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
- Failed to Reset the CVM Password or the CVM Password Is Invalid

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
Troubleshooting Issues
Instance Related Failures
Failed to shut down or restart a CVM

Last updated : 2020-04-01 11:12:01

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.

```
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:
- Check **Forced Restart**, as shown below:

```
Restart Instance

You have selected 1 Instance. Learn More

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

Are you sure you want to restart the selected instances?

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

✔ Forced restart

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

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

Last updated : 2020-04-27 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](#).
About Linux Instances
Unable to Log into a Linux Instance via SSH

Last updated: 2020-05-08 12:35:19

This document uses the CVM with CentOS 7.5 as an example to show how to troubleshoot the problem where a Linux instance cannot be logged in to by using SSH.

Problems

During login to a Linux instance by using SSH, a message indicating that the connection is unavailable or failed appears.

Locating and Troubleshooting the Issues

Step 1: Checking the security group rule configuration

Use the port verification tool for security groups to check whether security group rules are correct.

- If the problem is caused by the security group port configuration, you can use the Open All Ports feature to open all ports. You can also customize security group rules based on your actual needs. For more information, see Adding Security Group Rules.
- If the security group port configuration is correct, proceed to the next step.

Step 2: Querying the SSHD service port

1. Log in to a Linux instance by using VNC.
2. On the operating system interface, run the following command to check whether a port is listened on by the SSH daemon (SSHD) service:

   netstat -tnlp | grep sshd

   - If the following result is returned, the SSHD process is listening on port 22. In this case, submit a ticket.

   tcp 0 0 0.0.0.0:22 0.0.0.0:* LISTEN 1015/sshd
If no result is returned, the SSHD service be not launched yet. In this case, proceed to the next step.

**Step 3: Checking whether the SSHD service has been launched**

Run the following command to check whether the SSHD service has been launched.

```
systemctl status sshd.service
```

- If yes, submit a ticket.
- If no, run the following command to launch the SSHD service and try to log in to the Linux instance again by using SSH.

```
systemctl start sshd
```

If you still cannot log in to your instance after performing these steps, we recommend that you report this problem by submitting a ticket.
This document describes the 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
- Excessive bandwidth utilization
- High server load
- Incorrect remote port configuration
- Incorrect security group rules

If you cannot check your problem by using the self-diagnose tool, we recommend that you log in to the CVM through VNC and troubleshoot step by step.

Troubleshooting

Logging in by using VNC

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

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 in to Linux Instance" window that appears, 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 **Resetting the Instance Password**.

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

**SSH problems**

**Problem**: during login to a Linux instance by using SSH, a message indicating that the connection is unavailable or failed appears.

**Steps**: see **Unable to Log In to a Linux Instance by Using SSH** for troubleshooting.

**Password problems**

**Problem**: unable to log in because you forget the password, enter it incorrectly, or fail to reset it.

**Solution**: reset the password of this instance in the Tencent Cloud console, and restart the instance.

**Steps**: for information on how to reset the password of an instance, see **Resetting the Instance Password**.

**Excessive bandwidth utilization**

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

**Steps**:

1. Log in to the instance by using VNC.
2. Check the bandwidth utilization of the instance and troubleshoot accordingly. For details, see **Unable to Log In Due to High Bandwidth Utilization**.

**High server load**
Problem: Cloud Monitor shows that load of the server CPU is high, and the system cannot be accessed remotely 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, causing CVM login failures or slow access.

Steps:
1. Log in to the instance by using VNC.
2. In “Task manager”, find the process with a high load. For details, see Unable to Log In Due to High CPU and Memory Usage.

Incorrect remote port configuration

Problem: the remote port is inaccessible, the remote access port is not the default port or has been modified, or port 22 is not open.

Diagnosis: check whether the public IP address of the instance can be pinged through. Run the `telnet` command to check whether the port is open.

Steps: see Unable to Log In Remotely Due To Port Issues.

Incorrect security group rules

Problem: unable to log in due to incorrect security group rules.

Steps: troubleshoot by using the port verification tool for security groups.

If the problem is caused by the incorrect security group port configuration, you can use Open All Tools to open all ports.

If you need to define a custom rule for the security group, see Adding Rules to Security Groups for information on how to reconfigure security group rules.

Other Solutions

If you still cannot log in to the Linux instance after trying the preceding troubleshooting methods, save your self-diagnosis results and submit a 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 `k`.

3. Enter the PID of the process which needs to be terminated, and press **Enter** to terminate it as shown below:
   
   For example, you need to terminate a process whose PID is 23.

   ![Top Command Output]

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

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

**Low CPU usage but high load average**

**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.

```
---
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, 0.0 wa, 0.0 hi, 0.0 si, 0.0 st
KiB Mem: 1016656 total, 950428 used, 66228 free, 170148 buffers
KiB Swap: 0 total, 0 used, 0 free. 452740 cached Mem
---
```

**Solution**

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

```
ps -axjf
```

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

**kswapd0 process uses much CPU**

**Problem Description**

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

**Solution**

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

```
top
```
2. Observe the state of the kswapd0 process.
   If the process is not sleeping, has run for a long time, and has been using a lot of CPU, please take Step 3 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:

   ![Login Window](image)

   **Password issues**
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.

Procedure: See [Remote Login Failure Due to Port Issues](https://intl.cloud.tencent.com/document/product/213/32540) for the detailed procedure.

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:

---

**Modifying the Windows registry**

1. In the operating system interface, click **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.
Connection to a Windows CVM through Remote Desktop was denied

Last updated: 2020-05-08 10:47:52

Problems

**Problem 1**

When trying to connect to a Windows instance by using Windows Remote Desktop, you are prompted with the message stating "The connection was denied because the user account is not authorized for remote login."

**Problem 2**

When trying to connect to a Windows instance by using Windows Remote Desktop, you are prompted with the message stating "To sign in remotely, you need the permission to sign in through Remote Desktop Services. By default members of the Remote Desktop Users group have this permission. If the group you’re in doesn’t have the permission, or if the permission has been removed from the Remote Desktop Users group, you need to be granted the permission manually."

Problem Analysis

The user is not allowed to log in to the Windows instance through Remote Desktop connections:

Solution

- If you encounter problem 1 when trying to connect to a Windows instance through Remote Desktop, you need to add the user account to the list of accounts that are permitted by the Windows instance to log in through Remote Desktop Services. For details, see Configuring the permission that allows remote login.
- If you encounter problem 2 when trying to connect to a Windows instance through Remote Desktop, you 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 permission that denies remote login.
Directions

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 and click Log In, as shown in the following figure:

3. In the "Log In to Windows Instance" window, 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 Ctrl-Alt-Delete in the upper-left corner, and click Ctrl-Alt-Delete to enter the system login interface, as shown in the following figure:

Configuring the permission that allows remote login
The following operations take Windows Server 2016 as an example.

1. On the operating system interface, click 
   enter `gpedit.msc`, and press Enter to open "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 **Allow log in through Remote Desktop Services**.
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 in the user list of "Allow log in through Remote Desktop Services".
   - If the user is not in the list, perform step 4.
   - If the user is in the list, submit a ticket.
4. Click **Add User or Group** to go to the "Select User or Group" window.
5. Enter the account that you want to use for remote login and click **OK**.
6. Click **OK** and close Local Group Policy Editor.
7. Restart the instance and try to connect to the Windows instance with the account through Remote Desktop again.

**Configuring the permission that denies remote login**

The following operations take Windows Server 2016 as an example.

1. On the operating system interface, click 
   enter `gpedit.msc`, and press Enter to open "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 in through Remote Desktop Services**.
3. In the "Properties" window, check whether the account you want to use for remote login is in the user list of "Deny log in through Remote Desktop Services".
   - If the user is in the list, remove the user account from the list and restart the instance.
   - If the user is not in the list, 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 
   ![Search icon](), 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](#)
Problems occurred when you tried to log in to a Windows CVM remotely on Mac

Last updated: 2020-04-01 11:27:55

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:

![CVM Console Screenshot](image)

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 Ctrl+Alt+Delete in the top left corner, and click Ctrl-Alt-Delete to enter the system login interface as shown below:

![Login Interface Screenshot](image)

Modifying the local group policy of the instance

1. In the operating system interface, click search, enter gedit.msc, and press Enter to open the Local Group Policy Editor.
You can also use the shortcut “Win+R” to open the Run interface.

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.

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:

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 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

![Windows Credential Manager](image)

```
Windows PowerShell
Copyright (C) 2014 Microsoft Corporation. All rights reserved.
PS C:\Users\Administrator> gpupdate /force
Updating policy...
Computer Policy update has completed successfully.
User Policy update has completed successfully.
```
2. Check to see if there is an entry for the credentials you used to log in to Windows CVM.
   - No. Follow the next step to add it.
   - Yes. Proceed to Step 4 Turn Off Password Protected Sharing

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

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

### Step 4: Turn off password protected sharing

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

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

3. Check whether you can connect to your Windows CVM now.
   - Yes. Problem solved.
   - No. Please submit a ticket.
This document describes how to troubleshoot Windows CVM login failures due to high CPU or memory utilization.

Possible Causes

High CPU or memory utilization can result in slow service responsiveness or CVM login failure. Hardware, system processes, service processes, trojans, and viruses may cause high CPU or memory utilization. You can use CloudMonitor to create a CPU or memory usage alarm threshold. In this way, you will be alerted when the CPU or memory utilization exceeds the set threshold.

Troubleshooting

1. Identify the process that causes high CPU or memory utilization.
2. Analyze the process.
   - If it is an unexpected process, it may be the result of a virus or trojan. In this case, terminate the process or scan your system by using an antivirus application.
   - If it is a service process, check whether the high CPU or memory utilization is caused by an access volume change and whether it can be optimized.
   - If it is a Tencent Cloud component process, submit a ticket and contact Tencent engineers for assistance.

Tools

**Task Manager**: this is a tool for managing applications and processes in the Microsoft Windows OS. It provides information on computer performance and running software, including the names of running processes, CPU load, memory usage, I/O details, logged-in users, and Windows services.
• **Processes**: shows a list of all running processes.
• **Performance**: provides system performance statistics such as overall CPU usage and memory usage.
• **Users**: lists all users with sessions.
• **Details**: offers a detailed list of running processes, including information such as the PID, status, CPU usage, and memory usage.
• **Services**: provides a list of all services, including those that are not running.

## Troubleshooting

### Logging in to the CVM instance by using VNC

If you cannot log in to your CVM instance due to high CPU or memory utilization, use VNC to log in to the Windows instance.

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 into Windows instance" window that appears, select **Alternative login methods (VNC)** and click **Log In Now** to log in to the CVM instance.
4. In the login window that appears, select “Send CtrlAltDel" in the upper-left corner and click **Ctrl-Alt/Delete** to go to the OS login page, as shown in the following figure:
Viewing the resource usage of processes
1. In the CVM, right-click the "taskbar" and choose **Task Manager**, as shown in the following figure:

![Task Manager](image)

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

   ![Task Manager Window](image)

   You can click the CPU or memory column to sort the processes in ascending or descending order.
Analyzing processes

Analyze processes in Task Manager to identify the causes and take appropriate measures.

A system process causes the issue

If a system process causes the issue, complete these steps:

1. Check process names.
   Some malicious programs use names that are similar to system processes, such as svchost.exe, explore.exe, and iexplorer.exe.

2. Check the locations of the executable files of processes.
   The executable files of system processes are usually located in `C:\Windows\System32` with valid
signatures and descriptions. To locate the executable file of a process, such as `svchost.exe`, right-click the process in Task Manager and choose **Open file location**.

- If the executable file is not in `C:\Windows\System32`, your CVM instance may be infected with viruses. In this case, scan for viruses with an antivirus application or manually fix the issue.
- If the executable file is in `C:\Windows\System32`, restart your CVM instance or terminate secure but unnecessary system processes.

The following lists common system processes:

- **System Idle Process**: displays the percentage of time that the processor is idle.
- **system**: indicates the memory management process.
- **explorer**: indicates the desktop and file management process.
- **iexplore**: indicates the process for Microsoft Internet Explorer.
- **csrss**: indicates the runtime subsystem on the Microsoft client or server.
- **svchost**: indicates the system process for running DLLs.
- **Taskmgr**: indicates the task manager.
- **Isass**: indicates the local security permission service.

**An unexpected process causes the issue**

If you find that a process with a strange name, such as xmr64.exe (a cryptocurrency mining malware) causes high CPU or memory utilization, your CVM instance may be infected with viruses or trojans. In this case, use a search engine to verify whether the process is a virus or trojan.

- If the process is a virus or trojan, use an antivirus application to remove the virus or trojan. Back up your data and reinstall the OS if necessary.
- If the process is not a virus or trojan, restart your CVM instance or terminate secure but unnecessary processes.

**A service process causes the issue**

If you find that a service process such as IIS, HTTPD, PHP, or Java causes the issue, further analyze the issue. For example, check whether your business volume is high.

- If yes, we recommend that you **upgrade your CVM instance**. If you do not upgrade your CVM instance, optimize your service processes.
- If no, use service error logs to further analyze the issue. For example, check whether resources are wasted due to incorrect parameter settings.

**A Tencent Cloud process causes the issue**
If a Tencent Cloud component process causes the issue, submit a ticket to contact Tencent engineers for assistance.
Failed to connect to a remote computer through Remote Desktop

Scenario

When trying to remotely connect to a Windows instance from Windows, you are prompted with the message shown in the following figure:

You cannot connect to the remote computer by using Remote Desktop 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.

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

Possible causes for this problem include but are not limited to the following. Troubleshoot the problem based on your actual circumstances.

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

Troubleshooting Steps

Checking if the instance is running

1. Log in to the CVM console.
2. On the instance management page, check whether the instance is Running, as shown in the following figure:

   ![Instance Status](image)

   - If yes, check whether the CVM has a public IP address.
   - If no, start up the Windows instance.

Checking whether the CVM has a public IP address
Check whether the CVM has a public IP address in the CVM console, as shown in the following figure:

- If yes, check whether you have purchased a public network bandwidth.
- If no, apply for an elastic public IP address and bind it with the CVM.

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

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

- If yes, increase the bandwidth to 1 Mbps or above by adjusting the network configuration.

- If no, check whether the remote login port (3389) of the instance has been opened to the Internet.

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

1. On the instance management page in the CVM console, click the ID or name of the instance for login to go to the instance details page.
2. On the “Security Groups” tab page, check whether the remote login port (port 3389 by default) has been opened to the Internet in the security group(s) bound with the instance, as shown in the
If yes, check the system settings of the Windows instance.
If no, edit the corresponding security group rules to open the port to the Internet. For directions, see Adding a Security Group Rule.

Checking the system settings of the Windows instance

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

The following operations take Windows Server 2012 as an example.

2. In the operating system of the logged-in instance, right-click \(\text{Run}\), choose Run, enter services.msc in Run, and press Enter to go to the "Service" window.
3. Double-click "Remote Desktop Services" to go to the "Remote Desktop Services Properties" window and check whether Remote Desktop Services are running, as shown in the following
If yes, go to step 4.

If no, set "Startup type" to "Automatic" and click **Start** to set "Service status" to "Running".


5. On the "Remote" tab page, check whether "Remote Desktop" is set to "Allow remote connections to this computer", as shown in the following figure:
If yes, go to step 6.
If no, set Remote Desktop to "Allow remote connections to this computer".

6. Click and choose **Control Panel** to open the control panel.
7. In "Control Panel", choose **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 in the following figure:
If the state is "On", go to step 9.
If the state is "Off", submit a ticket.

9. In "Windows Defender Firewall", select **Allow an app through Windows Firewall** to go to the "Allowed apps" window.

0. In the "Allowed apps" window, check whether "Remote Desktop" is selected in "Allowed apps and features", as shown in the following figure:
- If yes, go to step 11.
- If no, select "Remote Desktop" to permit "Remote Desktop" through Windows Firewall.

1. In "Windows Defender Firewall", select **Turn Windows Defender Firewall on or off** to go to 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 in the following figure:
If you still cannot connect to the Windows instance through Remote Desktop after completing the preceding steps, **submit a ticket.**
Remote Login Failure Due To Port Issues

Last updated : 2020-05-18 10:39:40

This article describes how to troubleshoot remote login failures caused by port problems.

The following uses a CVM instance running Windows Server 2012 as an example to describe the steps.

Tools

You can use the following tools to check if the login issues are related to ports and security group configurations:

- Self-diagnosis
- Security group (port) helper

If the problem is indeed a security group configuration problem, use **Open all ports** in the Security group (port) helper to open related ports and try to log in again. If you still cannot log in after opening the ports, refer to the following for troubleshooting.

Troubleshooting

**Checking network connectivity**

You can use the Ping command to test network connectivity from your PC. You should run the test from computers in different network environments (such as different IP ranges or ISPs) to check whether it is a local network problem or a server problem.

1. Open the command line tool on your local computer.
   - Windows: Click **Start** -> **Run** and enter **cmd**. A Command Prompt window appears.
   - MacOS: Open a Terminal window.
2. Run the following command to test network connection.

```
ping + CVM_Instance_public_IP_address
```

For example, `ping 139.199.xxx.xxx`. 
If you see results similar to what is shown in the following figure, your network connection to the CVM instance is normal. In this case, check the remote desktop configuration.

![Ping Result Example]

If Request Timeout appears, your network connection to the CVM instance is not working properly. In this case, refer to Instance IP Address Ping Failure for troubleshooting instructions.

3. Run the following command to check whether the remote port is open.

```
telnet CVM_instance_public_IP_address port_number
```

For example, `telnet 139.199.xxx.xxx 3389`, as shown in the following figure:

![Telnet Command Result]

If you see a black screen with only the cursor, that indicates the port (3389) is open. For the next step, check whether remote desktop service is enabled on the instance.

If the connection fails, as shown in the following figure, that means a network exception occurred. Check the corresponding part of the network.

![Telnet Connection Failed]

### Checking remote desktop configuration

#### Logging in to the CVM instance using VNC

It is recommended that you use VNC to login only if the standard login methods fail.
1. Log in to the CVM Console.
2. Select the desired CVM and click Log In, as shown in the following figure:

![CVM Console Log In](image)

3. The Log into Windows instance page appears. Select Alternative login methods (VNC) and click Log In Now to log in to the CVM instance.
4. The log in page appears. Select Send Ctrl-Alt-Del in the top left corner and click Ctrl-Alt-Delete to enter the system login interface, as shown in the following figure:

![System Login Interface](image)

### Checking if remote desktop is enabled on the CVM instance

1. Log in to the CVM instance. Right click This Computer from the Desktop and select 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. Check whether **Allow remote connections to this computer** under **Remote Desktop** is selected, as shown in the following figure:

![System Properties](image)

- If it is selected, remote connection is enabled. Next, you should check whether **remote access ports are open**.
- If it is cleared, select **Allow remote connections to this computer** and try to connect to the instance again.

**Checking whether remote access ports are open**

1. Log in to the CVM instance. Click ![Open](image) to open a **Windows PowerShell** window.
2. In the **Windows PowerShell** window, run the following command to check the status of remote desktop (by default, the remote desktop uses port 3389).

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

- If you see results similar to what is shown in the following figure, the status is normal. You can try to **restart remote desktop** and connect to the instance again to check whether the
If no connection is shown, remote desktop is not functioning properly. You can check whether the remote desktop ports in registry are consistent.

**Checking whether the remote desktop ports in registry are consistent**

This section describes how to check the values of **TCP PortNumber** and **RDP Tcp PortNumber**. They must be the same.

1. Log in to the CVM instance, click [ ] , select [ ] and enter `regedit`. Press Enter to open the **Registry Editor** window.
2. In the navigation pane on the left, expand the following directories: **HKEY_LOCAL_MACHINE -> SYSTEM -> CurrentControlSet -> Control -> Terminal Server -> Wds -> rdpwd -> Tds -> tcp**.
3. Locate the PortNumber in **tcp** and record the port number (3389 by default), as shown in the following figure:
4. In the navigation pane on the left, expand the following directories: **HKEY_LOCAL_MACHINE -> SYSTEM -> CurrentControlSet -> Control -> Terminal Server -> WinStations -> RDP-Tcp**.

5. Locate PortNumber in **RDP-Tcp** and check whether the PortNumber value in **RDP-Tcp** is the same as the one in **tcp**, as shown in the following figure:

   - If they are not the same, follow **Step 6**.
   - If they are the same, **restart remote desktop**.

6. Double click PortNumber in **RDP-Tcp**.

7. In the dialog box that appears, modify **Value Data** to an unoccupied port number between 0 - 65535. Ensure **TCP PortNumber** and **RDP Tcp PortNumber** are the same, and click **OK**.

8. Restart the instance using the **CVM Console**, and try to remotely connect to the instance again to check whether the connection is successful.

**Restarting remote desktop**
1. Log in to the CVM instance. Click and select Enter services.msc and press Enter to open the Services window.

2. In the Services window, right-click Remote Desktop Services and select Restart to restart the remote desktop service, as shown in the following figure:

If All Else Fails

If you are still unable to remotely log in after performing the above-mentioned steps, submit a ticket for further assistance.
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 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 showing Manage and Remove Roles and Features options](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

Last updated: 2020-04-27 14:59:14

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.

   ```
   uname -r
   ```

2. Execute the following command to check whether version 4.4.0-98-generic is available for upgrade.

   ```
   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.

   ```
   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>Possible Causes</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:

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

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

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

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

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

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

```
sshd 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.
Failed to Reset the CVM Password or the CVM Password Is Invalid

Last updated: 2020-05-14 17:50:48

This document uses Windows Server 2012 as an example to describe how to troubleshoot CVM password reset failure or ineffectiveness.

Symptoms

- After the CVM password is reset, the system prompts "The system is busy, and the password of your instance failed to be reset (7617d94c)."
- After the CVM password is reset, the new password does not take effect, and the login password is still the old password.

Possible Causes

Possible causes to both issues are:

- The Cloudbase-Init component in the CVM is damaged, modified, forbidden, or disabled.
- The security software program, such as 360 antivirus installed on the CVM, intercepts related system process components.

Troubleshooting

Based on the possible causes, use these inspection methods:

**Checking the Cloudbase-Init service**

1. Log in to the Windows instance by using VNC.
2. On the desktop, right-click and choose Run. In the Run dialog box, enter *services.msc* and press Enter to open the "Services" window.
3. Check whether the cloudbase-init service exists, as shown in the following figure:

- If yes, proceed to the next step.
- If no, reinstall the cloudbase-init service. For more information, see Installing Cloudbase-Init on Windows.

4. Double-click the cloudbase-init service to open the cloudbase-init property dialog box, as shown in the following figure:
5. On the **General** tab page, check whether the cloudbase-init startup type is **Automatic**.
   - If yes, proceed to the next step.
   - If no, set the cloudbase-init startup type to **Automatic**.

6. Switch to the **Log On** tab page and check whether **Local System account** is selected for the cloudbase-init service.
   - If yes, proceed to the next step.
   - If no, select **Local System account** for the cloudbase-init service.

7. Switch to the **General** tab page, click **Start** in the **Service status** area to manually enable the cloudbase-init service, and check whether an error appears.
   - If yes, check the security software program installed on the CVM.
   - If no, proceed to the next step.

8. On the desktop, right-click and choose **Run**. In the **Run** dialog box, enter **regedit** and press **Enter** to open the "Registry Editor" window.

9. In the leftside navigation tree, choose **HKEY_LOCAL_MACHINE > SOFTWARE > Cloudbase Solutions > Cloudbase-Init**.
0. Locate all "LocalScriptsPlugin" registry keys and check whether the LocalScriptsPlugin value is 2.

- If yes, proceed to the next step.
- If no, set the LocalScriptsPlugin value to 2.

1. On the desktop, click [This PC] and choose This PC. Check whether the CD driver is loaded under Devices and drivers, as shown in the following figure:
If yes, check the security software program installed on the CVM.
If no, start the CD-ROM driver in Device Manager.

Checking the security software program installed on the CVM

Scan for vulnerabilities in the CVM by using the installed security software program and check whether Cloudbase-Init core components are intercepted.

- If the CVM has vulnerabilities, fix them.
- If core components are intercepted, unblock them.

To prevent CVM password reset failure or ineffectiveness, we recommend that you add the following directories and files to the whitelist and trusted file area in the security software program.

- Add the following directories to the whitelist of the security software program:
  
  ```
  C:\Windows\System32\WindowsPowerShell
  C:\Program Files\Cloudbase Solutions\Cloudbase-Init\Python\Scripts
  C:\Program Files\QCloud
  C:\Program Files\Cloudbase Solutions
  ```

- Add the following files to the trusted file area:

  ```
  C:\Windows\System32\cmd.exe
  C:\Windows\SysWOW64\cmd.exe
  ```
Network Related Failures
International Linkage Latency

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

Last updated : 2020-05-09 17:04:18

This document describes how to locate and troubleshoot the problems that cause website access failure.

Possible Causes

Website access failure may be caused by network problems, firewall configurations or CVM overload.

Troubleshooting

Troubleshooting CVM problems

CVM shutdown, hardware failure, and high CPU/memory/bandwidth usage may all cause website access failure. Thus, we recommend that you check CVM running status and CPU/memory/bandwidth usage.

1. Log in to the CVM Console and verify whether the running status of the CVM instance is normal on the instance management page, as shown below:

   ![Instance Management Page]

   - If yes, please execute step 2.
   - If no, please restart the CVM instance.

2. Click the ID/name of the instance to enter its details page.
3. Select the **Monitoring** tab to view the instance resource usage, as shown below:

- If the CPU/memory usage is too high, please refer to [Failed to log in to a Windows CVM due to high CPU and memory usage](https://intl.cloud.tencent.com/document/product/213/32405) and [Failed to log in to a Linux CVM due to high CPU and memory usage](https://intl.cloud.tencent.com/document/product/213/32387) for troubleshooting.
- If the bandwidth usage is too high, please refer to [Login Failure Due to High Bandwidth Occupation](https://intl.cloud.tencent.com/document/product/213/32542) for troubleshooting.
- If CPU/memory/bandwidth usage is normal, please execute step 4.

4. Execute the following command to check whether the corresponding Web service port is being monitored normally.

   The following operations take port 80, which is commonly used in HTTP service, as an example.

   - For a Linux instance: execute the `netstat -ntulp | grep 80` command, as shown below:

```
[root@VM_2_184_centos ~]# netstat -ntulp | grep 80
tcp 0 0 0.0.0.0:80 0.0.0.0:* LISTEN 1309/httpd
```
For a Windows instance: open the CMD command line tool to execute the `netstat -ano|findstr :80` command, as shown below:

![Netstat Command Output](image)

- If the port is being monitored normally, please execute step 5.
  - If the port is not being monitored normally, please check whether the Web service process is launched or correctly configured.

5. Check whether the corresponding Web service port is opened in the firewall configuration.

- For a Linux instance: execute the `iptables -vnL` command to check whether iptables opens port 80.
  - If port 80 is open, please troubleshoot network-related problems.
  - If port 80 is not open, please execute the `iptables -I INPUT 5 -p tcp --dport 80 -j ACCEPT` command to open it.

- For a Windows instance: click Start > Control Panel > Windows Firewall on the OS interface to check whether Windows firewall configuration is off.
  - If yes, please troubleshoot network-related problems.
  - If no, please turn off the Windows firewall configuration.

### Troubleshoot network-related problems

Network problems can also cause network access failure. You can execute the following command to check whether the network has packet loss or high latency.

```
ping the public IP of the server
```

- If a result similar to the one below is returned, there is packet loss or high latency. Please use MTR for troubleshooting. For more information, please see CVM Network Latency and Packet Loss.
If there is no packet loss or high latency, please troubleshoot security group problems.

**Troubleshoot security group problems**

Security group is a virtual firewall that allows you to control the inbound and outbound traffic of the associated instance. You can specify protocols, ports and policies for security group rules. If you did not open the ports related to the Web processes, website access failure may occur.

1. Log in to the CVM Console and click the ID/name of the instance to enter its details page.
2. Click the **Security Group** tab to view the bound security groups and their outbound and inbound rules. Confirm that the ports related to the Web processes are open, as shown below:
Problem Description

Website access is slow.

Problem Analysis

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

Solutions

**Check the local client**

1. Access the [network testing website](#) to test the access speed to different domain names from the local client.
2. Based on the test result, check whether the local network has an exception.
   
   For example, the test result is as shown below:
<table>
<thead>
<tr>
<th>Domain</th>
<th>Network Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>inews.qq.com</td>
<td>Normal network, 194 milliseconds delay</td>
</tr>
<tr>
<td><a href="http://www.qq.com">www.qq.com</a></td>
<td>Normal network, 128 milliseconds delay</td>
</tr>
<tr>
<td>3g.qq.com</td>
<td>Normal network, 140 milliseconds delay</td>
</tr>
<tr>
<td>mail.qq.com</td>
<td>Normal network, 99 milliseconds delay</td>
</tr>
<tr>
<td>user.qzone.qq.com</td>
<td>Normal network, 98 milliseconds delay</td>
</tr>
<tr>
<td>r.qzone.qq.com</td>
<td>Normal network, 203 milliseconds delay</td>
</tr>
<tr>
<td>w.qzone.qq.com</td>
<td>Normal network, 188 milliseconds delay</td>
</tr>
<tr>
<td>ptlogin2.qq.com</td>
<td>Normal network, 96 milliseconds delay</td>
</tr>
<tr>
<td>check.ptlogin2.qq.com</td>
<td>Normal network, 189 milliseconds delay</td>
</tr>
<tr>
<td>ui.ptlogin2.qq.com</td>
<td>Normal network, 91 milliseconds delay</td>
</tr>
<tr>
<td>i.mail.qq.com</td>
<td>Normal network, 129 milliseconds delay</td>
</tr>
<tr>
<td>v.qq.com</td>
<td>Normal network, 129 milliseconds delay</td>
</tr>
<tr>
<td>c.3g.163.com</td>
<td>Normal network, 143 milliseconds delay</td>
</tr>
<tr>
<td>weibo.com</td>
<td>Normal network, 211 milliseconds delay</td>
</tr>
<tr>
<td><a href="http://www.baidu.com">www.baidu.com</a></td>
<td>Normal network, 94 milliseconds delay</td>
</tr>
<tr>
<td><a href="http://www.sina.com.cn">www.sina.com.cn</a></td>
<td>Normal network, 138 milliseconds delay</td>
</tr>
<tr>
<td><a href="http://www.taobao.com">www.taobao.com</a></td>
<td>Normal network, 136 milliseconds delay</td>
</tr>
</tbody>
</table>
The test result shows the access latency for each domain name and whether the network is normal.

- If the network has an exception, contact your ISP to locate and solve the problem.
- If the network is normal, please check the network linkage.

**Check the network linkage**

1. Ping the server's public IP from the local client to check if there is packet loss or high latency.
   - If any of the problems occurs, use MTR for troubleshooting. For more information, please see CVM Network Latency and Packet Loss.
   - If the ping test shows no packet loss or high latency, please execute **step 2**.
2. Use the `dig/nslookup` command to check whether the problem is caused by DNS resolution. You can also access the page directly with the public network IP to check whether DNS has caused access latency.

**Check the server**

1. Log in to the **CVM Console**.
2. Click the ID/name of the instance you want to check to enter its details page.
3. Select the **Monitoring** tab on the details page to view the instance resource usage, as shown below:
- If the CPU/memory usage is too high, please see [Failed to log in to a Windows CVM due to high CPU and memory usage](https://intl.cloud.tencent.com/document/product/213/32405) and [Failed to log in to a Linux CVM due to high CPU and memory usage](https://intl.cloud.tencent.com/document/product/213/32387) for troubleshooting.
- If the bandwidth usage is too high, please refer to [Login Failure Due to High Bandwidth Occupation](https://intl.cloud.tencent.com/document/product/213/32542) for troubleshooting.
- If the instance resource usage is normal, please [check other problems](#CheckOtherProblems).

**Check other problems**

Based on instance resource usage, check whether the increase in resource consumption is caused by server load.

- If yes, we recommend that you optimize the business processes, change instance configuration, or purchase new servers to reduce the pressure on existing servers.
- If no, we recommend that you check log files to locate the problem and carry out targeted optimization.
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 start](image)

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

![WinMTR stop](image)
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*:
  
  ```bash
  yum install mtr
  ```

- For *Ubuntu*:
  
  ```bash
  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 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 local server fails to ping through an instance. Possible causes include:

- Incorrect destination server configuration
- Unsuccessful domain name resolution
- Link failure

If the local network is working normally (for example, other websites can be pinged through from the local network), troubleshoot this problem as follows:

- Check whether the instance is configured with a public IP address.
- Check security group settings.
- Check OS settings.
- Perform other operations.

Directions

**Checking whether the instance is configured with a public IP address**

An instance can interwork with other computers on the Internet only if it has a public IP address. Without a public IP address, the instance cannot be pinged through outside the private IP address.

1. Log in to the CVM console.
2. On the "Instance List" page, select the instance ID or instance name to ping to go to the instance details page, as shown in the following figure:
3. Check whether the instance is configured with a public IP address in the "Network Information" area.
   - If yes, check security group settings.
   - If no, bind an elastic public IP address to the instance.

**Checking security group settings**

A security group is a virtual firewall that controls the inbound and outbound traffic of the associated instance. You can specify protocols, ports, and policies for the rules of a security group. Check whether ICMP that is used in the ping test is allowed in the security group associated with the instance. You can perform the following operations to view information on the security group associated with the instance and its inbound and outbound rules:

1. Log in to the CVM console.
2. On the "Instance List" page, select the instance ID or instance name that needs to be configured with a security group to go to the instance details page, as shown in the following figure:
3. Click the **Security Groups** tab to go to the security group management page for this instance, as shown in the following figure:
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, check OS settings.
   - If no, set the ICMP protocol policy to allow.

**Checking OS settings**

Choose a check method based on the OS type of the instance.

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

**Checking Linux kernel parameters and firewall settings**

In the Linux OS, whether a ping test is allowed depends on both kernel and firewall settings. If either of them forbids the ping test, "Request timeout" occurs.

**Checking the icmp_echo_ignore_all kernel parameter**

1. Log in to the instance.
2. Run the following command to view the icmp_echo_ignore_all setting in the OS:
   
   ```bash
cat /proc/sys/net/ipv4/icmp_echo_ignore_all
   ```
   
   - If the return result is 0, the OS allows all ICMP Echo requests. In this case, check firewall settings.
   - If the return result is 1, the OS forbids all ICMP Echo requests. In this case, perform step 3.
3. Run the following command to change the setting of the icmp_echo_ignore_all kernel parameter:
   
   ```bash
echo "0" > /proc/sys/net/ipv4/icmp_echo_ignore_all
   ```
Checking firewall settings

Run the following command to check whether the firewall rules and corresponding ICMP rules of the current server are banned:

```
iptables -L
```

- If the following result is returned, the ICMP rules are not banned. In this case, check whether the domain name is filed.

```
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 return result shows that the ICMP rules are banned, run the following commands to enable these rules:

```
#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 Windows firewall settings

1. Log in to the instance.
2. Open Control Panel and select Windows Firewall Settings.
3. On the "Windows Firewall" page, select Advanced Settings.
4. In the "Advanced Security Windows Firewall" window that appears, check whether the inbound and outbound rules for ICMP are banned.
   - If the inbound and outbound rules for ICMP are banned, enable these rules.

Other operations

If the preceding operations cannot solve the problem, do the following:

- If the domain name cannot be pinged through, check your website configuration.
- If the public IP address cannot be pinged through, attach information on the instance and two-way MTR data (from the local server to the CVM and from the CVM to the local server) to a ticket and submit the ticket to contact our engineers for assistance.
  For more information on how to use MTR, 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 on 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.
   
   ```
   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.

    rpm -q initscripts

A message similar to the one below is returned:

    initscripts-9.03.58-1.el6.centos.2.x86_64

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.
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.