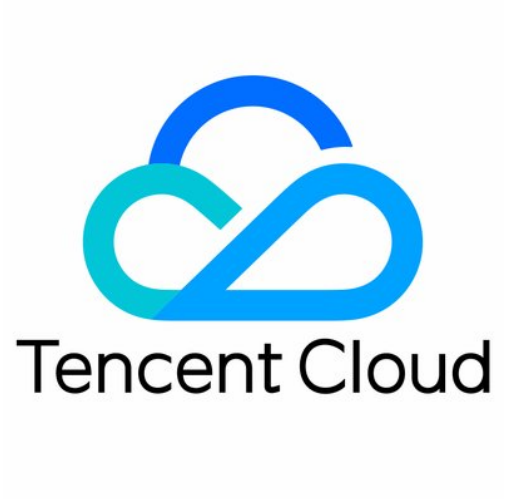
Direct Connect

Troubleshooting

Product Documentation



©2013-2022 Tencent Cloud. All rights reserved.

Copyright Notice

©2013-2024 Tencent Cloud. All rights reserved.

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

Trademark Notice

Tencent Cloud

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

Service Statement

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

Contents

©2013-2022 Tencent Cloud. All rights reserved.

Troubleshooting
General Troubleshooting Solutions

Last updated：2024-01-13 16:02:36

This document provides guidance on Direct Connect troubleshooting, helping you troubleshoot network connection failures.

Troubleshooting Sequence

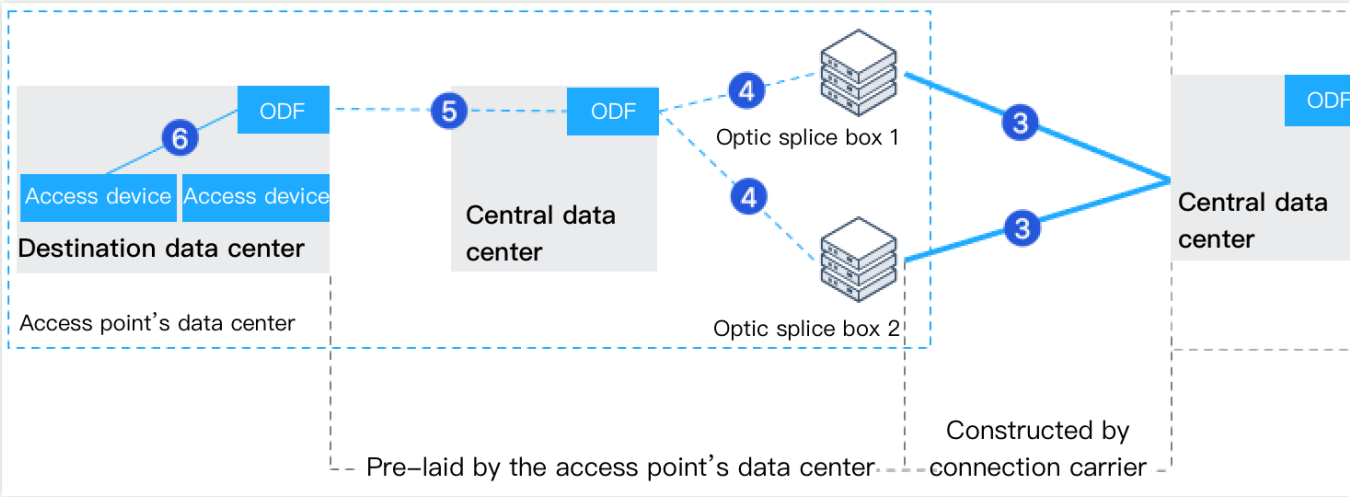
Troubleshoot the following items in sequence:
1. Troubleshooting physical layer linkage failures
2. Troubleshooting data link layer failures
3. Troubleshooting network layer or transport layer failures
4. Troubleshooting security failures
5. Troubleshooting route failures

Troubleshooting Physical Layer Linkage Failures

When you encounter port failure, fiber optic components exception at either or both ends, CRC, or packet error, follow the steps below to troubleshot physical layer linkage failures.
1. Confirm that your IDC CPE device is started with open ports.
2. Contact your DC connection provider and obtain the relevant certificates indicating the completed construction and network connectivity.
3. Check that the fiber optic components in IDC are normal. Please submit a ticket to request the after-sales manager to check fiber optic components in the access point's data center.
4. Contact your DC connection provider and access point's carrier to test link segments.
Assume that a Direct Connect service connects IDC to the access point's data center through the optic splice box outside the data center building, and then to the destination data center through Optical Distribution Frame (ODF), then the segment testing should be performed as follows:
(1) Test that the ODF in your local IDC can communicate with the access devices.
(2) If there are multiple ODFs in your local IDC, test that they can communicate with each other.
(3) Contact your DC connection provider to check that the connection between your local IDC and the data center's optic splice box works.
(4) Contact the access point's carrier to check that the optic splice box can communicate with ODF.

©2013-2022 Tencent Cloud. All rights reserved.

(5) Contact the access point's carrier to check that ODFs can communicate.
(6) Contact the access point's carrier to check that ODF can communicate with access devices at the access point.



Troubleshooting Data Link Layer Failures

1. When VLAN ID is not 0:
Ensure any Layer 2/Layer 3 devices between the carrier's connection, Tencent Cloud access devices and local IDC access devices (including the IDC access device itself) have enabled VLAN relay for your VLAN tags, that is, identify and allow your VLAN tag.
Ensure that any Layer 2/Layer 3 devices between the Tencent Cloud edge device and your local IDC edge device (including the IDC edge device itself) correctly relay without converting the VLAN.
2. Check that the IP addresses are correctly configured. Ensure the IP addresses are correctly configured on the local access devices, which remain stable without MAC address flapping records.
3. Ensure the layer-2 link detection protocols such as STP\\Loop-detection are disabled on IDC access devices; otherwise, ports may be blocked.

Troubleshooting Network Layer or Transport Layer Failures

1. Ensure that the IP addresses configured on both sides of the connection are in one subnet with the same subnet mask.
2. Ensure that each side configured a unique IP address, and no IP is reused.
3. If your connection has bidirectional forwarding Detection (BFD) enabled, ensure that the security policy of IDC devices allows the BFD message to pass.

©2013-2022 Tencent Cloud. All rights reserved.

4. If your connection has NQA detection enabled, note that Tencent Cloud supports the ICMP-echo type. Ensure that the security policy of IDC devices allows the ICMP message to pass.

Note:

NQA detection is only supported in dedicated tunnel 2.0 currently. If you are using dedicated tunnel 1.0 and you want to enable NQA detection feature, please contact us.

5. If a BGP session is required on both sides of the connection for propagating Tencent Cloud VPC routes and IDC routes:

Correctly configure BGP ASN and BGP PEER IP on IDC devices.

Configure the same BGP MD5 authentication key on both sides.

Allow the BGP message to pass in the security policy of IDC devices.

Open the TCP 179 port for the BGP session in the security policy.

Troubleshooting Security Issues

Check the ACL settings

Ensure that the Tencent Cloud subnet ACL allows the traffic going from or to IDC hosts.

Ensure that the IDC subnet ACL allows the traffic going from or to Tencent Cloud CVMs.

Check the security group settings

Ensure that the Tencent Cloud CVM security group allows the traffic going from or to IDC hosts.

Ensure that the IDC security group allows the traffic going from or to Tencent Cloud CVMs.

Troubleshooting Route Failures

VPC-based direct connect gateway

Static dedicated tunnel

Check that IDC IP range is correctly configured on the dedicated tunnel and propagated to Tencent Cloud VPC. Otherwise, the Tencent Cloud VPC route to IDC server will be unreachable and cause business to be inaccessible.

Check the CPE IP range in the dedicated tunnel

1. Log in to the Direct Connect console. Go to the **Dedicated Tunnels** page and click the **ID/Name** of the target dedicated tunnel to enter its details page. Select the **Advanced Configuration** tab and check whether the CPE IP range is correctly configured.

2. Reconfigure the CPE IP range if the previous configuration is incorrect. For detailed directions, see Creating a Dedicated Tunnel.

Check the route table

1. Log in to the Direct Connect console. Go to the **Dedicated Tunnels** page and click the **ID/Name** of the target dedicated tunnel to enter its details page. Select the **Basic Info** tab and click the VPC ID to view VPC details.

©2013-2022 Tencent Cloud. All rights reserved.

2. Click the **Route Table**.
3. Select the **Basic Information** tab and check if a routing policy with the CPE IP range as destination and the direct connect gateway as next hop type is enabled.
4. Reconfigure the routing policy if the previous configuration is incorrect. For detailed directions, see Configuring the Route Table.

BGP dedicated tunnel

Check that the direct connect gateway has obtained the IDC IP range according to the BGP protocol and propagated it to Tencent Cloud VPC. Otherwise, the Tencent Cloud VPC route to IDC server will be unreachable and cause business to be inaccessible.

Check the BGP route configurations

1. Log in to the Direct Connect console. Go to the **Dedicated Tunnels** page and click the **ID/Name** of the target dedicated tunnel to enter its details page. Select the **Advanced Configuration** tab and check BGP configurations.
2. Reconfigure BGP if the previous configuration is incorrect. For detailed directions, see Creating a Dedicated Tunnel.

Check the route table

1. Log in to the Direct Connect console. Go to the **Dedicated Tunnels** page and click the **ID/Name** of the target dedicated tunnel to enter its details page. Select the **Basic Configuration** tab and click the VPC ID to view VPC details.
2. Click the **Route Table**.
3. Select the **Basic Information** tab and check if a routing policy with the CPE IP range as destination and the direct connect gateway as next hop type is enabled.
4. Reconfigure the routing policy if the previous configuration is incorrect. For detailed directions, see Configuring the Route Table.

CCN-based direct connect gateway

Static dedicated tunnel

Check that IDC IP range is correctly configured on the dedicated tunnel and propagated to CCN. Otherwise, the Tencent Cloud VPC route to IDC server will be unreachable and cause business to be unaccessible.

Check the CPE IP range in the dedicated tunnel

1. Log in to the Direct Connect console. Go to the **Dedicated Tunnels** page and click the **ID/Name** of the target dedicated tunnel to enter its details page. Select the **Advanced Configuration** tab and check whether the CPE IP range is correctly configured.
2. Reconfigure the CPE IP range if the previous configuration is incorrect. For detailed directions, see Creating a Dedicated Tunnel.

Check the IDC IP range on the direct connect gateway

1. Log in to the Direct Connect Gateway console and click the **ID/Name** of the target direct connect gateway to enter its details.
2. Select the **IDC IP Range** tab, and check the configurations.

©2013-2022 Tencent Cloud. All rights reserved.

3. Reconfigure the IDC IP range if no configuration is available. For detailed directions, see Adding IDC IP Ranges to the Direct Connect Gateway.

BGP dedicated tunnel

Check that the dedicated tunnel BGP is correctly configured and the IDC IP range is synced to direct connect gateway and propagated to CCN. Otherwise, the Tencent Cloud VPC route to IDC server will be unreachable and cause business to be unaccessible.

Check the BGP route configurations

1. Log in to the Direct Connect console. Go to the **Dedicated Tunnels** page and click the **ID**/**Name** of the target dedicated tunnel to enter its details page. Select the **Advanced Configuration** tab and check BGP configurations.
2. Reconfigure BGP if the previous configuration is incorrect. For detailed directions, see Creating a Dedicated Tunnel.

Check the IDC IP range on the direct connect gateway

1. Log in to the Direct Connect Gateway console and click the **ID**/**Name** of the target direct connect gateway to enter its details.
2. Select the **IDC IP Range** tab, and check the configurations.
3. Reconfigure the IDC IP range if no configuration is available. For detailed directions, see Adding IDC IP Ranges to the Direct Connect Gateway.

©2013-2022 Tencent Cloud. All rights reserved.

Access Failure and Packet Loss

Last updated：2024-01-13 16:02:36

Error Description

Your business is unable to connect to the network and encounters packet loss, resulting in exceptions.

Possible Reasons

The reasons are as follows:

Connection interruption: the connection is damaged. For example, the cable is cut off.

Bandwidth exhaustion: the dedicated tunnel's bandwidth is insufficient to meet business requirements.

Security policy misconfiguration: the IDC route to and from VPC is different

Static route failure: the static route has no Bidirectional Forwarding Detection (BFD) configured, which causes business access exception.

BGP route failure: the BGP routes exceed the limit.

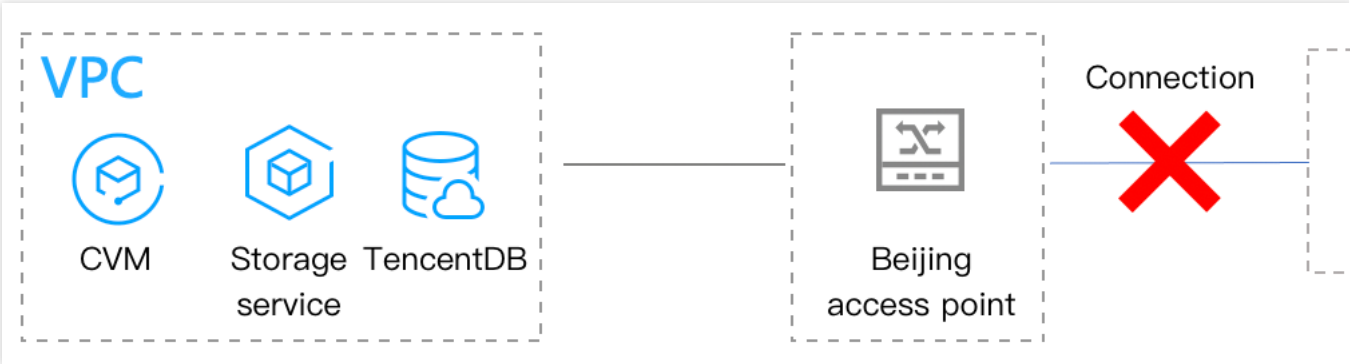
IP address conflict: the local IP address is overlapped with VPC IP.

Solutions

Connection interruption

A connection to one access point

Your IDC connects to one Tencent Cloud access point using a connection, and then accesses Tencent Cloud VPCs. The disconnection will directly cause business interruption.



Solution

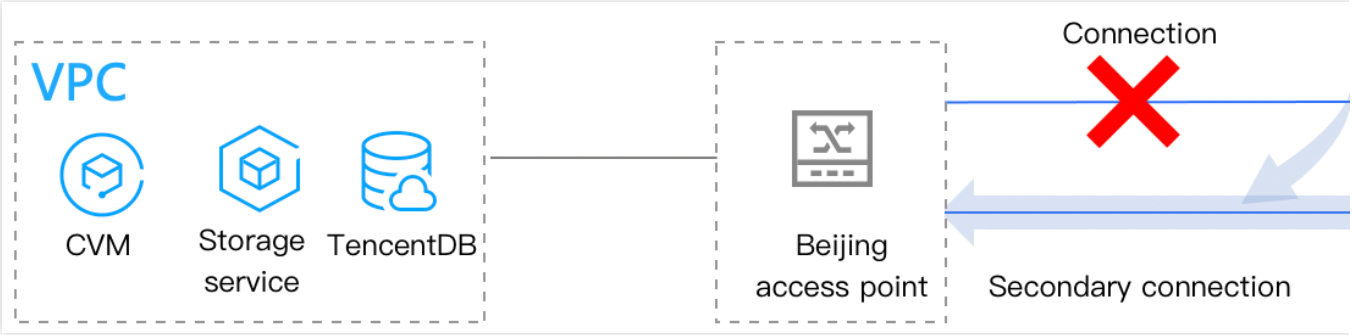
Report the failure to the carrier and provide the connection ID. This mode is incapable of disaster recovery. We

©2013-2022 Tencent Cloud. All rights reserved.

recommend that you plan connections to improve the stability and high availability of the Direct Connect network architecture. For more information, see Network Planning.

Two connections to one access point

Your IDC connects to one Tencent Cloud access point using two connections, and then accesses Tencent Cloud VPCs. When one connection interrupts, disaster recovery starts.



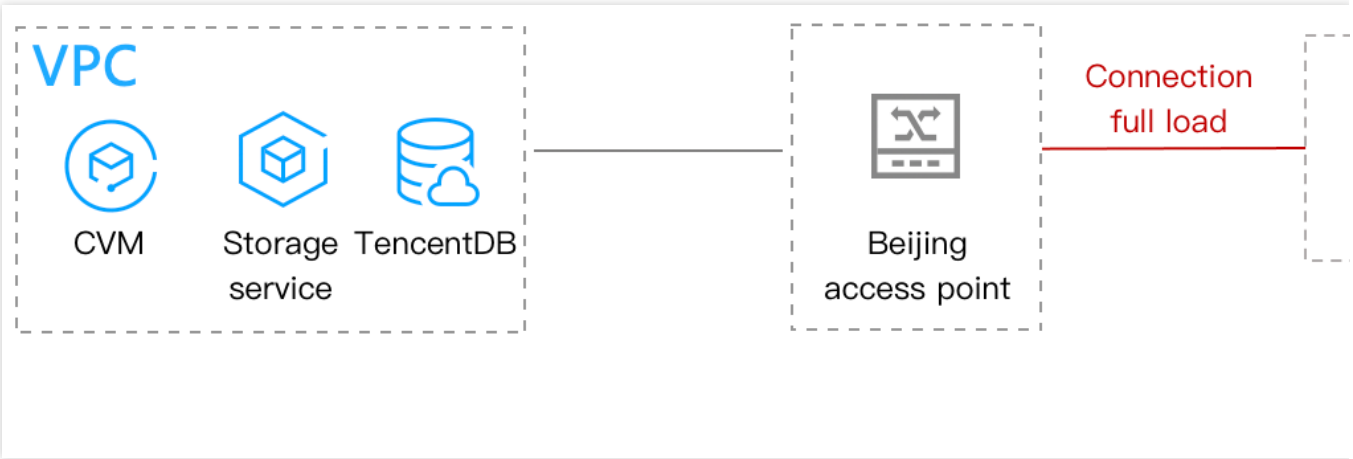
Solution

1. Check for business damage on your business monitoring system.
2. Collect the access latency and route change caused by traffic switch after disaster recovery, and judge whether the secondary connection works.
3. If the secondary connection fails to work, locate faults based on information collected from the ping and traceroute tests.

Bandwidth exhaustion

A connection to one access point

Your IDC connects to one Tencent Cloud access point using a connection, and then accesses Tencent Cloud VPCs. When the dedicated tunnel bandwidth is used up, packet will be lost, resulting in data loss.



Solution

1. Log in to the Direct Connect console and go to the **Dedicated Tunnels** page. Locate the dedicated tunnel and adjust its bandwidth on the **Change Tunnel** page as instructed in Changing Tunnel.

©2013-2022 Tencent Cloud. All rights reserved.

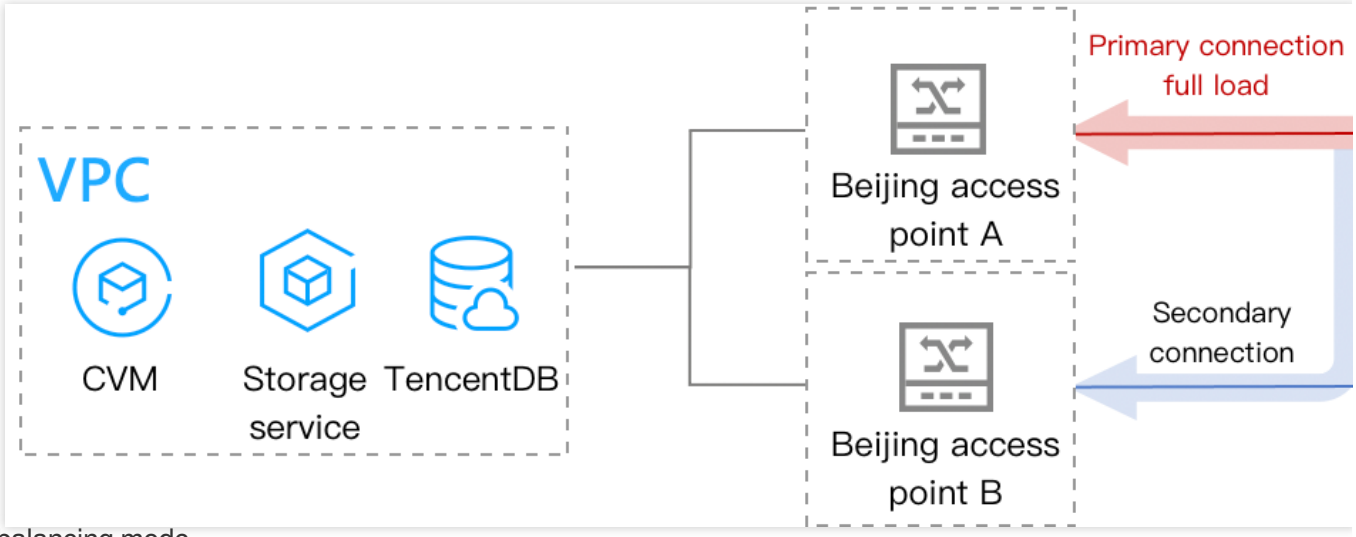
2. If the connection bandwidth cap is reached, first perform the disaster recovery switchover for your business and contact the Direct Connect representative for expansion.
3. Analyze the causes of bandwidth exhaustion while prioritizing the business recovery.

Two connections to two access points

Your IDC connects to two intra-region Tencent Cloud access points using one connection respectively, and then accesses Tencent Cloud VPCs.

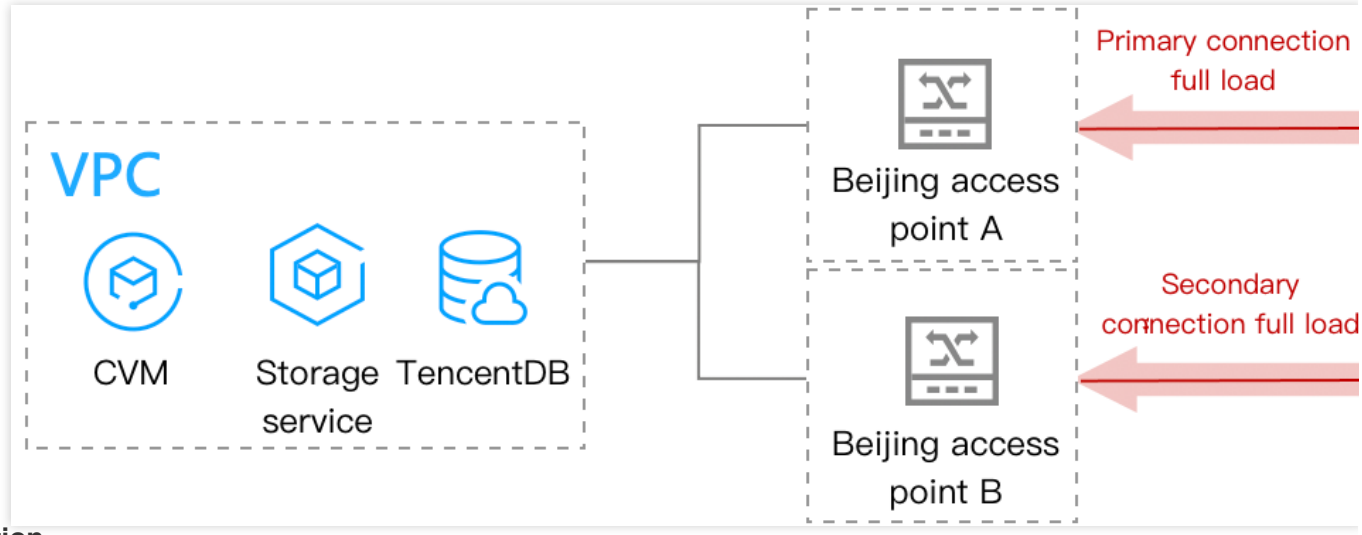
Primary/secondary mode

When the primary connection bandwidth is used up, packet will be lost, resulting in data loss. Change to the load-balancing mode to share traffic and resume service data.



Load-balancing mode

When both connections are full-loaded, packet will be lost, resulting in data loss.



Solution

3.1 Log in to the Direct Connect console and go to the **Dedicated Tunnels** page. Locate the dedicated tunnel and adjust its bandwidth on the **Change Tunnel** page as instructed in Changing Tunnel.

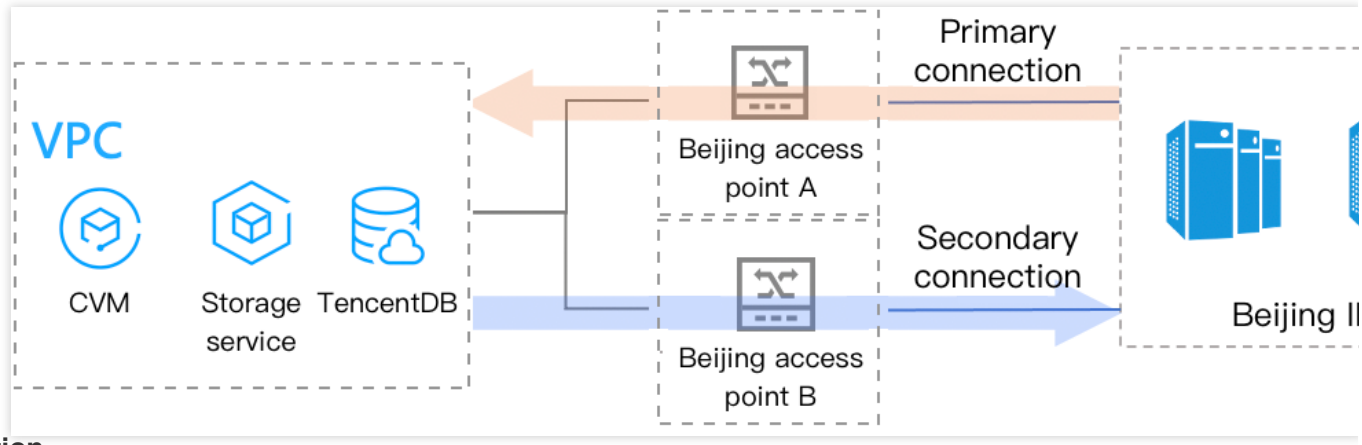
3.2 If your connection bandwidth cap is reached:

©2013-2022 Tencent Cloud. All rights reserved.

Primary/secondary mode: change to the load-balancing mode to share traffic and resume service data.
Load-balancing mode: first perform disaster recovery switchover for your business and contact the Direct Connect representative for expansion.
3.3 Analyze the causes of bandwidth exhaustion while prioritizing the business recovery.

Security policy misconfiguration

Your IDC connects to two intra-region Tencent Cloud access points using one connection respectively, and then accesses Tencent Cloud VPCs. If your IDC accesses Tencent Cloud VPC via the primary connection and is accessed by Tencent Cloud VPC via the secondary connection, different routes will cause inaccessibility.



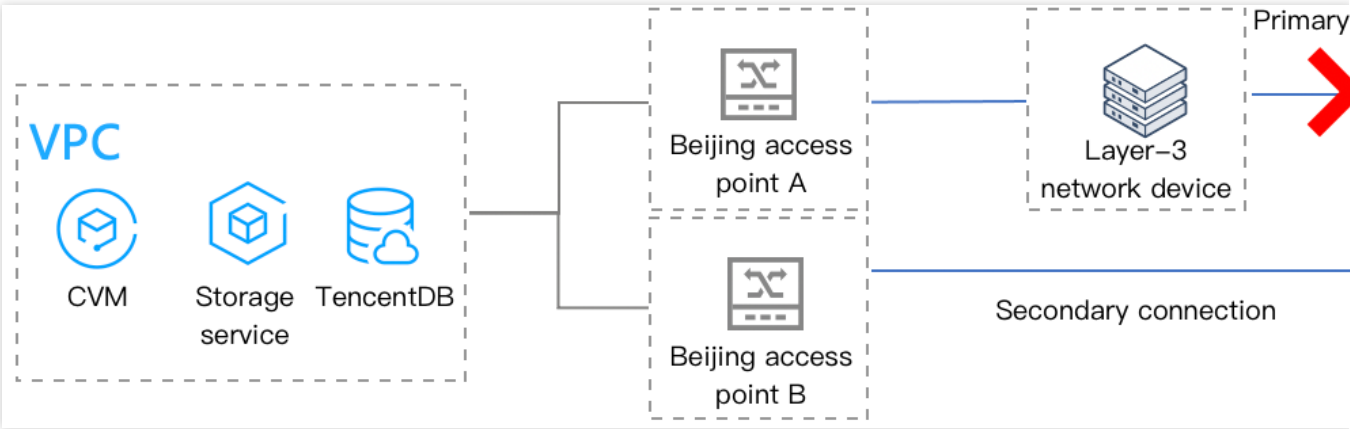
Solution

1. Check whether different security devices (such as firewall) are configured on the primary and secondary connections. If so, ensure that their security policies are the same and allow incoming and outgoing messages to pass.
2. Configure an IDC IP (an idle IP or test IP as confirmed by the owner) on IDC access devices, and use this IP to access the in-cloud business IP to test communication.
3. If the problem persists, troubleshoot the issue inside your IDC.

Static route failures

Your IDC connects to two intra-region Tencent Cloud access points using one connection respectively, and then accesses Tencent Cloud VPCs.
If the primary connection cascades a layer-3 device, the IDC server port exception or abnormal link from the layer-3 device to IDC is imperceptible to the access point A, and no alarm will be triggered. In this case, the dedicated tunnel still sends static route to the direct connect gateway and forward traffic to the faulty connection, causing service suspension.

©2013-2022 Tencent Cloud. All rights reserved.



Solution

We recommend that configure BFD on access devices at IDC and access point for the static route to periodically send a detection packet. If there is no reply within a specified period, the opposite end is determined to be faulty and the associated route will become invalid without forwarding to the direct connect gateway.

Please submit a ticket to enable the BFD feature of the dedicated tunnel and the configuration will be provided.

Note:

The default Tencent Cloud BFD is dynamic BFD. The local TX Interval is equal to VPC's Desired Min TX Interval or IDC's Required Min RX Interval, whichever is larger.

For 1.0 dedicated tunnel:

If you applied for the dedicated tunnel before October 1, 2019, both Desired Min TX Interval and Required Min RX Interval are 100 ms, and Detect Mult is 3.

If you applied for the dedicated tunnel on or after October 1, 2019, both Desired Min TX Interval and Required Min RX Interval are 300 ms, and Detect Mult is 3.

For 2.0 dedicated tunnel:

The minimum values of both Desired Min TX Interval and Required Min RX Interval are 1000 ms, and Detect Mult is 3.

BGP route failures

Each dedicated tunnel supports up to 100 BGP routes. If this limit is exceeded, your business may fail.

Solution

Plan network addresses and merge CIDR block subnet to reduce IDC routes to Tencent Cloud VPC.

IP address conflicts

Both VPC and IDC follow the TCP/IP protocol that has layer-3 addressing based on the destination IP and layer-2 addressing based on destination MAC. In a hybrid-cloud scenario, the overlap of the IDC and VPC address space may cause IP address conflicts and limit business access.

Solution

1. Implement a network planning.

1.1 Plan Tencent Cloud VPC and IDC addresses uniformly.

1.2 Plan IP and other interconnection addresses globally.

©2013-2022 Tencent Cloud. All rights reserved.

2. Use the NAT-type direct connect gateway to translate and mask the local VPC address and peer IDC address when the business scenario does not allow network splitting and re-planning. For detailed directions, see Configuring the Network Address Translation (NAT).

Note:

A NAT-type direct connect gateway supports up to 100 rules for local IP translation and peer IP translation each.

©2013-2022 Tencent Cloud. All rights reserved.