered. Likewise, if the duration is set to N, an alarm will be generated if the metric monitoring data reaches the threshold for the N+1 periods.

You can log in to the Tencent Cloud Observability Platform console, select the corresponding Tencent Cloud service, and click

to view the metric monitoring data, and use the time filter to check whether the metric monitoring data has met the alarm trigger conditions. If no, no alarm notification will be sent.

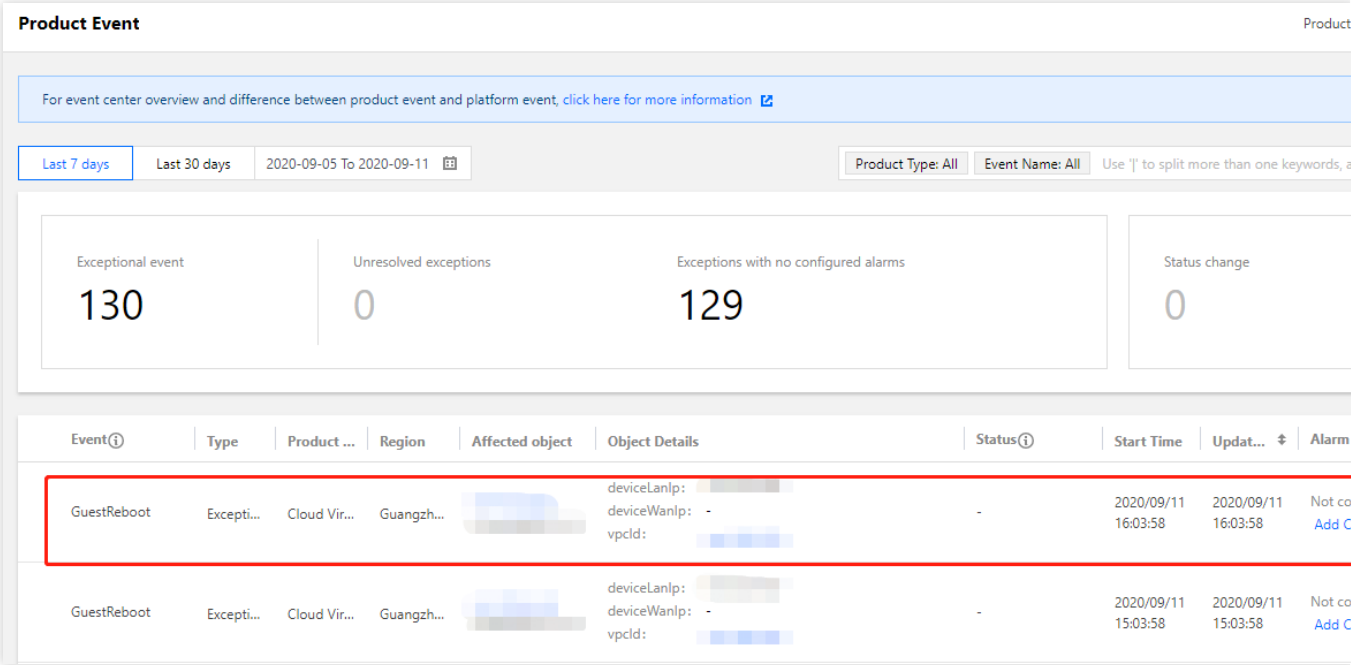
View the CPU utilization of the CVM, as shown in the figure below:



Checking whether the event alarm trigger conditions have been met

1. Go to the Product Events page in the Tencent Cloud Observability Platform console.
2. Check for event alarm records. If no records are found, the event alarm trigger conditions are not met, and therefore no alarm notifications are sent.

©2013-2022 Tencent Cloud. All rights reserved.



If the problem persists, submit a ticket.

©2013-2022 Tencent Cloud. All rights reserved.