Cloud Virtual Machine
Troubleshooting Issues
Product Documentation
Copyright Notice

©2013-2019 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

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 Issues

Instance Related Failures
  Shutdown or Restart CVM Failure
  Remote Connect Failure Due to Security Group Settings

About Linux Instances
  Unable to Log into a Linux Instance via SSH
  Linux Instance Login Failures
  Failing to log in to a Linux CVM due to high CPU and memory usage

About Windows Instances
  CVM Login Failure
  Requires network-level identity verification
  Connection to a Windows CVM through Remote Desktop was denied
  An authentication error occurred when you tried to log in to a Windows instance remotely
  Problems occurred when you tried to log in to a Windows CVM remotely on Mac
  Credentials Not Work
  Failed to log in to a Windows CVM due to high CPU and memory usage
  Failed to connect to a remote computer through Remote Desktop

Remote Login Failure Due To Port Issues

Network Namespace Creation Failure

CVM Login Failures

Login Failure Due to High Bandwidth Occupation

Login Failure Due to Server Isolation

Network Related Failures

International Linkage Latency

Website Access Failure

Slow Website Access

CVM Network Latency and Packet Loss

Instance IP Address Ping Failure

Domain Name Resolution Failure (CentOS 6.X System)

Performance Related Failures

High CPU Usage Rate (Linux System)

High CPU Usage Rate (Windows System)

High Bandwidth Usage Rate

Downloading Remote Desktop for Mac
Failure to shut down or restart a CVM is a rare event. Here are possible reasons for such failure and troubleshooting methods.

**Possible reasons for shutdown or restart failure**

1. Check the CPU/memory usage of the CVM. Excessive CPU utilization or memory exhaustion may cause shutdown or restart failure of the CVM on the console.

2. For Linux operating systems, you can check whether the ACPI management application is installed by running the `ps -ef | grep -w "acpid" | grep -v "grep"` command. Install the acpid module if no ACPI process exists.

3. For Windows operating systems, you can check whether such failure is caused by WindowsUpdate taking too long. Windows usually performs patch-related operations by the time when the system is about to shut down, and if the update takes a long time, shutdown/restart failure may occur.

4. In case of initial purchase of Windows, the initialization process is slightly longer due to the use of Sysprep for distributing images. Windows will ignore the shutdown/restart event until the initialization has been finished, thus causing CVM shutdown/restart failure.

5. If the operating system is broken due to some software installed or attacks from Trojans or other viruses, shutdown/restart failure may also occur.

**Forced shutdown/restart**

The forced shutdown/restart feature provided by Tencent Cloud can be used in case of multiple failed attempts to shut down or restart the CVM. This feature allows you to forcibly **shutdown/restart** the CVM, which however may cause data loss or file system damage.
Select **Forced Shutdown** in the shutdown operation window on the CVM console.
Select **Forced Restart** in the restart operation window on the CVM console.

### Restart Instance

You have selected 1 Instance, Learn More

<table>
<thead>
<tr>
<th>No.</th>
<th>Instance Name</th>
<th>Instance ID</th>
<th>Current Bandwidth</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Unnamed</td>
<td></td>
<td>1 Mbps</td>
</tr>
</tbody>
</table>

### Are you sure you want to restart the selected instances?

During restarting, this instance cannot work and your service may be affected.

- **Forced restart**

  Just like turning off the computer and then powering it on, forced restart may lead to data loss or damage to file system. This is allowed only when the instance cannot be restarted normally.

**OK**  **Cancel**
Remote Connect Failure Due to Security Group Settings

Last updated : 2020-02-11 11:34:22

This document introduces how to troubleshoot the problem where unable to connect remotely to a CVM due to security group configuration issues.

Diagnostic Tool

You can use the Port Verification to check whether the problem is caused by security group configurations.

1. Log in to the Port Verification.
2. In the Port Verification page, select the instance to check and click Quick Check. This is shown in the following figure:

If the check shows that the instance has ports that are not open to the Internet, you can use the
**Open All Ports** function to open all the commonly used ports of the CVM to the Internet, and then try to remotely connect again.

### Modifying Security Group Configurations

If you do not want to use the **Open All Ports** function to open all the commonly used ports of the CVM to the Internet, or you need a custom remote login port, you can also use the custom configuration of the inbound and outbound rules of the security group to resolve the inability to log in issue.
This document uses the CVM with CentOS 7.5 operating system as an example to show you how to troubleshoot the problem where a Linux instance cannot be logged in to via SSH.

**Problems**

- Log in to a Linux instance through SSH.

**Locating and troubleshooting the issues**

**Step 1: view the security group rule configuration**

**Steps**: Check by using the Port verification tool.

- If you determine the problem of setting the security group port, you can use the [open all] function Open to Internet port in the tool. You can also customize security group rules according to your actual needs.
- If there is no problem with the security group port setting, execute Next.

**Step 2: view the sshd service port**

- Log in to a Linux instance through SSH.

2. On the operating system UI, run the following command to check whether a port is listened on by the SSH daemon (SSHD) service:

```
netstat -tnlp | grep sshd
```

- If the SSHD service has started, send feedback by Submit Ticket.

```
tcp 0 0 0.0.0.0:22 0.0.0.0:* LISTEN 1015/sshd
```
If no result is returned, the SSHD service may haven't started yet. Go to **Step 3**.

**Step 3: check whether the sshd service is Launch**

9. Run the following command to check whether the SSHD service has started.

```
systemctl status sshd.service
```

- If the SSHD service has started, send feedback by **Submit Ticket**.
- If the SSHD service has not started, run the following command to start the SSDH service and log in to the Linux instance again via SSH.

```
systemctl start sshd
```

If you still cannot connect to your instance after performing these steps, we recommend you send feedback by **Submit Ticket**.
This document describes possible causes of Linux instance login failures and troubleshooting methods, helping you detect, locate and resolve problems.

Possible Causes

The primary causes of Linux instance login failures include:

- SSH key problems
- Password problems
- Bandwidth utilization too high
- Server workload too high
- Remote port configuration exception
- Incorrect security group rules

If your problem cannot be checked using the self-diagnose tool, we recommend you Log in to the CVM via VNC And troubleshoot step by step.

Troubleshooting

Logging in via VNC

If you cannot use the standard method (Webshell) or remote login software to log into a Linux instance, you can use Tencent Cloud VNC to login and locate the problem causes.

1. Log in to the CVM Console .
2. In the instance management page, select the instance to be logged in to and click Log In . This is shown in the following figure:
3. In the **Log into Linux instance** Window that pops up, select **Alternative login methods (VNC)**, and click **Log In Now**.

   During login, if you forget the password of this instance, you can reset it in the console. For more information, see **Reset Instance Password**.

4. Enter the username and password in the dialog box that pops up to complete the login process.

**Login failures due to SSH problems**

**Fault phenomenon**: **Log in to the Linux instance using SSH** Indicates that the connection cannot be made or that the connection fails.

**Processing steps**: referenc **Unable to log in to Linux instance through SSH** Conduct a canvassing.

**Login failures due to password problems**

**Problem**: You forget the password, enter it incorrectly or password reset failed resulting in login failures.

**Troubleshooting**: Reset the password for this instance in the **Tencent Cloud Console**, and restart the instance.

**Steps**: For information about how to reset the password of an instance, see **Reset Instance Password**.

**Bandwidth utilization too high**

**Problem**: The self-diagnosis tool shows that bandwidth utilization is too high.

**Steps**:

1. Log in to the instance via **VNC Login**.
2. Refer to **Unable to log in due to high bandwidth consumption** To view the bandwidth usage of the instance and handle failures
Server workload too high

**Problem**: The self-diagnosis tool or Cloud Monitor shows that server CPU workload is too high, and the system is unable to perform remote connection or access is slow.

**Possible Causes**: Viruses, Trojans, third-party anti-virus software, application exceptions, driver exceptions, and software backend automatic updates may lead to high CPU usage rate, causing CVM login failures or slow access.

**Steps**:

1. Log in to the instance via VNC Login.
2. Refer to Linux instance: unable to log in due to high CPU and memory occupancy To locate high-load processes in the job manager

Remote port configuration exception

**Problems**: The remote port cannot connect, remote access port is not the default port or has been modified, or port 22 is not open.

**Diagnosis**: Whether the public IP of the instance can be pinged, use the `telnet` Command to check whether the port is open.

**Processing steps** For specific operation, please refer to Port problem makes it impossible to log in remotely.

Improper security group rules

**Problems**: The self-diagnosis tool shows that the security group rule configuration is improper, leading to login failures.

**Steps**: Check by using the Port verification tool.

If the problem is caused by security group configurations, you can use the Open All Tools To open all ports.
If you need to customize security group rules, see Security Group Operations For reconfiguration.

Other Solutions

If you still cannot log into the Linux instance using above-mentioned troubleshooting methods, please save your self-diagnosis results and Submit Ticket.
Failing to log in to a Linux CVM due to high CPU and memory usage

Last updated : 2019-10-30 10:20:59

Scenario

This document describes how to investigate and solve issues such as failure to log in to a Linux CVM due to high CPU and memory usage.

Directions

Logging in and viewing the system load

1. Log in to the CVM in different ways depending on your actual needs.
   - Log in to the Linux CVM via third party software remotely.
     - When the Linux CVM has a high CPU load, you may fail to log in.
   - Log in to CVM via VNC.
     - Log in to the CVM console > click Log in in the right operation column > log in with alternative login methods (VNC).
     - When the Linux CVM has a high CPU load, you may be able to log in via the console normally.

2. Execute the following command to view the system load. View the %CPU column and the %MEM column and identify which processes consume more resources.

```
  top
```

Terminating processes
1. Compare the resource consumption of different processes and record the PIDs of processes which need to be terminated.

2. Enter \texttt{k}.

3. Enter the PID of the process which needs to be terminated, and press \texttt{Enter} to terminate it as shown below:

   For example, you need to terminate a process whose PID is 23.

   \begin{center}
   \includegraphics[width=\textwidth]{snippet.png}
   \end{center}

   If \texttt{kill PID 23 with signal [15]}: appears after you press \texttt{Enter}, press \texttt{Enter} again to keep the default settings.

4. If the operation is successful, the following message, \texttt{Send PID 23 signal [15/sigterm]} will show up. Press \texttt{Enter} to confirm the termination.

\textbf{Low CPU usage but high load average}

\textbf{Problem Description}

The load average is an indicator of CPU load. A high load average indicates a long queue of processes waiting to run.
Running `top` returns very low CPU usage but very high load average as shown below.

```
top - 19:46:57 up 27 days, 5:33, 1 user, load average: 23, 22, 23
Tasks: 99 total, 1 running, 93 sleeping, 0 stopped, 0 zombie
%CPU(s): 0.3 us, 0.0 sy, 0.0 ni, 99.7 id, 0.0 wa, 0.0 hi, 0.0 si, 0.0 st
KiB Mem: 1016656 total, 950428 used, 66228 free, 170148 buffers
KiB Swap: 0 total, 0 used, 0 free. 452740 cached Mem
```

Solution

Execute the following command to view process states and check whether there are processes in D state as shown below:

```
ps -axjf
```

Processes in D state are in uninterrupted sleep. Processes in the state cannot be terminated nor exit by itself. If there are many processes in D state, you can solve the problem by restoring resources on which the processes depend or restarting the system.

**kswapd0 process uses much CPU**

**Problem Description**

Linux manages memory with the paging mechanism, and it also sets aside a portion of the disk for virtual memory. kswapd0 is the process responsible for page replacement in the virtual memory management of Linux system. When there is not enough system memory, kswapd0 will frequently replace pages, which is very CPU consuming. That is why the process uses a lot of CPU.

**Solution**

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

```
top
```
2. Observe the state of the kswapd0 process.
   If the process is not sleeping, has run for a long time, and has been using a lot of CPU, please take Step3 to check the memory usage rate.

3. Execute commands, such as `free`, `ps` to check how much memory is being used by processes in the system.
   Restart the system or terminate the processes that are safe but unnecessary based on the memory usage rate.

If the problem is not solved, please refer to High CPU usage rate (Linux system) for more details.
If you cannot connect to an instance, you are recommended to conduct troubleshooting as follows:

**Port**

**Problem:**
Remote connection to the port fails.

**Solution:**
This problem is probably caused by non-default port used for remote access or inconsistent port settings.

**Excessive CPU/Memory Utilization**

**Problem:**
Login to the CVM fails, the service response slows down, or the instance disconnects suddenly.

**Solution:**
It may be caused by high CPU or memory load. Please check the resource utilization.
For Windows CVMs, please see Login Failure due to Excessive CPU/Memory Utilization in Windows.
For Linux CVMs, please see Login Failure due to Excessive CPU/Memory Utilization in Linux.

**Isolated Public Network**

**Problem:**
The CVM is partially isolated in case of violations or risks.

**Solution:**
For more information, please see Remote Connection Failure due to Isolated Public Network.

**High Bandwidth Usage of Public Network**
Problem: Login fails due to full or high bandwidth usage.

Solution: For more information, please see Login Failure due to High Bandwidth Usage of Public Network.

Security Group Configuration

Problem: Server telnet connection fails, and the problem persists after the firewall and the ENI configurations are checked and the system rolls back.

Solution: For more information, please see Remote Connection Failure due to Security Group Configuration.

Password Cannot Be Used after Key Is Associated

Problem: The CVM cannot be logged in to by password after it is associated with a key. Firewall and ENI IP configurations are correct.

Solution: After the CVM is associated with the key, login by user name and password is disabled by default for the CVM SSH service. Use the key to log in to the CVM. For more information on login by key, please see SSH Key.

Network Level Authentication for Remote Login

Problem: Connection to remote computers through Windows Remote Desktop Connector fails sometimes.

Solution: For more information, please see Network Level Authentication for Remote Login.

Login by Password Through xshell Failed
Problem:
The CVM cannot be logged in to by password through xshell.

Solution:
You have chosen to log in by key when installing the system. For how to use the key, please see SSH Key. If you need to log in by password, you can choose this option when reinstalling the system, or modify the sshd configuration file.
This document describes how to manage alarm prompts such as network level authentication when connecting to a Windows instance.

Problems

When using Windows remote desktop, you cannot connect to a remote computer and a prompt appears, requiring network level authentication.

Troubleshooting

The following operations take Windows Server 2016 as an example.

Logging in to the CVM using VNC

1. Log in to the CVM Console.
2. In the instance management page, find the target CVM instance, and click Log In. This is shown in the following figure:
3. In the **Log into Windows instance** window that pops up, select **Alternative login methods (VNC)**, and click **Log In Now** to log in to the CVM.

4. In the login window that pops up, select **Send Remote Command** in the top left corner, and click **Ctrl-Alt-Delete** to enter the system login interface as shown below:

![System login interface](image)

**Modifying the registry**

1. In the operating system interface, click 🔍, enter `regedit`, and press **Enter** to open the Registry Editor.

2. In the left-side navigation tree, expand the following directories: **Computer** > **HKEY_LOCAL_MACHINE** > **SYSTEM** > **CurrentControlSet** > **Control** > **Lsa**, and in the right-
side window, find **Security Packages**. This is shown in the following figure:

3. Double click **Security Packages** to open the **Edit Multi-String** dialog box.
4. In the **Edit Multi-String** dialog box, add **tspkg** in **Value Data**, and click **OK**. This is shown in the following figure.
5. In the left-side navigation tree, expand the following directories: **Computer > HKEY_LOCAL_MACHINE > SYSTEM > CurrentControlSet > Control > SecurityProviders**, and in the right-side window, find **SecurityProviders**. This is shown in the following figure:

![Registry Editor](image)

6. Double click **SecurityProviders** to open the **Edit Multi-String** dialog box.
7. Add `, credssp.dll` at the end of **Value Data** field in **Edit Multi-String** dialog box. Click **OK**. This is shown in the following figure:

![Edit String](image)

8. Close the registry editor and restart the instance. You can now log in remotely.
Connection to a Windows CVM through Remote Desktop was denied

Last updated : 2020-02-25 11:40:24

Problems

Problem 1
When trying to connect to a Windows instance via Remote Desktop from Windows, you get the following message: "The connection was denied because the user account is not authorized for remote login."

Problem 2
When trying to connect to a Windows instance via Remote Desktop from Windows, you get the following message: "To sign in remotely, you need the right to sign in through Remote Desktop Services. By default members of the Remote Desktop Users group have this right. If the group you're in doesn't have the right, or if the right has been removed from the Remote Desktop Users group, you need to be granted the right manually."

Problem Analysis

The user is not allowed to log in to the Windows instance via Remote Desktop Connections:

Solution

- If you encounter the Problem 1 When trying to connect to a Windows instance through Remote Desktop, you will need to add the user account to the list of accounts that are allowed by the Windows instance to log in through Remote Desktop Services. For details, see Configuring the right that allows remote login.
- If you encounter the Problem 2 Trying to connect to a Windows instance through Remote Desktop, you will need to remove the user account from the list of accounts that are denied by the Windows instance to log in through Remote Desktop Services. For details, see Configuring the right that denies remote login.
Directions

Logging in to the CVM using VNC

1. Log in to the CVM Console.
2. In the Instance page, find the CVM and click Log in.
3. In the "Log into Windows Instance" window, select "Alternative login methods (VNC)", click Log In Now To log in to the CVM.
4. In the login window, select "Send CtrlAltDel" in the top left corner, and click Ctrl-Alt-Delete To enter the system login interface.

Configuring the right that allows remote login

The following operations take Windows Server 2016 as an example.

1. In the operating system interface, click , enter Gpedit.msc, and press Enter To open the Local Group Policy Editor.
3. In the Allow log on through Remote Desktop Services Properties Window, check whether the user account you want to use for remote login is on the user list of "Allow log on through Remote Desktop Services".
   - If the user is not on the list, please take Step 4.
   - If the user is on the list, please Submit a ticket.
4. Click Add User or Group To open the "Select User or Group" window.
5. Enter the account you want to use for remote login and click OK.
6. Click OK And close the Local Group Policy Editor.
7. Restart the instance and try again to connect to the Windows instance with the account through Remote Desktop.

Configuring the right that denies remote login

The following operations take Windows Server 2016 as an example.
1. In the operating system interface, click , enter `Gpedit.msc`, and press `Enter` To open the Local Group Policy Editor.

2. In the left navigation tree, choose **Computer Configuration > Windows Settings > Security Settings > Local Policies > User Rights Assignment**, and double-click **Deny log on through Remote Desktop Services**

3. In the **Deny log on through Remote Desktop Services Properties** Window, check whether the user account you want to use for remote login is on the user list of "Deny log on through Remote Desktop Services".

- If the user is on the list, remove the user account from the list and restart the instance.
- If the user is not on the list, please **Submit a ticket**.
An authentication error occurred when you tried to log in to a Windows instance remotely

Last updated : 2019-10-17 14:23:36

Problem Description

When trying to log in to a Windows instance via Remote Desktop Connections, you get the message as shown below:

- “An authentication error has occurred. The token supplied to the function is invalid.”
- “An authentication error has occurred. The function requested is not supported.”

Problem Analysis

Microsoft published a security update in Mar 2018 which can address a remote code execution vulnerability in Credential Security Supporting Program protocol (CredSSP) by correcting how CredSSP validates requests during the authentication process. Both the client and server need to be updated, or the error described above may occur.

As shown in the figure above, in the following three scenarios, remote connection will fail.

- Scenario 1: The client is unpatched; the server is installed with the security update; the policy setting is “force updated clients”.
- Scenario 2: The server is unpatched; the client is installed with the security update; the policy setting is “force updated clients”.
- Scenario 3: The server is unpatched; the client is installed with the security update; the policy setting is “mitigated”.

Solution

If you only need to update the client locally, please directly use Solution 1: Install the security update (recommended).
Log in to the CVM using VNC

1. Log in to the CVM Console.

2. In the Instance page, find the CVM and click Log in as shown below:

3. In the “Log into Windows Instance” window, select “Alternative login methods (VNC)”, click Log In Now to log in to the CVM.

4. In the login window, select “Send CtrlAltDel” in the top left corner, and click Ctrl-Alt-Delete to enter the system login interface as shown below:

Solution 1: Install the security update (recommended)

Installing the security update can update the unpatched client/server. For updates for different systems, please refer to CVE-2018-0886 | CredSSP remote code execution vulnerability. Here we take Windows Server 2016 as an example.

In other operating systems, you may use the following operations to go to Windows update:

- Windows10: > Settings > Update and Security
- Windows 7: > Control Panel > System and Security > Windows Update

1. In the operating system interface, click , select Settings as shown below:

2. In the Settings window, select Update and Security as shown below:

3. In the “Update and Security” page, select Windows Update and click Check for updates as shown below:

4. Click Install updates.

5. After the installation is completed, restart the instance to finish the update.

Solution 2: Modify the policy setting
In a CVM installed with the security update, set the **Encryption Oracle Remediation** policy to "vulnerable". Here we take Windows Server 2016 as an example. Please follow the steps below:

1. In the operating system interface, click 🔍, enter `gpedit.msc`, and press Enter to open the Local Group Policy Editor.

   You can also use the shortcut “Win+R” to open the Run box.

2. In the left navigation tree, select **Computer Configuration** > ** Administrative Templates** > ** System** > **Credentials Delegation**, and double-click **Encryption Oracle Remediation** as shown below:

3. In the “Encryption Oracle Remediation” window, select **Enabled**, and set **Protection Level** to **Vulnerable** as shown below:

4. Click **OK** to complete the configuration.

**Solution 3: Modify the registry**

1. In the operating system interface, click 🔍, enter `regedit`, and press Enter to open the Registry Editor.

   You can also use the shortcut “Win+R” to open the Run box.

2. In the left navigation tree, select **Computer** > **HKEY_LOCAL_MACHINE** > **Software** > **Microsoft** > **Windows** > **CurrentVersion** > **Policies** > **System** > **CredSSP** > **Parameters** as shown below:

   If the directory path does not exist, please create one manually.
3. Right-click **Parameters**, select **New > DWORD (32-bit) value**, and name the file "AllowEncryptionOracle".

4. Double-click the newly created “AllowEncryptionOracle” file, set “Value data” to “2”, and click **OK** as shown below:

5. Restart the instance.

**Related Documentation**

- [CVE-2018-0886 | CredSSP remote code execution vulnerability](#)
- [CredSSP updates for CVE-2018-0886](#)
Problems occurred when you tried to log in to a Windows CVM remotely on Mac

This document describes the common problems you may encounter when remotely logging in to a Windows CVM on Mac through Microsoft Remote Desktop and how to solve them.

Problem Description

- When trying to remotely log in to a Windows CVM through Microsoft Remote Desktop, you get the message: “The certificate couldn’t be verified back to a root certificate.”

- When using Remote Desktop Connection on Mac, you get the message: “Remote Desktop Connection cannot verify the identity of the computer that you want to connect to.”

Troubleshooting

The following operations take Windows Server 2016 as an example.
Logging in to the CVM using VNC

1. Log in to the CVM Console.

2. In the Instance page, find the CVM and click Log in as shown below:

3. In the “Log into Windows Instance” window, select “Alternative login methods (VNC)”, click Log In Now to log in to the CVM.

4. In the login window, select “Send CtrlAltDel” in the top left corner, and click Ctrl-Alt-Delete to enter the system login interface as shown below:

Modifying the local group policy of the instance

1. In the operating system interface, click , enter gpedit.msc, and press Enter to open the Local Group Policy Editor.

   You can also use the shortcut “Win+R” to open the Run box.

2. In the left navigation tree, select Computer Configuration > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Session Host > Security, double click Require use of specific security layer for remote (RDP) connections as shown below:

3. In the “Require use of specific security layer for remote (RDP) connections” window, select Enabled, and set the Security Layer to RDP as shown below:

4. Click OK to complete the configuration.

5. Restart the instance and try to make the connection again. If the connection fails again, please submit a ticket.
Credentials Not Work

Last updated: 2020-03-06 12:20:05

Issue Description

The following error message appears when trying to log in to a Windows CVM remotely via RDP protocol, such as using MSTSC.
Your credentials did not work. The credentials that were used to connect to XXX.XXX.XXX.XXX did not work. Please enter new credentials.

Instructions

These instructions use Windows Server 2012 as an example. Different versions of Windows might have slightly different instructions.
Follow these instructions carefully and try to connect to your Windows CVM after each step. If one did not work, proceed to the next.

Step 1: Modify Network Access Policy
1. Log in to the Windows instance using VNC.

2. Once logged in, click to open a Windows PowerShell window.

3. In the Windows PowerShell window, enter `gpedit.msc` and press Enter to open the Local Group Policy Editor.

4. Use the navigation pane on the left to navigate to Computer Configuration > Windows Settings > Computer Settings > Security Options.

5. Locate and open Network access: Sharing and security model for local accounts under Security Options, as shown in the following image:

![Local Group Policy Editor](image)

6. Select Classic - local users authenticate as themselves and click OK, as shown in the following image:
7. Check whether you can connect to your Windows CVM now.
   - Yes. Problem solved.
   - No. Proceed to Step 2 Modify Credentials Delegation

**Step 2: Modify Credentials Delegation**

1. Open Local Group Policy Editor. In the left navigation pane, navigate to **Computer Configuration > Administrative Templates > System > Credentials Delegation**.
2. Locate and open **Allow delegating saved credentials with NTLM-only server authentication** under **Credentials Delegation**, as shown in the following image:
3. Select **Enable**. Click **Show...** under **Options** and enter `TERMSRV/*`. Click **OK**, as shown in the following image:
4. Click **OK**.

5. Click **Show** to open a Windows PowerShell window.

6. In the Windows Powershell window, enter `gpupdate /force` and press **Enter** to update group policy, as shown in the following image:
7. Check whether you can connect to your Windows CVM now.
   - Yes. Problem solved.
   - No. Proceed to Step 3 Configure Local Credentials

**Step 3: Configure Local Credentials**

1. Click and navigate to **Control panel > Users and accounts**. Select **Manage Windows credentials** under **Credential manager**. The Windows credential window then appears, as
2. Check to see if there is an entry for the credentials you used to log in to Windows CVM.
   - No. Follow the next step to add it.
   - Yes. Proceed to Step 4 Turn Off Password Protected Sharing

3. Click **Add Windows credentials**. The **Add Windows credentials** window then appears, as shown in the following image:
4. Input the IP of the CVM, the username you use to log in to the Windows CVM and the corresponding password. Click **OK**.

5. Check whether you can connect to your Windows CVM now.
   - Yes. Problem solved.
   - No. Proceed to Step 4 Turn Off Password Protected Sharing

**Step 4: Turn off password protected sharing**

1. From Desktop, click and navigate to **Control panel > Network and sharing center > Change advanced sharing settings**. The **Change advanced sharing settings** page then
appears, as shown in the following image:

2. Expand **All networks** and select **Turn off password protected sharing** under **Password protected sharing**. Click **Save changes**.

3. Check whether you can connect to your Windows CVM now.
   - Yes. Problem solved.
   - No. Please submit a ticket.
Failed to log in to a Windows CVM due to high CPU and memory usage

Last updated: 2019-10-16 17:18:52

Scenario

This document describes how to investigate and solve the problem of failing to log in to a Windows CVM due to high CPU and memory usage.

Directions

Logging in to the CVM using mstsc

1. On your local computer, use the Windows+R shortcut to open the Run box.
2. Enter mstsc and press Enter to open the “Remote Desktop Connection” interface.
3. In the “Remote Desktop Connection” window, enter the public IP address of the CVM and the login password to log in to the CVM.

If the CVM has a high load average, you will not be able to establish a remote connection. You will have to log in to the CVM using VNC. You can do so by logging in to the CVM console, clicking Log in in the right operation column, and selecting alternative login methods (VNC).

Viewing the resource usage of processes
1. In CVM, right click the taskbar, and select **Task Manager** as shown below:

![Task Manager](image)

2. In the “Task Manager”, you can view the resource usage as shown below:

You can sort the processes in ascending/descending order by clicking CPU or memory.
Analyzing the processes

Analyze the resource usage of the processes in Task Manager and adopt solutions according to your situation.

- Some business processes such as IIS, httpd, PHP, and Java are consuming a lot of resources.
  - If there is indeed heavy traffic currently, it is normal to have a high load. You may need to consider expansion.
  - If the current business load is not high, you may need to refer to the service error log for further analysis. The root cause may be improper parameter configuration which can cause a waste of resources.
- System processes such as `svchost.exe` are consuming a lot of resources.
- You can verify if a process is a system process on the Internet.
- A system process is usually located in the `C:\windows\system32` directory and has a signature and a complete description.
- Restart the system or shut down secure but unnecessary system processes.
- Neither business processes nor system processes are consuming a lot of resources.
- If there are some processes which have strange names, do not have a signature or a description, are not in the `C:\windows\system32` directory, and are consuming abnormally high amount of resources, the CVM may have been infected with viruses.
- Check the security of the server. Back up the data and reinstall the system if necessary.
Failed to connect to a remote computer through Remote Desktop

Last updated: 2020-02-25 11:42:09

Scenario

When trying to connect to a Windows instance remotely from Windows, you get the following message:

Remote Desktop can’t connect to the remote computer for one of these reasons:
I) Remote access to the server is not enabled
II) The remote computer is turned off
III) The remote computer is not available on the network

Make sure the remote computer is turned on and connected to the network, and that remote access is enabled.
Possible Causes

Possible causes include but are not limited to the following. Please make analysis based on the actual situation.

- The instance is in an abnormal state
- The CVM does not have a public IP or the public network bandwidth is 0
- The remote login port (3389 by default) is not opened to the Internet in the security group(s) bound with the instance
- Remote Desktop Services is not started
- There are issues with Remote Desktop settings
- There are issues with Windows Firewall settings

Troubleshooting Steps

**Checking if the instance is running**

1. Log in to the CVM Console.
2. In the instance list, check if the instance is **Running** as shown below:

   ![Instance Running](image)

   - If it is running, please check whether the CVM has a public IP.
   - If it is not, please start up the Windows instance.

**Checking whether the CVM has a public IP**
Please check whether the CVM has a public IP in the CVM console as shown below:

- If there is one, please **check whether you have purchased public network bandwidth**.
- If there is not, please **apply for an elastic public IP and bind it with the CVM**.

**Checking whether you have purchased public network bandwidth**

Check whether the public network bandwidth is 0 MB. You need to have at least 1 MB of public network bandwidth.

- If it is, please increase the bandwidth to 1 Mbps or above by **adjusting network configuration**.

**Checking whether the remote login port (3389) of the instance is opened to the Internet**

1. Click the instance you want to log in in the console to enter the instance information page.
2. In the Security Groups tab, check whether the remote login port (3389 by default) is opened to the Internet in the security group(s) bound with the instance as shown below:
If it is, please check the system settings of the Windows instance
If it is not, please edit the corresponding security group rules to open the port to the Internet. For directions, see Operation Guide on security group.

**Checking the system settings of the Windows instance**

1. Log in to the instance using VNC and check the system settings of the Windows instance.

   For details on VNC login, refer to the “Login via VNC” section in Log into Windows Instances.

2. In the operating system interface, click **Start > Run**, enter **services.msc** in the Run box, press **Enter** to open the Services window.

3. Double click Remote Desktop Services to open the “Remote Desktop Services Properties” window and check whether Remote Desktop Services is running as shown below:
If it is, please go to Step 4.

If it is not, please set the “Startup type” to “Automatic” and click **Start** to set “Service status” to “Running”.

4. Click **Start > Run**, enter `sysdm.cpl` in the Run box, and press **Enter** to open the “System Properties” window.

5. In the “Remote” tab, check whether the “Remote Desktop” is set to “Allow remote connections to this computer” as shown below:
If it is, please go to [Step 6] (#step04_6).

If it is not, please set Remote Desktop to “Allow remote connections to this computer”.

6. Click **Start**, select **Control Panel** to open the control panel.

7. In the “Control Panel”, select **System and Security > Windows Defender Firewall** to open “Windows Defender Firewall”.

---

©2013-2019 Tencent Cloud. All rights reserved.
8. In “Windows Defender Firewall”, check the status of Windows Defender Firewall as shown below:

![Windows Defender Firewall status](image)

- If the status is “On”, please go to [Step 9] (#step04_9).
  
  If the status is “Off”, please [submit a ticket](#).

9. In “Windows Defender Firewall”, select **Allow an app through Windows Firewall** to open the “Allowed apps” window.

0. In the "Allowed apps" window, check whether "Remote Desktop" is checked in "Allowed apps and features" as shown below:
- If it is, please go to Step 11.
- If it is not, please check “Remote Desktop”, to allow “Remote Desktop” through Windows Firewall.

1. In “Windows Defender Firewall”, select **Turn Windows Defender Firewall on or off** to open the “Customize Settings” window.

2. In the “Customize Settings” window, set “Private network settings” and “Public network settings” to “Turn off Windows Defender Firewall (not recommended)” as shown below:
If you still cannot connect to the Windows instance through Remote Desktop after taking the steps above, please [submit a ticket](#).
Remote Login Failure Due To Port Issues

This document describes how to diagnose and troubleshoot remote login failures caused by port problems.

The following operations take a CVM with the Windows Server 2012 system as an example.

Diagnosis Tool

You can use the following tool to check whether login issues are related to port or security group configuration:

- **Self-Diagnose**
- **Port Verification**

For security group configuration problems, you can use **Open all ports** in Port Verification To open related ports to the Internet and then try to log in again. If you still cannot log in after opening the ports to the Internet, refer to the following methods for troubleshooting.

Troubleshooting

**Checking network connectivity**

You can use the local Ping command to test network connectivity. At the same time, you can test on computers in different environments (different IP ranges or carriers) to check whether it is a local network problem or a server problem.

1. Open the command line tool on your local computer.

   - Windows systems: Click **Start > Run**, enter **Command**, and the command line dialog box will pop up.
   - Mac OS systems: Open the **Terminal** Tool.

2. Execute the following command to test network connection.
ping + CVM Instance public IP address

For example, execute the ping 139.199.XXX.XXX Command.

- If the network is normal, the following result is returned. In this case, please Check the remote desktop service configuration.

```
C:\Users\Administrator>ping 193.112.1.1
Pinging 193.112.1.1 with 32 bytes of data:
Reply from 193.112.1.1: bytes=32 time<1ms TTL=127
Reply from 193.112.1.1: bytes=32 time<1ms TTL=127
Reply from 193.112.1.1: bytes=32 time<1ms TTL=127
Reply from 193.112.1.1: bytes=32 time<1ms TTL=127
Ping statistics for 193.112.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

- If the network has an exception, the Request Timeout Prompt will appear. In this case, refer to Instance IP Address Ping Failure For troubleshooting.

3. Execute the following command and press Enter To check whether the remote port is open and accessible.

telnet + CVM instance public IP address + Port number

For example, execute the telnet 139.199.XXX.XXX 3389 Command. This is shown in the following figure:

```
telnet 139.199.XXX.XXX 3389
```

- Normal: Black screen, only the cursor appears. This indicates that the port (3389) is accessible. Please Check whether the instance remote desktop service is enabled.
- Abnormal: The connection fails, as shown in the following figure. A network exception occurs, please check the corresponding part of the network.
Checking remote desktop service configuration

Logging in to the CVM using the VNC

We recommend you use the VNC method if standard CVM login methods fail.

1. Log in to the CVM Console.
2. Select the CVM to be checked and click Log In. This is shown in the following figure:

3. In the Log into Windows instance Window that pops up, select Alternative login methods (VNC), and click Log In Now To log in to the CVM.
4. In the login window that pops up, select Send Remote Command In the top left corner, and click Ctrl-Alt-Delete To enter the system login interface as shown below:
Checking whether the remote desktop configuration of the CVM is enabled

1. In the CVM, right click **This Computer** > **Properties** To open the **SYSTEM** Window.
2. In the **SYSTEM** Window, select **Advanced System Configurations** To open the **System Properties** Window.
3. In the **System Properties** Window, select the **Remote** Tab page. Check whether **Allow remote connections to this computer** Under **Remote Desktop** Is checked. This is shown in the
following figure.

![System Properties Dialog Box](Image)

- If yes, the remote connection configuration is enabled. Please [Check whether remote access ports are enabled](#).
- If no, check **Allow remote connections to this computer**, and try to remotely connect to the instance again to check whether the connection is successful.

### Checking whether remote access ports are open

1. In the CVM, click ![Windows PowerShell](Image) to open the **Windows PowerShell** Window.
2. In the Windows PowerShell window, execute the following command to check the operation of the remote Desktop (by default, the remote Desktop service port number is 3389).

   ```
   netstat -ant | findstr 3389
   ```

- If a result similar to the following is returned, the status is normal. You can [Restart the remote desktop](#) and try to remotely connect to the instance again to check whether the connection is successful.
If no connection is shown, the status is abnormal. You can Check whether the remote ports of the registry are correct.

Checking whether the remote ports in the registry are consistent

This step guides you to check whether the TCP PortNumber and RDP Tcp PortNumber are the same.

1. In the CVM, click , select , and enter Regedit. Press Enter To open the Registry Editor Window.
2. In the registry navigation on the left, expand the following directories in order: HKEY_LOCAL_MACHINE > SYSTEM > CurrentControlSet > Control > Terminal Server > Wds > Rdpwd > Tds > Tcp.
3. Locate the PortNumber in **Tcp** And note down the port number (3389 by default), as shown below:

![Registry Editor](image)

4. In the registry navigation on the left, expand the following directories in order:

```
HKEY_LOCAL_MACHINE > SYSTEM > CurrentControlSet > Control > Terminal Server > WinStations > RDP-Tcp
```

5. Locate PortNumber in **RDP-Tcp** And check whether the PortNumber data in **RDP-Tcp** is the same as the one in **Tcp**. This is shown in the following figure:

![Registry Editor](image)
6. If they are not the same, execute Step 6.
7. If they are the same, Restart the remote login service.

6. Double click PortNumber in RDP-Tcp.
7. In the dialog box that pops up, modify Value Data to an unoccupied port number between 0-65535, ensuring TCP PortNumber and RDP Tcp PortNumber Port numbers are the same, and click OK.
8. After modification, restart the instance in CVM Console, and try to remotely connect to the instance again to check whether the connection is successful.

**Restarting the remote log in service**

1. In the CVM, click , select , and enter Services.msc. Press Enter to open the Services Window.
2. Locate and right-click Remote Desktop Services, select Restart to restart the remote login service. This is shown in the following figure:
Other Operations

If you are still unable to remotely log in after performing the above-mentioned operations, please Submit a ticket.
Network Namespace Creation Failure

Problem Description

The command for creating a network namespace got stuck and did not continue. dmesg message:
"unregister_netdevice: waiting for lo to become free. Usage count = 1"

Cause of the Problem

It is caused by a bug of the kernel.
The following kernel versions have this bug:

- Ubuntu 16.04 x86_64 kernel version: 4.4.0-91-generic.
- Ubuntu 16.04 x86_32 kernel version: 4.4.0-92-generic.

Solution

 Upgrade the kernel version to 4.4.0-98-generic, in which the bug has been fixed.

Procedure

1. Check the current kernel version.

   ```bash
   uname -r
   ```

2. Check whether version 4.4.0-98-generic is available for upgrade.

   ```bash
   sudo apt-get update
   sudo apt-cache search linux-image-4.4.0-98-generic
   ```

   If the following information is shown, it means the version to upgrade to exists in the source:

   ```bash
   linux-image-4.4.0-98-generic - Linux kernel image for version 4.4.0 on 64 bit x86 SMP
   ```
3. Install the new version kernel and corresponding Header package.

```bash
sudo apt-get install linux-image-4.4.0-98-generic linux-headers-4.4.0-98-generic
```

4. Restart the system.

```bash
sudo reboot
```

5. Enter the system to check the kernel version.

```bash
uname -r
```

If the following result is displayed, it means the version upgrade is successful:

```
4.4.0-98-generic
```
This document describes how to determine possible causes of instance login failures after you purchase Cloud Virtual Machine (CVM) instances, helping you locate and resolve CVM login failures.

Possible Causes

The following figure shows the primary causes of CVM instance login failures and their probabilities. If you cannot connect to an instance, we recommended you use the diagnosis tool and perform troubleshooting as instructed below.

![Possible Causes Diagram]

Troubleshooting

Confirming the instance type

You must first determine whether your purchased instance is a Windows system instance or Linux system instance. The causes of login failures vary by instance types. According to your purchased instance type, refer to the following documentation to locate and resolve the issue.

- Unable to log into a Windows instance
- Unable to log into a Linux instance

Using the diagnosis tool to locate the causes
Tencent Cloud provides Port Verification to help you determine possible causes of login failures. More than 70% of login issues can be checked and located by this tool.

**Self-Diagnosis Tool**

Problems that can be diagnosed include high bandwidth usage rate, zero public network bandwidth, high server workload, improper security group rules, DDoS attack blocking, security isolation, and account in arrears.

**Port Verification Tool**

This tool can diagnose security group- and port-related problems. If there is a security group configuration issue, you can use **Open All Ports** function of the tool to open all commonly used interfaces of the security group.

If you locate the cause of the issue using the tool, we recommend you follow the corresponding issue guidelines to resolve it.

**Restarting Instance**

After the diagnosis tool has located and managed the corresponding issue, or it is still not possible to locate the cause of the login failure using the diagnosis tool, you can restart the instance and connect remotely again to see whether the connection succeeds.

For information about how to restart an instance, see **Restart Instance**.

**Other common causes of login failures**

If you cannot locate the cause of the issue following the above-mentioned steps, or you receive the following error messages when logging in to the CVM, refer to the following solutions.

**Windows Instances**

- Windows instance: Unauthorized to log in via remote desktop service
- Windows instance: Mac remote login exception
- Windows instance: Authentication error
- Windows instance: Remote desktop cannot connect to the remote computer

**Linux Instances**

Linux instance: Unable to login due to high CPU and memory usage rates

**Subsequent Operations**

If you still cannot log in remotely following the above-mentioned steps, save the related logs and self-diagnosis results, then **Submit Ticket**.
Login Failure Due to High Bandwidth Occupation

Last updated : 2020-02-11 11:52:56

This document describes how to diagnose and troubleshoot Linux or Windows CVM login issues caused by high bandwidth usage.

Problems

- In CVM Console, the bandwidth monitoring data of the CVM shows that bandwidth usage is too high, and connection to CVM fails.

Locating and troubleshooting the issues

1. Log in to the CVM Console.
2. Select the CVM to be checked and click Log In. This is shown in the following figure:

3. In the Log into Windows/Linux instance window that pops up, select Alternative login methods (VNC), and click Log In Now to log in to the CVM.
4. In the login window that pops up, select Send Remote Command in the top left corner, and click Ctrl-Alt-Delete to enter the system login interface as shown below:
Windows CVMs

After using VNC to log into Windows CVM, perform the following operations:

The following operations take a CVM with the Windows Server 2012 system as an example.

1. In the CVM, click Ctrl-Alt-Delete. Select Task Manager to open the Task Manager window.
2. Select the Performance tab page and click Open Resource Monitor. This is shown in the following figure:
3. Once **Resource Monitor** opens, check which process consumes more bandwidth. According to your actual business, determine whether the process is normal. This is shown in the following
If the process that consumes a lot of bandwidth is normal, check whether it is due to changes in access volume, and whether you need to optimize the capacity or upgrade CVM configurations.

If the process that consumes a lot of bandwidth is abnormal, there may be a virus or a Trojan. You can terminate the process on your own or use security software. You can also reinstall the system after data backup.

In Windows systems, many virus processes are disguised as system processes. You can use process information in **Task Manager > Processes** to perform preliminary inspection:

Normal system processes have complete signatures and descriptions, and most of them locate under the C:\Windows\System32 directory. Virus programs may have the same name as system processes, but they do not have signatures or descriptions. The location will also be abnormal.
If the process that consumes a lot of bandwidth is a Tencent Cloud component process, submit a ticket to contact us. We will help you locate and troubleshoot the problem.

Linux CVMs
After using VNC to log into the Linux CVM, perform the following operations:

The following operations take a CVM with the CentOS 7.6 system as an example.

1. Execute the following command to install the iftop tool. The iftop tool is a traffic monitoring gadget for Linux CVM.
   
   ```
   yum install iftop -y
   ```

   For Ubuntu system, execute the `apt-get install iftop -y` command.

2. Execute the following command to install lsof.
   
   ```
   yum install lsof -y
   ```

3. Execute the following command to run iftop. This is shown in the following figure:
   
   ```
   iftop
   ```

- `<` 、 `=>` indicates the direction of traffic
- TX indicates the delivery traffic
RX indicates the receiving traffic
TOTAL indicates total traffic
cum indicates the total traffic from the moment iftop starts to run until now
peak indicates traffic peaks
rates indicate the average traffic over the last 2s, 10s, and 40s respectively

4. According to the IP of the consumed traffic in iftop, execute the following command to check the process connected to this IP.

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

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

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

If the following results are returned, CVM bandwidth is mainly consumed by the SSH process.

```
sshd 12179  root  0t0  IPV4 3294018 0t0  TCP 10.144.90.86:ssh->203.205.141.123:58614(ESTABLISHED)
sshd 12145  root  3u  IPV4 3294018 0t0  TCP 10.144.90.86:ssh->203.205.141.123:58614(ESTABLISHED)
```

5. View the process that consumes bandwidth, and determine whether the process is normal.
   - If the process that consumes a lot of bandwidth is normal, check whether it is due to changes in access volume, and whether you need optimize the capacity or upgrade CVM configurations.
   - If the process that consumes a lot of bandwidth is abnormal, there may be a virus or a Trojan. You can terminate the process on your own or use security software. You can also reinstall the system after data backup.
   - If the process that consumes a lot of bandwidth is a Tencent Cloud component process, submit a ticket to contact us. We will help you locate and troubleshoot the problem.

We recommend you check the location of the destination IP on What Is My IP Address. If the IP location is in other countries/regions, the security risk is greater.
This document describes how to resolve login failures if the CVM is isolated from the public network.

Problems

The CVM may have been isolated because it violates current laws and regulations. You can use the following methods to check whether the CVM is isolated.

- When a CVM is isolated from the public network, you will be notified of the isolation via an internal message in the console or a text message.

Causes

When a regulation violation or risk event occurs for a CVM, the offending machine will be partially isolated (except for the private network login port 22, 36000, and 3389, all network access will be isolated. Developers can use a jump server to log in to the server.

For details, see [Cloud Security Violation Levels Classification and Penalties Description].

Solutions

1. Delete the violating content as instructed by the internal message or text message. Resolve security risks and reinstall the system if necessary.
2. If the violation is not caused by your own action, your CVM may have encountered malicious intrusion. To resolve this, see Host Security.
3. After resolving security risks and deleting violating content, you can submit a ticket to contact customer service to remove the isolation.
Network Related Failures
International Linkage Latency

Last updated: 2019-08-16 20:45:16

Problem Description

The latency is too long when users log in to CVMs located in North America. Due to the small number of international routing egresses within the country and other factors, high concurrency may cause serious congestion of the international linkage and make the access unstable. Tencent Cloud has reported this issue to the ISP. If you need to manage and operate a CVM located in North America at home, in the short term, you can purchase a CVM located in Hong Kong (China) and use it as a transfer point to log in to the CVM located in North America.

Solution

1. Purchase a Windows CVM located in Hong Kong (China) as a jump server in the custom configuration page (Windows operating systems support login to both Windows and Linux CVMs located in North America).

   Note: You need to buy at least 1 Mbps bandwidth, or you will be unable to log in to the jump server.

2. After the purchase is made successfully, log in to the Windows CVM located in Hong Kong (China):

   Log in to a Windows CVM with a public IP from a Windows machine
   Log in to a Windows CVM from console VNC

3. Log in to your CVM located in North America from the Windows CVM located in Hong Kong (China):

   • Log in to a Linux CVM located in North America
Log in to a Linux CVM with a public IP from a Windows machine using password

- Log in to a Windows CVM located in North America

Log in to a Windows CVM with a public IP from a Windows machine

Log in to a Windows CVM from console VNC
Website Access Failure

Last updated: 2019-08-09 18:43:49

Website access failure may be caused by network problems, firewall configuration or CVM overload. This document describes how to troubleshoot and locate the problems that cause website access failure.

CVM Problem

Since CVM shutdown, hardware failure and CPU/memory/bandwidth overuse may contribute to the inaccessibility of website, it is recommended to check the CVM's running status and the usage of CPU/memory/bandwidth.

1. Check the CVM's running status Log in to Tencent Cloud console and check the running status of the CVM to make sure it is running normally. If it is not in running status, restart it or perform other operations.

2. Check resource usage. Click Monitoring tab on the instance details page to check the usage of CPU/memory/bandwidth. In case of high CPU utilization, please see troubleshooting for High CPU Utilization (Windows) and High CPU Utilization (Linux). In case of high bandwidth utilization, please see High Bandwidth Utilization.

3. Check whether the port relevant to Web service is listened normally. Let's take port 80, which is commonly used in HTTP service, as an example to describe how to troubleshoot problems on Linux or Windows system:
   - **Linux system**
     
     Check the listening status of port 80 using `netstat`. The command is as follows. `-t` indicates tcp port, `-p` indicates process identifier and corresponding program name, and `-l` indicates listening socket.

     ```bash
     [root@VM_2_184_centos -]# netstat -ntulp | grep 80
tcp    0      0 0.0.0.0:80          0.0.0.0:*        LISTEN      1309/httpd
     ```

   - **Windows system**
     
     Check the listening status of port 80 using `netstat -ano|findstr :80`. You can check the name of the process being listened using process ID.
If the port is not being listened normally, check whether the Web service process is enabled or correctly configured.

4. Check whether the port relevant to Web service process is open in the firewall configuration. For Linux, check whether the port 80 is open for iptables. For Windows, check Windows firewall configuration.

Network Problem

Another possible cause of network access failure is network problem. You can ping the public IP of the destination server using ping command to check whether packet loss or high latency occurs. If any of the problems occurs, use MTR for further troubleshooting. For more information, please see Network Delay and Packet Loss for CVM.

Security Group Configuration
Security group is a virtual firewall, which allows you to control the inbound and outbound traffic of the associated instance. You can specify protocols, ports and policies for the rules of a security group. A website may also be inaccessible if the ports relevant to Web processes are not open. After troubleshooting CVM and network problems, you need to check the rules of security group to which the instance belongs.

You can view the information of the associated security group and its inbound/outbound rules in the **Security Group** tab of the instance details page to check whether the ports relevant to Web processes are open. If no relevant port is open, edit the associated security rules to open the ports.

### Domain Name Licensing and Resolution Problems

If none of the above methods works, you can access the website using the CVM's public IP. If the website can be accessed via the public IP instead of a domain name, the domain name may not be licensed or correctly resolved.

1. According to the regulations of MIIT, websites that have not obtained permission nor completed ICP licensing cannot engage in any Internet information services, otherwise it is considered illegal. To ensure the persistent and normal operation of your website, complete website ICP licensing before setting up a website. The website cannot be accessed until you obtain the ICP license number issued by MIIT. If your domain name has not been licensed, complete Domain Name ICP Licensing.

   If you are using Tencent Cloud DNS, go to the **console** -> **Domain Name and Website** -> **Domain Name Management** to view the information of an appropriate domain name.

2. A website may also be inaccessible if the request is not routed to the Web server due to incorrect domain name resolution configuration. If you are using Tencent Cloud DNS, go to the **console** -> **Domain Name and Website** -> **Domain Name Management**, and click the **Resolve** button of a domain name to view the its resolution details.
Slow Website Access

Last updated: 2019-09-26 14:28:17

A complete HTTP request includes resolving domain name, establishing TCP connection, initiating the request, CVM receiving and processing the request, CVM returning the result, and browser parsing HTML code, requesting other resources and rendering the page. These processes involve the local client, network nodes between the client and the access server, and the server. Any problem occurs with any of them may cause stuttering and latency of network access.

1. Check Local Client Problem

Access the network testing website (ping.huatuo.qq.com) on the local client and test the speed of access to different domain names from the local client to check whether there is any problem in local network. The following test result shows the delay of accessing each domain name and whether the network is normal. If the network is exceptional, contact your ISP to locate and solve the problem.

<table>
<thead>
<tr>
<th>Domain Name</th>
<th>Network Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>inews.qq.com</td>
<td>Normal network, 194 milliseconds delay</td>
</tr>
<tr>
<td><a href="http://www.qq.com">www.qq.com</a></td>
<td>Normal network, 128 milliseconds delay</td>
</tr>
<tr>
<td>3g.qq.com</td>
<td>Normal network, 140 milliseconds delay</td>
</tr>
<tr>
<td>mail.qq.com</td>
<td>Normal network, 99 milliseconds delay</td>
</tr>
<tr>
<td>user.qzone.qq.com</td>
<td>Normal network, 98 milliseconds delay</td>
</tr>
<tr>
<td>r.qzone.qq.com</td>
<td>Normal network, 203 milliseconds delay</td>
</tr>
<tr>
<td>w.qzone.qq.com</td>
<td>Normal network, 188 milliseconds delay</td>
</tr>
<tr>
<td>ptlogin2.qq.com</td>
<td>Normal network, 96 milliseconds delay</td>
</tr>
<tr>
<td>check.ptlogin2.qq.com</td>
<td>Normal network, 189 milliseconds delay</td>
</tr>
<tr>
<td>ui.ptlogin2.qq.com</td>
<td>Normal network, 91 milliseconds delay</td>
</tr>
</tbody>
</table>
2. Check Network Linkage Problem

If no exception is found in step 1, check whether there is any network problem between the local client and the server.
(1) Ping the server's public IP from the local client to check whether packet loss or high latency occurs.
(2) If any of the problems occurs, use MTR for further diagnosis. For more information, please see Network Delay and Packet Loss for CVM.
(3) If no exception is found in the ping test of the server's IP, use dig/nslookup to check whether the problem is caused by DNS resolution. You can also access the page directly with the IP to check whether DNS is the cause of access latency.

3. Check Server Problem

Analyze the Web server if no problem is found in the client and network linkage. Check whether the system resources are insufficient, or the system is attacked by viruses, Trojan-horse programs, or suffers DDoS attacks.
(1) Log in to CVM console. Click Monitoring tab in CVM details page to check the usage of instance resources.
(2) Overuse of CPU/memory/bandwidth/disk may be caused by high CVM load or virus attacks. Please see the following documents for troubleshooting:

- High CPU Utilization (Linux)
- High CPU Utilization (Windows)
- High Bandwidth Utilization

4. Check Business Problem

(1) It is considered normal if the problem is caused by the resource overconsumption due to high CVM load in step 3. You can solve this problem by optimizing business processes, upgrading server configuration or purchasing new servers to reduce the pressure of existing servers.
(2) If no problems are found in the above three steps, it is recommended to check log files to locate and optimize the step that leads to a slow response.
If stutters occur when you access a CVM from a local server or access other network resources from a CVM, and packet loss or high latency is found after you ping, this is probably caused by backbone linkage congestion, linkage node failure, excessive server load or inappropriate system configuration. You can use MTR to further diagnose after ruling out CVM problems. MTR is a powerful network diagnostic tool, providing reports that allow users to find out the causes of network problems. This document describes how to use MTR and analyze report results in Linux and Windows.

In this document, the server on which MTR runs is referred to as the source server, and the server to be queried is referred to as the destination server. See relevant sections based on the operating system of your source server.

**WinMTR Introduction and Instructions (for Windows)**

**WinMTR** is a free network diagnostic tool for Windows integrated with Ping and tracert features. Through its graphical interface, you can see the response time and packet loss of each node intuitively.

**Installation and use of WinMTR**

1. Download the installer package based on the operating system type, decompress it, and double-click and run WinMTR.exe in it, as shown below.
2. Enter the IP or domain name of the destination server in the Host field. Then click **Start** to run the test.

3. Click **Stop** to stop the test after a while.
4. View the test result.

![WinMTR v0.92 64 bit by Appnor MSP - www.winmtr.net](image)

<table>
<thead>
<tr>
<th>Hostname</th>
<th>Nr</th>
<th>Loss %</th>
<th>Sent</th>
<th>Recv</th>
<th>Best</th>
<th>Avrg</th>
<th>Worst</th>
<th>Last</th>
</tr>
</thead>
<tbody>
<tr>
<td>100.119.162.130</td>
<td>1</td>
<td>0</td>
<td>144</td>
<td>144</td>
<td>1</td>
<td>2</td>
<td>13</td>
<td></td>
</tr>
<tr>
<td>100.119.170.58</td>
<td>2</td>
<td>0</td>
<td>144</td>
<td>144</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>10.200.135.197</td>
<td>3</td>
<td>0</td>
<td>144</td>
<td>144</td>
<td>0</td>
<td>2</td>
<td>14</td>
<td></td>
</tr>
<tr>
<td>10.200.16.165</td>
<td>4</td>
<td>0</td>
<td>144</td>
<td>144</td>
<td>33</td>
<td>34</td>
<td>70</td>
<td></td>
</tr>
<tr>
<td>10.200.7.173</td>
<td>5</td>
<td>0</td>
<td>144</td>
<td>144</td>
<td>30</td>
<td>33</td>
<td>65</td>
<td></td>
</tr>
<tr>
<td>10.200.8.101</td>
<td>6</td>
<td>0</td>
<td>144</td>
<td>144</td>
<td>31</td>
<td>31</td>
<td>46</td>
<td></td>
</tr>
<tr>
<td>111.231.134.51</td>
<td>7</td>
<td>0</td>
<td>144</td>
<td>144</td>
<td>34</td>
<td>34</td>
<td>38</td>
<td></td>
</tr>
</tbody>
</table>

Explanation of the result data:

**Hostname**: IP or name of each server on the data forwarding path to the destination server.

**Nr**: Number of nodes that have been passed through.

**Loss%**: Packet loss of each node.

**Sent**: Number of data packets sent.

**Recv**: Number of responses received.

**Best**: Shortest response time.

**Avrg**: Average response time.

**Worst**: Longest response time.

**Last**: Last response time.

---

**MTR Introduction and Instructions (for Linux)**
**MTR** is a network diagnostic tool for Linux integrated with Ping, traceroute and nslookup features. ICMP packets are used to test the network connection between two nodes by default.

**MTR installation**

Almost all released versions of Linux are preinstalled with MTR. You can also install MTR using the following command:

- CentOS:
  ```bash
yum install mtr
  ```

- Ubuntu:
  ```bash
  sudo apt-get install mtr
  ```

**Explanation of MTR-related parameters**

- `--help`: Displays help menu.
- `--version`: Displays MTR version information.
- `--report`: Outputs the result in a report.
- `--split`: Different from `--report`, `--split` lists the result of each trace separately.
- `--report-cycles`: Sets the number of data packets sent per second. Default is 10.
- `--psize`: Sets the size of each data packet.
- `--no-dns`: Disables the domain name resolution for IP addresses.
- `--address`: Sets the IP address from which data packets are sent. It is mainly used for scenarios with a single server and multiple IP addresses.

`-4`: IPv4.

`-6`: IPv6.

We take the following MTR report from a local server to a CVM (119.28.98.39) as an example to explain the returned results.
### Host: IP address or domain name of a node.
### Loss%: Packet loss.
### Snt: Number of data packets sent per second.
### Last: Last response time.
### Avg: Average response time.
### Best: Shortest response time.
### Wrst: Longest response time.
### StDev: Standard deviation. A higher standard deviation indicates a larger difference between the response time of data packets on this node.

## Report Analysis and Troubleshooting

We have introduced how to use network diagnostic tools in different operating systems. Next, we will describe how to analyze a report.

Due to the asymmetry of network conditions, if any network error between the local server and the CVM occurs, it is recommended that you collect two-way MTR data (both from the local server to the CVM and from the CVM to the local server).

### Steps for analyzing MTR results

```bash
[root@VM_103_80_centos ~]# mtr 119.28.98.39 --report
Start: Mon Feb 5 11:33:34 2018

<table>
<thead>
<tr>
<th>HOST: VM_103_80_centos</th>
<th>Loss%</th>
<th>Snt</th>
<th>Last</th>
<th>Avg</th>
<th>Best</th>
<th>Wrst</th>
<th>StDev</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. -- 100.119.162.130</td>
<td>0.0%</td>
<td>10</td>
<td>6.5</td>
<td>8.4</td>
<td>4.6</td>
<td>13.7</td>
<td>2.9</td>
</tr>
<tr>
<td>2. -- 100.119.170.58</td>
<td>0.0%</td>
<td>10</td>
<td>0.8</td>
<td>0.8</td>
<td>0.6</td>
<td>1.1</td>
<td>0.0</td>
</tr>
<tr>
<td>3. -- 10.200.135.213</td>
<td>0.0%</td>
<td>10</td>
<td>0.4</td>
<td>0.6</td>
<td>0.4</td>
<td>2.5</td>
<td>0.6</td>
</tr>
<tr>
<td>4. -- 10.200.16.173</td>
<td>0.0%</td>
<td>10</td>
<td>1.6</td>
<td>1.5</td>
<td>1.4</td>
<td>1.6</td>
<td>0.0</td>
</tr>
<tr>
<td>5. -- 14.18.199.58</td>
<td>0.0%</td>
<td>10</td>
<td>1.0</td>
<td>1.3</td>
<td>1.0</td>
<td>4.1</td>
<td>0.9</td>
</tr>
<tr>
<td>6. -- 14.18.199.25</td>
<td>0.0%</td>
<td>10</td>
<td>4.1</td>
<td>4.7</td>
<td>3.3</td>
<td>10.2</td>
<td>1.9</td>
</tr>
<tr>
<td>7. -- 113.96.7.214</td>
<td>0.0%</td>
<td>10</td>
<td>5.8</td>
<td>7.3</td>
<td>3.1</td>
<td>10.1</td>
<td>2.1</td>
</tr>
<tr>
<td>8. -- 113.96.0.106</td>
<td>0.0%</td>
<td>10</td>
<td>3.9</td>
<td>7.8</td>
<td>3.9</td>
<td>11.0</td>
<td>2.5</td>
</tr>
<tr>
<td>9. -- 202.97.90.206</td>
<td>30.0%</td>
<td>10</td>
<td>2.4</td>
<td>2.4</td>
<td>2.4</td>
<td>2.5</td>
<td>0.0</td>
</tr>
<tr>
<td>10. -- 202.97.94.77</td>
<td>0.0%</td>
<td>10</td>
<td>3.5</td>
<td>4.8</td>
<td>3.5</td>
<td>7.0</td>
<td>1.2</td>
</tr>
<tr>
<td>11. -- 202.97.51.142</td>
<td>0.0%</td>
<td>10</td>
<td>164.7</td>
<td>163.4</td>
<td>161.3</td>
<td>165.3</td>
<td>1.2</td>
</tr>
<tr>
<td>12. -- 202.97.49.106</td>
<td>0.0%</td>
<td>10</td>
<td>162.3</td>
<td>164.9</td>
<td>161.7</td>
<td>167.8</td>
<td>2.0</td>
</tr>
<tr>
<td>13. -- ix-xe-10-2-6-0.tc172.lvw</td>
<td>10.0%</td>
<td>10</td>
<td>168.4</td>
<td>167.9</td>
<td>161.5</td>
<td>168.9</td>
<td>2.3</td>
</tr>
<tr>
<td>14. -- 180.87.15.25</td>
<td>10.0%</td>
<td>10</td>
<td>348.1</td>
<td>348.3</td>
<td>347.7</td>
<td>350.2</td>
<td>0.7</td>
</tr>
<tr>
<td>15. -- 180.87.96.21</td>
<td>0.0%</td>
<td>10</td>
<td>345.0</td>
<td>343.9</td>
<td>343.4</td>
<td>345.0</td>
<td>0.3</td>
</tr>
<tr>
<td>16. -- 180.87.96.142</td>
<td>0.0%</td>
<td>10</td>
<td>187.4</td>
<td>187.5</td>
<td>187.3</td>
<td>187.6</td>
<td>0.0</td>
</tr>
<tr>
<td>17. -- ??</td>
<td>100.0</td>
<td>10</td>
<td>0.0</td>
<td>0.0</td>
<td>0.0</td>
<td>0.0</td>
<td>0.0</td>
</tr>
<tr>
<td>18. -- 100.78.119.231</td>
<td>0.0%</td>
<td>10</td>
<td>187.7</td>
<td>190.2</td>
<td>187.3</td>
<td>194.0</td>
<td>2.5</td>
</tr>
<tr>
<td>19. -- 119.28.98.39</td>
<td>0.0%</td>
<td>10</td>
<td>186.5</td>
<td>186.5</td>
<td>186.4</td>
<td>186.5</td>
<td>0.0</td>
</tr>
</tbody>
</table>
```
1. Check whether there is packet loss on the destination IP. No packet loss indicates basically normal network conditions. Packet loss on intermediate nodes may be caused by ICMP restrictions of linkage nodes or other policies, and there is no actual packet loss. Therefore, when checking the WinMTR/MTR results, you need to check whether there is packet loss on the destination IP first. No packet loss indicates normal network conditions.

2. If there is packet loss on the destination IP, check the result from its bottom to the top to locate the node where the first packet loss occurs.

3. Packet loss occurred at the destination server is probably caused by incorrect network configuration of the destination server. Please check its firewall configuration. Packet loss occurred at the first three hops is probably caused by local ISPs' network problems. If this also happens when you are visiting other addresses, report this problem to your ISP. Packet loss occurred at the hops closing to the destination server is probably caused by destination server ISPs' network problems. Submit a ticket to report the problem. Screenshots of MTR tests from the local to the destination and from the destination to the local need to be attached for error locating.
A failed ping test from a local server to an instance may be caused by incorrect destination server configuration, unsuccessful domain name resolution or linkage failure. The following describes how to troubleshoot this problem if the local network is normal (other websites can be pinged):

1. Check whether the instance is bound with a public IP.

Only an instance with public IP can access and be accessed by other computers on the Internet. An instance without public IP cannot be pinged outside the private IP. You can check the information of public IP on the instance details page in the console, as shown below. Bind an EIP to the instance if it is not bound with any public IP.

2. Check the security group configuration

Security group is a virtual firewall, which allows you to control the inbound and outbound traffic of the associated instance. You can specify protocols, ports and policies for the rules of a security
group. Check whether the ICMP protocol that is used in ping test is allowed in the security group associated to the instance. You can view the information of the associated security group and its inbound/outbound rules in the Security Group tab of the instance details page.

3. Check the system configurations

Check kernel parameters and firewall settings on Linux

On Linux system, whether a ping test is allowed depends on both kernel and firewall configuration. If either of them blocks the ping test, "Request timeout" occurs.

Kernel parameter icmp_echo_ignore_all

icmp_echo_ignore_all indicates whether to ignore all ICMP Echo requests. 1: Disabled; 0: Enabled. Check icmp_echo_ignore_all configuration using the following command.

```
cat /proc/sys/net/ipv4/icmp_echo_ignore_all
```

You can modify the configuration using echo command.

```
echo "1" >/proc/sys/net/ipv4/icmp_echo_ignore_all
```

Firewall settings
Check the firewall rules of the CVM using `iptables -L`, and check whether ICMP-related rules are blocked.

```
[root@VM_103_80_centos ~]# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source          destination
ACCEPT     icmp  --  anywhere       anywhere           icmp echo-request

Chain FORWARD (policy ACCEPT)
target     prot opt source          destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source          destination
ACCEPT     icmp  --  anywhere       anywhere           icmp echo-request
```

**Firewall settings on Windows**

Go to **Control Panel -> Windows Firewall Settings -> Advanced Settings** to check whether inbound and outbound rules related to ICMP are blocked.
Domain Name Resolution Failure (CentOS 6.X System)

Problem Description

After a CVM with CentOS 6.x operating system is restarted or the command `service network restart` is executed against the CVM, domain names cannot be resolved for the CVM. In addition, the DNS information in the configuration file `/etc/resolv.conf` is found to be cleared.

Possible Cause

Defects exist in initscripts with versions earlier than 9.03.49-1 in CentOS 6.x operating system due to different grep versions.

Solution

Upgrade the initscripts to the latest version and regenerate DNS information.

Procedure

1. Log in to the CVM and execute the following command to check the initscripts version.

   ```bash
   $ rpm -q initscripts
   initscripts-9.03.40-2.e16.centos.x86_64
   
   As shown in the example above, the initscripts version is initscripts-9.03.40-2, which is earlier than the defective version of initscripts-9.03.49-1, so there involves a risk of cleared DNS.
   
2. Execute the following command to upgrade initscripts to the latest version and regenerate DNS information.

   ```bash
   cat /dev/null > /etc/resolv.conf
   service network restart
   yum makecache
   yum -y update initscripts
   ```
3. Execute the following command after upgrade to check the version information of initscripts and verify whether the initscripts is upgraded successfully.

```
$ rpm -q initscripts
initscripts-9.03.58-1.el6.centos.2.x86_64
```

The version displayed is different from that before upgrade and is later than initscripts-9.03.49-1, which indicates that the initscripts is upgraded successfully.
Performance Related Failures
High CPU Usage Rate (Linux System)

Last updated: 2019-08-09 18:43:16

High CPU utilization may cause problems such as slow service response speed and server login failure. You can use Cloud Monitor to create an alarm threshold for CPU utilization so that you are promptly notified when CPU utilization exceeds the threshold.

Troubleshooting high CPU utilization involves locating the processes consuming CPU power and analyzing those using a large amount of CPU power. If they are exceptional processes which may be caused by viruses or Trojans, you can terminate the processes or use your security software to check and kill them. If they are business processes, you need to analyze whether high CPU utilization is caused by large number of visits and whether it can be optimized. If they are processes generated by Tencent Cloud components, contact us by submitting a ticket, and we will help you locate and troubleshoot the problem.

The following describes how to locate a process with too high CPU utilization under Linux.

Tool for Locating Programs: top Command

top: A commonly used monitoring tool for Linux systems to get process-level CPU usage in real time.

The output information of top command is as follows:

```
  top - 22:16:25 up 6:18, 1 user, load average: 0.00, 0.01, 0.05  
Tasks: 68 total, 1 running, 67 sleeping, 0 stopped, 0 zombie  
%CPU(s): 0.0 us, 0.3 sy, 0.0 ni, 99.7 id, 0.0 wa, 0.0 hi, 0.0 si, 0.0 st  
KiB Mem: 1016516 total, 605016 free, 77224 used, 334276 buff/cache  
KiB Swap: 0 total, 0 free, 0 used. 778708 avail Mem

   PID USER PR NI VIRT  RES SHMR %CPU %MEM   TIME+ COMMAND
   257 root 20  0   0    0   0 0   0.3  0.0 0:00.73 jbd2/mdl-8
   984 root 20  0 569592 5068 2568 S    0.3  0.5 0:16.51 YDService
  1253 root 20  0 534620 12288 2104 S    0.3  1.2 0:34.21 barad_agent
     1 root  0  0 43104 3512 2404 S    0.0  0.3 0:01.87 systemd
     2 root  0  0    0    0 0 S    0.0  0.0 0:00.00 kthread
     3 root  0  0    0    0 0 S    0.0  0.0 0:00.33 ksoftirqd/0
     4 root  0  0    0    0 0 S    0.0  0.0 0:00.00 kworker/0:0
     5 root  0  0    0    0 0 S    0.0  0.0 0:00.00 kworker/0:0H
     7 root  0  0    0    0 0 S    0.0  0.0 0:00.00 migration/0
     8 root  0  0    0    0 0 S    0.0  0.0 0:00.00 rcu_bh
     9 root  0  0    0    0 0 S    0.0  0.0 0:01.20 rcu_sched
    10 root  0  0    0    0 0 S    0.0  0.0 0:00.05 watchdog
```

The upper part shows the overall usage of CPU and memory resources:
The current time of the system, the number of currently logged in users and the system load.

Total number of processes, number of running processes, number of dormant processes, number of sleeping processes, and number of zombie processes.

Current CPU usage.

Current memory usage.

Current swap usage.

The lower part shows the occupancy of resources by process.

**PID**: Process ID.

**USER**: Process owner.

**PR**: Process priority. NI: NICE value. A smaller NICE value means a higher priority.

**VIRT**: Used VM size, in KB.

**RES**: Currently used memory size, in KB.

**SHR**: Used shared memory size, in KB.

**S**: Process status.

**%CPU**: The percentage of CPU time used by the process during the update interval.

**%MEM**: The percentage of memory used by the process during the update interval.

**TIME+**: CPU time used by the process, accurate to 0.01 sec.

**COMMAND**: Process name.

### Problem Locating and Troubleshooting

**Locating processes with high CPU utilization with top**

The following describes how to use top to locate processes with high CPU utilization.

1. Log in to the instance via SSH or VNC
   
   Note: Too high CPU utilization may cause server login failure. At this point, you can try to log in via VNC. For more information on how to log in to an instance via VNC, please see [Logging In to Linux Instances](#).

2. Enter the top command to view the system load.

3. Enter "P", and then processes are listed in descending order of CPU utilization, which makes it easy for you to get the processes with high CPU utilization for further analysis.
4. Analyze the processes with high CPU utilization.
   
   (1) If they are business processes, it is recommended to analyze whether these processes can be optimized or whether the resource configuration of the instance can be enhanced.
   
   (2) If they are exceptional processes, the instance may be poisoned. You can terminate the processes, use your security software to check and kill them, or reinstall the system after data backup.
   
   (3) If they are processes generated by Tencent Cloud components and take up over 20% CPU power, contact us by submitting a ticket, and we will help you locate and troubleshoot the problem.

   Common Tencent Cloud components include:
   
   sap00x: Security component process
   Barad_agent: Monitoring component process
   secu-tcs-agent: Security component process

**Terminating processes with top**

1. Enter "k" and the pid of the process (the first process in the list by default) you want to terminate, and then press Enter.
2. After that, a prompt of "Send pid 984 signal [15/sigterm]" appears. Press **Enter** to confirm.

### Handling of the process kswapd0 with high CPU utilization

kswapd0 is the process that swaps pages in virtual memory management in Linux. In addition to managing memory through paging mechanism, Linux also assigns part of disks as virtual memory. When the system is running out of memory, kswapd0 will frequently swap pages, which consumes a large amount of CPU resources, resulting in the process continuously occupying high CPU resources. After you locate the process kswapd0 with high CPU utilization by using the command `top`, execute `vmstat` to view the system's virtual memory. If "si" and "so" are also relatively high, it proves that frequent page swapping operations are performed in the system, which outgrows the physical memory. It is recommended that you upgrade the system's memory.
High CPU Usage Rate (Windows System)

Last updated: 2019-08-09 18:46:46

High CPU utilization may cause problems such as slow service response speed and server login failure. You can use Cloud Monitor to create an alarm threshold for CPU utilization so that you are promptly notified when CPU utilization exceeds the threshold.

Troubleshooting high CPU utilization involves locating the processes consuming CPU power and analyzing those using a large amount of CPU power. If they are exceptional processes which may be caused by viruses or Trojans, you can terminate the processes or use your security software to check and kill them. If they are business processes, you need to analyze whether high CPU utilization is caused by large number of visits and whether it can be optimized. If they are processes generated by Tencent Cloud components, contact us by submitting a ticket, and we will help you locate and troubleshoot the problem.

The following describes how to locate a process with too high CPU utilization under Windows.

Tool for Locating Programs

**Task Manager**: A Windows application and process management tool that displays the information about PC performance and running software, including process name, use of CPU and memory, I/O, logged in user, and Windows services. You can launch Task Manager by pressing Ctrl+Shift+Esc, right clicking *Task Manager* in the *Start* menu, or running taskmgr.

**Process**: A list of all running processes on Windows.

**Performance**: Information about system performance, such as overall CPU usage and memory in use.

**User**: All users with sessions on the current system.

**Details**: An enhancement to the Process tab, which displays details of processes such as PID, status, and use of CPU/memory.

**Service**: All services in the system (including those that are not running).

Problem Locating and Troubleshooting

Excessive CPU usage may be caused by hardware, system/business processes, Trojans, viruses, and other factors. The following describes how to locate the processes that use the most CPU power and how to analyze and handle these processes.
1. Log in to the Windows server.
   Note: When the server is under high load, the remote connection may fail. It is recommended to log in to the server via VNC. For more information on how to log in to a Windows server via VNC, please see Login via VNC in Logging in to a Windows instance.

2. Launch Task Manager by pressing Ctrl+Shift+Esc or by right clicking Task Manager in the Start menu. On the Details tab, click CPU to sort the processes in descending order of CPU utilization.

3. Analyze the processes with high CPU utilization. Most of the processes with high CPU utilization are system, business, or exceptional processes. The following describes how to handle such processes respectively.

   i. System process.
      When you find that system processes occupy a large amount of CPU resources, check their process names carefully. Many viruses may confuse you by using names similar to those of system processes, such as svchost.exe, explore.exe, and iexplorer.exe. Next, check the location of the executable files of these processes. System processes are often located in c:\windows\system32 and accompanied with complete signatures and descriptions. Right click Process in Task Manager, click Open File Location, and then you can see the location of the executable files. If the processes are not under c:\windows\system32, the server may be poisoned. Check and kill viruses manually or using a security tool.
      Common system processes include: System Idle Process (system space process showing the percentage of CPU idleness time), system (memory management process), explorer (desktop and file management), iexplore (Microsoft browser), csrss (Microsoft client/server runtime subsystem), svchost (system process for executing DLL), Taskmgr (Task Manager), Isass (local security permission service), etc.

   ii. Exceptional process. If the processes with high CPU utilization have strange names, they may be Trojans or viruses. It is recommended that you search and confirm them (such as xmr64.exe) by using a browser. After that, check and kill them with a security tool.

   iii. Business process. If the processes with high CPU utilization are your business processes (such as iis, httpd, php, and java), it is recommended that you analyze whether your current business volume is large. If yes, you are advised to upgrade the server configuration. Otherwise, try optimize spaces for business processes.
When users find that their instance bandwidth is used too much, they often want to locate the process that occupies the most bandwidth, and then analyze and troubleshoot it. This document describes how to use the appropriate tools to locate processes with high bandwidth usage in Linux and Windows.

**Viewing Bandwidth Usage per Progress in Linux**

**NetHogs overview**

NetHogs is an open source command line tool that collects bandwidth usage per process in real time in Linux. You can install NetHogs in CentOS by executing the following command:

```
yum install nethogs
```

**How to use NetHogs**

Enter the following command in the terminal, and then you can see the available parameters of NetHogs and how to use it.

```
nethogs -h
```

When nethogs is running, press:
- q: quit
- s: sort by SENT traffic
- r: sort by RECEIVE traffic
- m: switch between total (KB, B, MB) and KB/s mode

The available parameters are as follows:
- **-d**: Sets refresh interval. Default is 1 second.
- `-t`: Tracking mode.
- `-c`: Number of updates.
- **device**: Sets the ENI to monitor. Default is eth0.

When NetHogs is running, enter the following parameters to perform corresponding operations:

- `q`: Quits.
- `s`: Sorts by sent traffic.
- `r`: Sorts by received traffic.
- `m`: Switches between total (KB, B, MB) and KB/s mode. Switching sequence: KB/s > KB > B > MB.

The following figure lists the processes by sent traffic after `nethogs -d 10` runs in Linux, which provides an example for the output of NetHogs. The list of processes can be displayed either by sent traffic or by received traffic, making it easy for you to get the process that sends/receives the most traffic.

```
<table>
<thead>
<tr>
<th>PID</th>
<th>USER</th>
<th>PROGRAM</th>
<th>DEV</th>
<th>SENT</th>
<th>RECEIVED</th>
</tr>
</thead>
<tbody>
<tr>
<td>11704</td>
<td>root</td>
<td>barad_agent</td>
<td>eth0</td>
<td>0.347 KB/sec</td>
<td>0.267 KB/sec</td>
</tr>
<tr>
<td>3340</td>
<td>root</td>
<td>/usr/local/sbin/nmcli</td>
<td>eth0</td>
<td>0.043 KB/sec</td>
<td>0.050 KB/sec</td>
</tr>
<tr>
<td>?</td>
<td>root</td>
<td>10.135.2.184:445-36.24.201.62:9971</td>
<td>eth0</td>
<td>0.000 KB/sec</td>
<td>0.000 KB/sec</td>
</tr>
<tr>
<td>31721</td>
<td>root</td>
<td>unknown TCP</td>
<td>eth0</td>
<td>0.000 KB/sec</td>
<td>0.000 KB/sec</td>
</tr>
</tbody>
</table>
```

**PID**: Process ID.

**USER**: The user who runs the process.

**PROGRAM**: Program name or IP port number.

**DEV**: Network interface to which traffic goes.

**SENT**: Traffic sent by a process per second.

**RECEIVED**: Traffic received by a process per second.

---

**Viewing Bandwidth Usage per Progress in Windows**

**Windows Resource Monitor**

Resource Monitor is a Windows utility that displays the information about the use of CPU, memory, disk, network and other resources per process.

You can launch Resource Monitor via **Task Manager -> Performance**.

You can also launch Resource Monitor by executing `resmon.exe`.

By clicking the **Network** tab in Resource Monitor, you can see the bandwidth usage of every
process. By clicking **SENT** or **RECEIVED**, you can see the processes displayed by sent or received traffic respectively and locate the process that takes up the most network resources.

### Analyzing and Troubleshooting the Process

After locating the process with high CPU utilization, you need to analyze the type of the progress:

1. Analyze whether it is a normal process (system/business/Tencent Cloud process). You can search by the process name to confirm whether it is a normal one.

2. If it is an exceptional process, the instance may be poisoned. You can terminate the process, use your security software to check and kill it, or reinstall the system after data backup.

3. If it is a Tencent Cloud component process, contact us by **submitting a ticket**, and we will help you locate and troubleshoot the problem.
   
   Common Tencent Cloud components include:
   
   - sap00x: Security component process
   - Barad_agent: Monitoring component process
   - secu-tcs-agent: Security component process

4. If it is a normal business progress, analyze whether there is a large number of network visits, and whether you can break the resource bottleneck of network bandwidth by compressing files. Otherwise, you are advised to upgrade the instance.
Microsoft provides Get started with Remote Desktop on Mac to describe two ways to obtain Microsoft Remote Desktop for Mac. You can choose one of the following 3 ways to get Remote Desktop for Mac OS:

1. Remote Desktop Beta client

We recommend downloading the beta client of the Remote Desktop for Mac provided by Microsoft from Microsoft Remote Desktop for Mac. Please note that Microsoft removed the download link from its official website on 2017, and released this beta client at HockeyApp, a subsidiary of Microsoft.

Note:
Users from Mainland China may not be able to access this address due to network issues.

2. Download Microsoft Remote Desktop from Mac App Store.

Note:
This app is not available for Mainland China users. You need an AppleID from other regions to download it.

3. You can also use a search engine to search and download the app.