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 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
  Failed to shut down or restart a CVM
  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
  Windows instance: no remote Desktop license server can provide license

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)

Downloading Remote Desktop for Mac
When you shut down or restart the CVM, a failure may occur. While it is a rare event, you can troubleshoot as follows:

### Possible Causes

- High CPU or memory usage.
- ACPI has not been installed on the Linux CVM.
- System update of the Windows CVM takes too long.
- Windows CVM has not completed initialization yet when you purchase it for the first time.
- The operating system is damaged due to installed software or viruses such as Trojan.

### Troubleshooting

**Check CPU/memory usage**

1. Check CPU/memory usage based on the operating system of the CVM.
   - For Windows CVM: Right-click the "Taskbar" and select **Task Manager** on the CVM.
   - For Linux CVM: Execute the `top` command to view information in `%CPU` and `%MEM` columns.
2. Terminate processes with high CPU or memory usage.
   - If you still cannot shut down or restart the CVM, please execute **forced shutdown or restart**.

**Check whether ACPI has been installed**

This operation is for Linux CVM.

Execute the following command to see if an ACPI process exists.

```bash
ps -ef | grep -w "acpid" | grep -v "grep"
```
If an ACPI process exists, please execute [forced shutdown or restart](#ForcedShutdownOrRestart).
If no ACPI process exists, please install ACPI. For specific operations, see Linux Power Management Configuration.

**Check whether WindowsUpdate is running**

This operation is for Windows CVM.

On the operating system interface of Windows CVM, click **Start** > **Control Panel** > **Windows Update** to see if any patches or programs are being updated.

- Windows may perform patching when the system is shutting down. The update may take a long time, causing CVM shutdown/restart to fail. We recommend you wait for the Windows update to complete and then try to shut down or restart the CVM.
- If no patches or programs are being updated, please execute **forced shutdown or restart**.

**Check whether the CVM has completed initialization**

This operation is for Windows CVM.

When you purchase Windows CVM for the first time, initialization may take longer because Sysprep is used to distribute images. Before the initialization is complete, Windows will ignore shutdown and restart operations.

- If the Windows CVM you purchased is initializing, we recommend you wait for the initialization to complete before shutting down or restarting the CVM again.
- If the CVM has completed initialization, please execute **forced shutdown or restart**.

**Check whether the software installed is normal**

Use a check tool or antivirus software to see if the software installed on the CVM is normal or attacked by viruses such as Trojan.

- If an exception is found, the system may be damaged, causing shutdown and restart to fail. We recommend you uninstall the software, back up data or scan with security software, and then reinstall the system.
- If no exception is found, please execute **forced shutdown or restart**.
**Forced shutdown/restart**

Forced shutdown/restart provided by Tencent Cloud can be used if you fail to shut down or restart the CVM after multiple attempts. This feature allows you to force a shutdown or restart on the CVM, which may cause data loss or damage the file system.

1. Log in to the **CVM Console**.
2. On the instance management page, select the CVM you want to shut down or restart.
   - Shut down CVM: Click **More > Instance Status > Shutdown**.
   - Restart CVM: Click **More > Instance Status > Restart**.
3. In the **Shutdown** or **Restart Instance** window that pops up, check **Forced Shutdown** or **Forced Restart**, and Click **Ok**.
Check **Forced Shutdown**, as shown below:

---

**Shutdown**

You have selected 1 Instance, Learn More

<table>
<thead>
<tr>
<th>No.</th>
<th>Instance Name</th>
<th>Instance ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Unnamed</td>
<td></td>
<td>Can be shut down</td>
</tr>
</tbody>
</table>

Are you sure you want to shut down the selected instances?

- [ ] CVM No Charge when Shut down

---

**No Charge When Shut Down is available when the following conditions are met:**

- Pay-as-you-go instances
- The instance’s system disk and the data disk are both cloud disks.
- Non-GPU and FPGA-based instances

- [ ] Forced shutdown

---

Forced shutdown may lead to data loss or file system damage. This is only allowed when the instance cannot be shut down normally.

---

[OK]  [Cancel]
Check **Forced Restart**, as shown below:

### Restart Instance

You have selected 1 Instance. 

<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: 2020-04-27 15:00:30

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

Diagnostic Tool

You can use 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, you can select Open all ports to open all commonly used ports of the CVM to the Internet, and try to log in remotely again.
Modifying security group configurations

If you do not want to use **Open all ports** to open all commonly used ports of the CVM to the Internet, or you need to customize the remote login port, you can use custom configuration of the inbound and outbound rules of the security group to resolve remote login failures. For more information, see [Modifying Security Group Rules](#).
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 ssdh service is Launch**

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

   ```bash
   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.

   ```bash
   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.

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: 94 total, 1 running, 93 sleeping, 0 stopped, 0 zombie
%CPU(s): 0.3 us, 0.0 sy, 0.0 ni, 99.7 id, 0.0wa, 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.
This document describes the possible causes of Windows instance login failures and their troubleshooting methods. You can follow the instructions to identify the cause of your problem and learn how to fix it.

**Possible Causes**

Failure to log into a Windows instance may be the result of:

- Password issues
- High bandwidth utilization
- High server load
- Improper remote port configuration
- Improper security group rules
- Exception caused by the firewall or security software
- Authentication error during access through the remote desktop

If you cannot troubleshoot with a diagnosis tool, we recommend that you **log in through VNC** and follow the instructions on the CVM.

**Troubleshooting**

**Logging in through VNC**

If you cannot log in to a Windows instance through RDP or remote access software, you can log in through VNC instead, which helps you identify the cause of the problem.

1. Log in to the **CVM console**.
2. On the instance management page, select the instance to access and click **Log In**, as shown in the following figure:
3. In the **Log into Windows instance** window that appears, select **Alternative methods (VNC)** and click **Log In Now**.

If you forget the password for the instance, you can reset it in the console. For more information, see **Resetting the Instance Password**.

4. In the login window that appears, select **Send CtrlAltDel** in the upper-left corner, and press **Ctrl-Alt-Delete** to open the system login window, as shown in the following figure:
Problem: the login attempt failed because you forgot the password, entered an incorrect password, or failed to reset your password.

Solution: reset the password for this instance in the CVM console and restart the instance.

Procedure: see Resetting the Instance Password for the detailed procedure.

High bandwidth utilization

Procedure:
1. Log in to the instance by using VNC login.
2. Check the bandwidth utilization of the instance and troubleshoot accordingly. For details, see Login Failure Due to High Bandwidth Occupation.

High server load

Problem: Cloud Monitor shows a high load on the server’s CPU, and the system cannot be accessed remotely or access is slow.

Possible cause: viruses, trojans, third-party antivirus software, application exceptions, driver exceptions, and automatic updates of software on the backend may lead to high CPU utilization, causing CVM login failures or slow access.

Procedure:
1. Log in to the instance by using VNC login.
2. In Task Manager, locate the process that causes the high load. For details, see Failed to Log In to a Windows CVM Due to High CPU and Memory Usage.

Improper remote port configuration

Problem: the remote access attempt to an instance failed, the remote access port is not the default port or has been modified, or port 3389 is not open.

Diagnosis: ping the public IP address of the instance to check network connectivity and run telnet to check whether the port is open.


Improper security group rules

Procedure: Troubleshoot with the security group (port) verification tool.

For a remotely logged-in Windows instance, you need to open port 3389.
If the problem is caused by a port issue of the security group, you can use the **Open all ports** function to open all ports.

To define a custom rule for the security group, see [Adding Rules for a Security Group](#).

**Exception caused by the firewall or security software**

**Problem:** the login attempt failed due to the CVM firewall or security software.

**Diagnosis:** log in to a Windows instance through VNC to check whether the firewall is enabled and whether security software such as 360 Total Security or security dongles are installed on the server.
This operation involves shutting down the CVM firewall. To perform it, check that you have the corresponding permission.

**Procedure**: shut down the firewall or the installed security software, and then try to access remotely again. For example, you can shut down the firewall of Windows Server 2016 as follows:

1. Log in to the instance by using **VNC login**.
2. On the desktop of the operating system, click 📋 and choose **Control Panel**.
3. In the **Control Panel** window, click **Windows Firewall**.
4. In the **Windows Firewall** window, click **Enable or Disable Windows Firewall** on the left to open **Custom Settings**.
5. Set **Private Network Settings** and **Public Network Settings** to **Disable Windows Firewall**, and then click **OK**.
6. Restart the instance and try to access remotely again.

**Authentication error during access through the remote desktop**

**Problem**: when you tried to log in to a Windows instance through the remote desktop, the prompt stating "Authentication error. Invalid flag is provided to the function." or "Authentication error. The required function is not supported." appears.

**Possible cause**: Microsoft released a security update in March 2018. This update fixes a remote code execution vulnerability in the Credential Security Supporting Program (CredSSP) by correcting how CredSSP validates requests during the authentication process. Both the client and server need to be updated or the preceding error may occur.

**Procedure**: install the security update (recommended). For details, see An Authentication Error Occurred when You Tried to Log In to a Windows Instance Remotely.

**Other Solutions**

After trying the preceding methods, if you still cannot log in to the Window instance, please save your self-diagnosis results and submit a ticket for assistance.
This document describes how to solve the issue of network level authentication when connecting to a Windows instance using Remote Desktop.

**Issue**

Windows Remote Desktop fails to connect to your Windows instance with the error message *The remote computer requires Network Level Authentication, which your computer does not support. For assistance, contact your system administrator or technical support.*

**Troubleshooting**

In the following steps, we use Windows Server 2016 as an example.

**Logging in to the CVM using VNC**

1. Log in to the CVM Console.
2. On the instance management page, find the desired CVM instance. Click Log In, as shown in the following figure:
3. In the **Log in to Windows instance** window that appears, select **Alternative login methods (VNC)**. Click **Log In Now** to log in to the CVM.

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

![Remote Command Interface]

**Modifying the Windows registry**

1. In the operating system interface, click ![regedit icon]. Enter `regedit` and press **Enter** to open the Registry Editor.

2. Using navigation tree on the left-side, navigate to **Computer > HKEY_LOCAL_MACHINE > SYSTEM > CurrentControlSet > Control > Lsa**. In the right-side pane, select **Security**
**Packages**, as 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** under **Value Data** and click **OK**, as shown in the following figure.
5. Using navigation tree on the left-side, navigate to **Computer > HKEY_LOCAL_MACHINE > SYSTEM > CurrentControlSet > Control > SecurityProviders**. In the right-side pane, select **SecurityProviders**, as shown in the following figure:

![Registry Editor](image)

6. Double-click **SecurityProviders** to open the **Edit Multi-String** dialog box.

7. Append `,credssp.dll` to the end of the **Value Data** field in the **Edit Multi-String** dialog box. Click **OK** as shown in the following figure:

![Edit String](image)

8. Close the registry editor and restart the instance. You can now log in remotely.
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

Problem Description

When users try to log in to a Windows instance through a Remote Desktop Connection, an error occurs.

- The error message states "Authentication error. The token supplied to the function is invalid."
- "Authentication error. The requested function is not supported."

Problem Analysis

Microsoft published a security update in March 2018. By correcting how the Credential Security Support Provider protocol (CredSSP) validates requests during authentication, this update fixes the remote code execution vulnerability in the CredSSP. Both the client and server need to install the security update, or the preceding error may occur.

Remote connection fails in the following conditions:

- Condition 1: the security update is installed on the server but not on the client, and the "force updated clients" policy is configured.
- Condition 2: the security update is installed on the client but not on the server, and the "force updated clients" policy is configured.
- Condition 3: the security update is installed on the client but not on the server, and the "mitigated" policy is configured.

Solution

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

1. Log in to the CVM console.
2. On the instance management page, find the target CVM instance and click Log In.
3. In the Log in to Windows instance window that appears, select Alternative login methods (VNC) and click Log In Now.
4. In the login window that appears, select Send CtrlAltDel in the upper-left corner and click Ctrl-Alt-Delete to go to the system login page.

Solution 1: Install the security update (recommended)

Install the security update on the unpatched client or server. For updates for different operating systems, see CVE-2018-0886 | CredSSP remote code execution vulnerability. This solution uses Windows Server 2016 as an example.

In other operating systems, you can use the following methods to go to Windows Update:

- Windows 10: Settings > Update and Security
- Windows 7: Control Panel > System and Security > Windows Update

1. On the desktop, click and choose Settings.
2. In the Settings window, choose Update and Security.
3. On the Update and Security page, choose Windows Update and click Check for updates.
4. Click Install updates.
5. After the installation is completed, restart the instance to finish the update.

Solution 2: Modify the policy

In a CVM with the security update installed, set the Encryption Oracle Remediation policy to vulnerable. This solution uses Windows Server 2016 as an example. Complete the following steps:

If no group policy editor is available in the Windows 10 Home operating system, you can modify the policy in the registry. For details, see Solution 3: Modify the registry.

1. On the desktop, click , enter gedit.msc, and press Enter to open "Local Group Policy Editor".

You can also press Win+R to open the Run dialog box.
2. In the left-side navigation tree, choose **Computer Configuration > Administrative Templates > System > Credentials Delegation** and double-click **Encryption Oracle Remediation**.

3. In the **Encryption Oracle Remediation** window, select **Enabled** and set **Protection Level** to **Vulnerable**.

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

**Solution 3: Modify the registry**

1. On the desktop, click 🔍, enter `regedit`, and press **Enter** to open "Registry Editor".

   You can also press **Win+R** to open the **Run** dialog box.

2. In the left-side navigation tree, choose **Computer > HKEY_LOCAL_MACHINE > Software > Microsoft > Windows > CurrentVersion > Policies > System > CredSSP > Parameters**.

   If this path does not exist, create one manually.

3. Right-click **Parameters**, choose **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**.

5. Restart the instance.

**Related Documents**

- CVE-2018-0886 | CredSSP remote code execution vulnerability
- CredSSP updates for CVE-2018-0886
This document describes common problems you may encounter when logging in to Windows CVM on Mac through Microsoft Remote Desktop and how to solve them.

Problems

- When logging in to Windows CVM through Microsoft Remote Desktop, you get a “The certificate couldn't be verified back to a root certificate” prompt.

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

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, locate the CVM you need, 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 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.
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**

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

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

5. Restart the instance and try to connect 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.

![Windows Security dialog box](image)

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]

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 ![Windows PowerShell icon] 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:

![Advanced sharing settings window](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: 2020-04-25 11:57:15

This document describes how to troubleshoot the issue of Windows CVM login failure due to high CPU or memory usage.

The following procedure uses Windows Server 2012 R2 as an example. The specific procedure may vary depending on your operating system.

Possible Causes

High CPU or memory usage may cause service slowdown or login failure. The causes can range from hardware, system processes, service processes, or even trojans or viruses. You can use Cloud Monitor to create alerts to track CPU or memory usage. You will be alerted when CPU or memory usage exceeds the set threshold values.

Troubleshooting

1. Identify the process causing high CPU or memory usage.
2. Analyze the process.
   - If it is an abnormal process, it may be caused by a virus or trojan. Terminate the process and use an antivirus application to scan your system.
   - If it is a normal process, see if a change to parameters caused the high usage and if it can be optimized.
   - If it is a Tencent Cloud component process, submit a ticket for further assistance.

Tools

Task Manager: this is a tool to manage programs and processes included with Microsoft Windows systems. It provides information about computer performance and running software, including the names of running processes, CPU load, I/O details, logged-in users, and Windows services.
• **Processes**: a list of all running processes.
• **Performance**: system performance statistics such as overall CPU usage and memory usage.
• **Users**: all current user sessions.
• **Details**: a detailed list of running processes, including information such as PID, status, CPU usage, and memory usage.
• **Services**: a list of services, including those that are not running.

## Troubleshooting

### Logging in to CVM instances using VNC

If you cannot log in to your CVM instance due to high CPU or memory load, we recommend [Logging in to Windows Instances via VNC](#).

1. Log in to the [CVM Console](#).
2. On the instance management page, find the desired CVM instance and click **Log In**.
3. In the [Log in to Windows instance](#) window that appears, select **Alternative login methods (VNC)** and click **Log In Now** to log in to the CVM.
4. In the login window that appears, select **Send Remote Command** in the top-left corner. Click **Ctrl-Alt-Delete** to enter the system login interface.

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

![Task Manager in Taskbar](image)

2. In “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

Identify the process causing the issue. Analyze it to find the root cause and implement a fix.

A system process is causing the issue

If a system process is causing the issue, follow these steps:

1. Verify the name of the process.
   Several viruses use names that are very similar to system processes, such as svchost.exe, explore.exe, or iexplorer.exe.

2. Locate the executable file that corresponds to the process.
   System processes are usually located in C:\Windows\System32. They should all have valid digital
signatures and descriptions. To locate the corresponding executable file, select a process in Task Manager, right-click the process, and select **Open file location**.

- If the executable file is not in `C:\Windows\System32`, it is likely that your CVM instance is infected. Use an antivirus application or manually fix the issue.
- If the executable file is in `C:\Windows\System32`, reboot your instance or close non-essential processes.

The following is a list of typical system processes:

- **System Idle Process**: The System Idle Process indicates the percentage of time that the processor is idle.
- **system**: The system process is responsible for the system memory and compressed memory in the NT kernel.
- **explorer**: The explorer process is responsible for desktop and file management.
- **iexplore**: The iexplore process is the process for Microsoft Internet Explorer.
- **csrss**: The csrss process is responsible for console windows, creating and/or deleting threads, and implementing some portions of the 16-bit virtual MS-DOS environment.
- **svchost**: The svchost process is a system process that can host one or more Windows services in the Windows NT family of operating systems.
- **Taskmgr**: The Taskmgr process is the process for Task Manager.
- **Isass**: The Isass process is a process in Microsoft Windows operating systems that is responsible for enforcing the security policy on the system.

**Strange processes are causing the issue**

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

- Use an antivirus application to remove the virus or trojan. Back up data and reinstall the operating system if necessary.
- If the process is not a virus or trojan, reboot your CVM instance and close non-essential processes.

**A service process is causing the issue**

If you find that a service process, such as IIS, HTTPD, PHP, or Java, is causing the issue, further investigate the situation.

Is your business volume high?

- If so, we recommend that you **upgrade your CVM instance**. Otherwise, consider optimizing your service deployment.
- If not, use logs to troubleshoot and see if a misconfigured parameter is causing the issue.
A Tencent Cloud process is causing the issue.

- If the process causing the issue is a Tencent Cloud component process, submit a ticket for further assistance.
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:
1) Remote access to the server is not enabled
2) The remote computer is turned off
3) 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 Status](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”.
8. In “Windows Defender Firewall”, check the status of Windows Defender Firewall as shown below:

- 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.
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**.

```
Microsoft Windows [Version 6.3.9600]
© 2013 Microsoft Corporation. All rights reserved.
C:\Users\Administrator>ping 193.112.0.0
Pinging 193.112.0.0 with 32 bytes of data:
Reply from 193.112.0.0: bytes=32 time<1ms TTL=127
Reply from 193.112.0.0: bytes=32 time<1ms TTL=127
Reply from 193.112.0.0: bytes=32 time<1ms TTL=127
Reply from 193.112.0.0: bytes=32 time<1ms TTL=127
Ping statistics for 193.112.0.0:
   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:

![CVM Console Screenshot]

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
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 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:

![PortNumber in Tcp](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:

![PortNumber in RDP-Tcp](image)

- If they are not the same, execute Step 6.
- 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:

![Services Window](image)

**Other Operations**

If you are still unable to remotely log in after performing the above-mentioned operations, please Submit a ticket.
Windows instance: no remote Desktop license server can provide license

Last updated: 2020-04-24 15:51:46

This document describes how to manage alarm prompts such as "Remote session has been disconnected as no remote desktop authorization server is available for licensing" when you try to remotely connect to a Windows instance.

Problem

When you try to connect to a Windows instance by using Windows Remote Desktop, a prompt stating "Remote session has been disconnected as no remote desktop authorization server is available for licensing. For assistance, please contact your system administrator" appears, as shown in the following figure:

![Remote Desktop Connection](image)

Problem Analysis

The possible causes to this problem include but are not limited to the following. Therefore, always analyze the problem based on the actual situation.

- The RDP-TCP limit is set by the system by default, and it allows only one session for each user. If the account has been logged in, no additional sessions can be established.
- The "Remote Desktop Session Host" role feature was added by the system, but the validity period of the feature has expired.
  The "Remote Desktop Session Host" role feature is free for use for 120 days. After the period, you must pay for the feature to continue to use it.
Solution

Logging in to the CVM through VNC

1. Log in to the CVM console.
2. On the instance management page, locate the target CVM instance and click Log In, as shown in the following figure:

3. In the Log in to Windows instance window that appears, select Alternative login methods (VNC), and click Log In Now to log in to the CVM.
4. In the login window that appears, select Send Remote Command in the upper-left corner, and press Ctrl-Alt-Delete to go to the system login interface, as shown in the following figure:

Solution 1: Modify the policy configuration
1. On the operating system interface, click \(\text{\textcolor{blue}{Start}}\) to open a Windows PowerShell window.

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

3. In the left navigation tree, choose **Computer Configuration > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Session Host > Connections**, and double-click **Limit number of connections**, as shown in the following figure:

![Local Group Policy Editor](image)

4. In the "Limit number of connections" window that appears, modify **Maximum RD connections supported** and click `OK`, as shown in the following figure:
5. Switch to the Windows PowerShell window.
6. In the Windows PowerShell window, enter `gpupdate` and press Enter to update the policy.

**Solution 2: Delete the "Remote Desk Session Host" role**

If you want to keep the "Remote Desktop Session Host" role, skip this step and go to the Microsoft official website to purchase and configure the appropriate certificate.

1. On the operating system interface, click to open Server Manager.
2. Click **Manage** in the upper-right corner of the "Server Manager" window and select **Delete roles and features**, as shown in the following figure:

![Server Manager window](image)

3. In the "Delete roles and features" wizard, click **Next**.
4. On the "Delete server roles" page, uncheck **Remote Desktop Services**. In the prompt box that appears, select **Remove Feature**.
5. Click **Next** twice.
6. Check **Restart the destination server automatically if required**, and click **Yes** in the prompt box that appears.
7. Click **Delete**.
   Wait for the CVM to restart.
Network Namespace Creation Failure

Problem Description

When you create a new network namespace, the corresponding command gets stuck and does not continue. Dmesg message: "unregister_netdevice: waiting for lo to become free. Usage count = 1"

Causes

This problem is caused by a bug in the kernel. The following kernel versions have this bug:

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

Solution

Upgrade the kernel to version 4.4.0-98-generic. In this version, the bug has already been fixed.

Directions

1. Execute the following command to check the current kernel version.

   ```bash
   uname -r
   ```

2. Execute the following command to 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 displayed, it means this version exists in the source and is available for upgrade.

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

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

4. Execute the following command to restart the system.

```
sudo reboot
```

5. Execute the following command to enter the system to check the kernel version.

```
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.

<table>
<thead>
<tr>
<th>Cause</th>
<th>Probability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password and SSH key issues</td>
<td>15%</td>
</tr>
<tr>
<td>High CPU/memory usage</td>
<td>12%</td>
</tr>
<tr>
<td>Identity verification error occurring with Windows instance remote desktop</td>
<td>8%</td>
</tr>
<tr>
<td>Remote connection method error</td>
<td>6%</td>
</tr>
<tr>
<td>Incorrect security group settings</td>
<td>6%</td>
</tr>
<tr>
<td>Server remote access permission settings issues</td>
<td>6%</td>
</tr>
<tr>
<td>Server isolated due to being in violation/arrears</td>
<td>4%</td>
</tr>
<tr>
<td>Login exception caused by firewall/security software settings</td>
<td>4%</td>
</tr>
<tr>
<td>Public network bandwidth is 0</td>
<td>3%</td>
</tr>
</tbody>
</table>

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:

   ![CVM Console Login](image)

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.
   
   ```bash
   yum install iftop -y
   ```

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

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

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

   - `<` and `=>` indicate 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.

```
lsf -i | grep IP
```

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

```
lsf -i | grep 201.205.141.123
```

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

```
sshd 12145  root  3u  IPV4 3294018  0t0  TCP 10.144.90.86:ssh->203.205.141.123:58614(ESTABLISHED)
sshd 12179 ubuntu 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 : 2020-04-20 18:33:19

Problem Description

The user experiences high latency when logging in to CVMs located in North America.

Problem Analysis

Due to the limited number of international egress routers within the country, high concurrency may cause linkage congestion and unstable access. Tencent Cloud has reported this issue to ISPs. If you need to manage within the country a CVM located in North America, 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 “1. Select a model” of the “Custom Configuration” page, choose Hong Kong, China.
   - Click here to purchase >>
   - Windows operating system supports login to both Windows and Linux CVMs located in North America, which is recommended to purchase.
   - When purchasing the Windows CVM located in Hong Kong (China), you need to buy at least 1 Mbps bandwidth. Otherwise, you cannot log in to the jump server.

2. After the purchase is completed, log in to the Windows CVM located in Hong Kong (China) based on your needs:
   - Log in to the Windows instance using the RDP file
   - Logging into Windows instance via remote desktop
   - Logging into Windows instance via VNC
3. Log in to your CVM located in North America from the Windows CVM located in Hong Kong (China) based on your needs:
   - Log in to a Linux CVM located in North America
     - Log into Linux instance using standard login method
     - Logging into Linux instance via remote login tools
     - Logging into Linux instance via SSH key.
   - Log in to a Windows CVM located in North America
     - Log in to the Windows instance using the RDP file
     - Logging into Windows instance via remote desktop
     - Logging into Windows instance via VNC.
Website Access Failure

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.

     ![Netstat Command Example](image)

   - **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.
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>The following are the test results of Tencent's domain name.</th>
<th></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.
CVM Network Latency and Packet Loss

Problem Description

When you access the CVM from a local machine or access other network resources from the CVM, network stutters. Packet loss or high latency is found when you execute the `ping` command.

Problem Analysis

Packet loss or high latency may be caused by backbone network congestion, network node failure, high load or system configuration. You can use MTR for further diagnosis after ruling out CVM problems.

MTR is a network diagnostic tool and provides reports that help you locate networking problems.

Solution

This document takes Linux and Windows CVM as an example to describe how to use MTR and analyze the report.

Please see the MTR introduction and instructions corresponding to the host operating system.

- WinMTR Introduction and Instructions (for Windows)
- MTR Introduction and Instructions (for Linux)

WinMTR Introduction and Instructions (for Windows)

WinMTR is a free network diagnostic tool for Windows integrated with Ping and tracert features. Its graphical interface allows you to intuitively see the response time and packet loss of each node.

Installing WinMTR

1. Log in to the Windows CVM.
2. On the operating system interface, visit the official website (or other legal channels) through the browser to download the WinMTR installer package corresponding to your operating system.
3. Unzip the WinMRT installer package.
Using WinMTR

1. Double-click WinMTR.exe to open WinMRT tool.
2. Enter the IP or domain name of the host in the Host field. Then click **Start** as shown below:

   ![WinMTR Tool](image1)

   1. **Copy Text to clipboard**
   2. **Copy HTML to clipboard**
   3. **Export TEXT**
   4. **Export HTML**

<table>
<thead>
<tr>
<th>Hostname</th>
<th>Nr</th>
<th>Loss %</th>
<th>Sent</th>
<th>Recv</th>
<th>Best</th>
<th>Avg</th>
<th>Worst</th>
<th>Last</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>192.168.100.12</td>
<td>1</td>
<td>0</td>
<td>28</td>
<td>28</td>
<td>1</td>
<td>2</td>
<td>13</td>
<td>12</td>
</tr>
<tr>
<td>192.168.110.130</td>
<td>2</td>
<td>0</td>
<td>28</td>
<td>28</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

3. Wait for WinMTR to run for a while and click **Stop** to stop the test, as shown below:

   ![WinMTR Tool](image2)

   ![WinMTR Tool](image3)
Key information of the test result is as shown below:

- **Hostname**: IP or name of each host passed through on the 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 by default to test the network connection between two nodes.

#### Installing MTR Installation

Currently, all released versions of Linux have MTR preinstalled. If not, you can install MTR using the following command:

- For **CentOS**:
  
  ```
  yum install mtr
  ```

- For **Ubuntu**:
  
  ```
  sudo apt-get install mtr
  ```

### MTR Parameters

- **-h/--help**: Displays help menu.
- **-v/--version**: Displays MTR version information.
- **-r/--report**: Outputs the result in a report.
- **-p/--split**: Different from **--report**, **-p/--split** lists the result of each trace separately.
- **-c/--report-cycles**: Sets the number of data packets sent per second. Default is 10.
- **-s/--psize**: Sets the size of each data packet.
- **-n/--no-dns**: Disables domain name resolution for IP address.
- **-a/--address**: Sets the IP address from which data packets are sent. It is mainly used for scenarios with a single host and multiple IP addresses.
- **-4 : IPv4**
- **-6 : IPv6**
Use Cases

Take a local machine to server (IP: 119.28.98.39) as an example.

Execute the following command to output the diagnostic result of MTR in a report.

```
mtr 119.28.98.39 -- report
```

A message similar to the one below is returned:

```
[root@VM_103_80_centos ~]# mtr 119.28.98.39 -- report
Start: Mon Feb 5 11:33:34 2019
HOST:VM_103_80_centos Loss% Snt Last Avg Best Wrst StDev
1. |-- 100,119,162,130 0.0% 10 6.5 8.4 4.6 13.7 2.9
2. |-- 100,119,170,58 0.0% 10 0.8 8.4 0.6 1.1 0.0
3. |-- 10,200,135,213 0.0% 10 0.4 8.4 0.4 2.5 0.6
4. |-- 10,200,16,173 0.0% 10 1.6 8.4 1.4 1.6 0.0
5. |-- 14,18,199,58 0.0% 10 1.0 8.4 1.0 4.1 0.9
6. |-- 14,18,199.25 0.0% 10 4.1 8.4 3.3 10.2 1.9
7. |-- 113,96,7,214 0.0% 10 5.8 8.4 3.1 10.1 2.1
8. |-- 113,96,0,106 0.0% 10 3.9 8.4 3.9 11.0 2.5
9. |-- 202,97,90,206 30.0% 10 2.4 8.4 2.4 2.5 0.0
10. |-- 202,97,94,77 0.0% 10 3.5 4.6 3.5 7.0 1.2
11. |-- 202,97,51,142 0.0% 10 164.7 8.4 161.3 165.3 1.2
12. |-- 202,97,49,106 0.0% 10 162.3 8.4 161.7 167.8 2.0
13. |-- ix-xe-10-2-6-0.tcore2.LVW 10.0% 10 168.4 8.4 161.5 168.9 2.3
14. |-- 180,87,15,25 10.0% 10 348.1 8.4 347.7 350.2 0.7
15. |-- 180,87,96,21 0.0% 10 345,0 8.4 343.4 345.0 0.3
16. |-- 180,87,96,142 0.0% 10 187.4 8.4 187.3 187.6 0.0
17. |-- ?? 100.0% 10 0.0 8.4 0.0 0.0 0.0
18. |-- 100,78,119,231 0.0% 10 187.7 8.4 187.3 194.0 2.5
19. |-- 119,28,98,39 0.0% 10 186.5 8.4 186.4 186.5 0.0
```

The main output information is as follows:

- **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 in the response time of data packets at this node.

Report analysis and troubleshooting
Due to network asymmetry, we recommend you collect two-way MTR data (from the local machine to the destination server and from the destination server to the local machine) if any network error occurs.

1. According to the report, check whether there is packet loss on the destination IP.
   - If there is no packet loss on the destination IP, network conditions are normal.
   - If there is packet loss on the destination IP, perform Step 2.
2. Check the result to locate the node where the first packet loss occurs.
   - If packet loss occurred at the destination server, it may be caused by incorrect network configuration of the destination server. Please check its firewall configuration.
   - If packet loss occurred at the first three hops, it may be caused by network problems of the local machine’s ISP. If the problem also happens when you access other addresses, report it to your ISP.
   - If packet loss occurred at the hops closing to the destination server, it may be caused by network problems of the destination server’s ISP. Submit a ticket to report the problem. When submitting the ticket, please attach screenshots of MTR test results from the local machine to the destination server and from the destination server to the local machine.
Problem

A failed ping test from a local server to an instance may be caused by the following:

- Incorrect server configuration
- Unsuccessful domain name resolution
- Linkage failure

If the local network is normal (i.e. other websites can be pinged), you can troubleshoot this problem by the following steps:

- Check whether the instance is configured with a public IP
- Check the security group configuration
- Check the OS configuration
- Check the domain name registration
- Other operations

Directions

Check whether the instance is configured with a public IP

Only 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.

1. Log in to the CVM Console.
2. On the “Instances” page, select the ID/name of the instance to be pinged to enter the instance details page, as shown below:
3. Check whether the instance is configured with a public IP in “Network Information”.
   - If yes, please check security group configuration.
   - If no, please bind an elastic public IP with the CVM.

### Check the security group configuration

Security group is a virtual firewall that allows you to control the inbound and outbound traffic of the associated instance. You can specify the protocol, port and policy of a security group rule. Check whether the ICMP protocol used in ping test is allowed in the security group associated with the instance. You can view the security group associated with the instance and its inbound/outbound rules by the following steps:

1. Log in to the CVM Console.
2. On the “Instances” page, select the ID/name of the instance to be configured with the security group to enter the instance details page, as shown below:
3. Select the **Security Groups** tab to enter the security group management page of the instance, as shown below:
4. Verify whether the security group associated with the instance allows ICMP based on the security group used by the instance and the detailed inbound and outbound rules.
   - If yes, please check OS configuration.
   - If no, please configure the ICMP protocol policy as allow.

**Check the system configuration**

Choose different methods to check the system configuration based on its operating system.

- For Linux OS, please [check Linux kernel parameters and firewall configuration](# CheckLinux).
- For Windows OS, please check Windows firewall configuration.

**Checking kernel parameters and firewall configuration 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.

**Checking kernel parameters icmp_echo_ignore_all**

1. Log in to the instance.
2. Execute the following command to view the icmp_echo_ignore_all configuration of the system.
   ```bash
cat /proc/sys/net/ipv4/icmp_echo_ignore_all
   ```
   - If 0 is returned, the system allows all ICMP Echo requests. Please check the firewall configuration.
   - If 1 is returned, the system blocks all ICMP Echo requests. Please execute Step 3.
3. Execute the following command to modify the configuration of the kernel parameter icmp_echo_ignore_all.
   ```bash
echo "1" > /proc/sys/net/ipv4/icmp_echo_ignore_all
   ```
Checking firewall configuration

Execute the following command to check whether firewall rules of the current server and corresponding rules for ICMP are disabled.

```bash
iptables -L
```

- If the following result is returned, corresponding rules for ICMP are not disabled. Please check the domain name registration.

  ```
  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
  ```

- If the result is returned that corresponding rules for ICMP are disabled. Please execute the following command to enable them.

  ```
  #Chain INPUT
  iptables -A INPUT -p icmp -- icmp-type echo-request -j ACCEPT
  
  #Chain OUTPUT
  iptables -A OUTPUT -p icmp -- icmp-type echo-reply -j ACCEPT
  ```

Checking firewall configuration on Windows

1. Log in to the instance.

2. Open Control Panel to select Windows Firewall

3. On the "Windows Firewall" page, select Advanced settings

4. In the pop-up ‘Windows Firewall with Advanced Security’ window, check whether inbound and outbound rules for ICMP are disabled.

   - If inbound and outbound rules for ICMP are disabled, please enable them.

   - If inbound and outbound rules for ICMP have been enabled, please check the domain name registration.
Check whether the domain name has been registered

If you can ping the public IP but not the domain name, it may be because the domain name has not been registered or domain name resolution has an exception.

The Ministry of Industry and Information Technology stipulates that websites that have not obtained a permit or have not fulfilled ICP filing must not engage in Internet information services, otherwise the act is illegal. To ensure the normal running of the website, if you need to start a website, we recommend you perform website ICP filing first, obtain the ICP number issued by the Communications Authority, and then enable access.

- If your domain name has not been registered, please perform domain name ICP filing first.
- If you use Tencent Cloud domain name service, you can log in to [Domain Name Service Console](https://console.cloud.tencent.com/domain) to view the corresponding domain name situation.
- If your domain name has been registered, please check DNS.

Other Operations

If the above operations cannot solve the problem, please refer to:

- If the domain name cannot be pinged, check your website configuration.
- If the public IP cannot be pinged, contact our technical personnel to locate the problem by submitting a ticket along with relevant instance information and MTR data (from local server to CVM and from CVM to local server).
  For more information on how to use MTR, please see CVM Network Latency and Packet Loss.
Domain Name Resolution Failure (CentOS 6.X System)

Last updated: 2020-04-20 18:33:19

Problem Description

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

Possible Reasons

In CentOS 6.x operating system, initscripts with versions earlier than 9.03.49-1 has a defect due to different grep versions.

Solution

Upgrade initscripts to the latest version and generate DNS information again.

Directions

1. Log in to the CVM.
2. Execute the following command to check the initscripts version, and verify whether a defect exists because the initscripts version is earlier than 9.03.49-1.

   ```bash
   rpm --q initscripts
   ```

   A message similar to the one below is returned:

   ```
   initscripts-9.03.40-2.e16.centos.x86_64
   ```

   As shown above, the initscripts version of initscripts-9.03.40-2 is earlier than the defective version of initscripts-9.03.49-1. There is a risk of DNS information being cleared.
3. Execute the following command to upgrade initscripts to the latest version and generate DNS information again.
4. Execute the following command after the upgrade is completed to check the version information of initscripts, and verify whether the upgrade is successful.

```
yum makecache
yum -y update initscripts
service network restart
```

A message similar to the one below is returned:

```
rpm -q initscripts
```

As shown above, the version displayed is different from that before the upgrade and is newer than initscripts-9.03.49-1. This indicates that initscripts has been upgraded successfully.
Downloading Remote Desktop for Mac

Last updated: 2019-08-09 18:33:54

Microsoft provides Get started with Remote Desktop on Mac to describes 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.