Direct Connect

Product Documentation

Contents

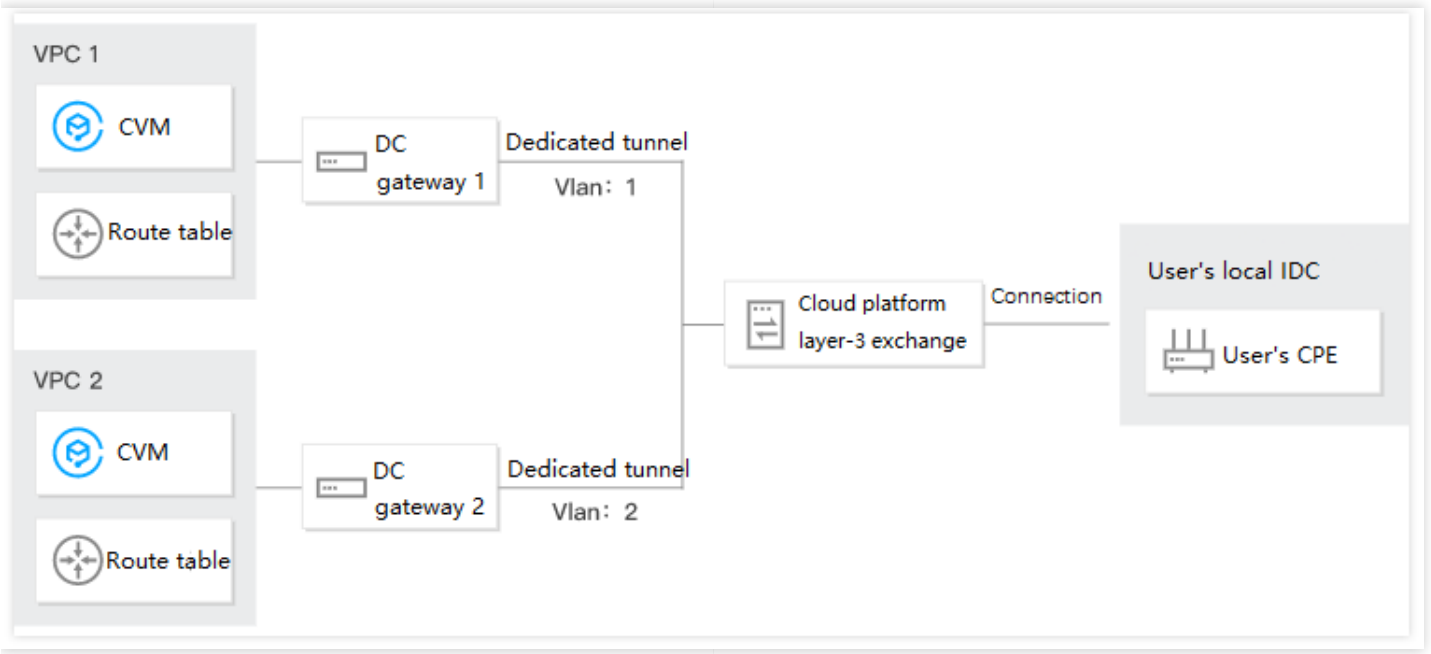
Direct Connect 3
- Product Introduction 3
  - Direct Connect Overview 3
  - Product Features 6
  - Use Cases 12
  - Limits 13
  - Related products 16
- Purchase Guide 17
  - Billing Overview 17
- Quick Start 18
- Operation Guide 24
  - Managing Connection 24
    - Applying for Connection 24
    - Canceling Connections 28
    - Sharing Connection 29
    - View Monitoring Information 30
    - Setting Alarms 31
  - Managing a DC Tunnel 33
    - Applying for Tunnel 33
    - Changing a Tunnel 38
    - Delete a Channel 48
    - View Monitoring Information 49
    - Setting Alarms 50
  - Managing DC Gateway 52
    - Creating a Direct Connect Gateway 52
    - Configuring Network Address Translation (NAT) 54
    - Deleting a DC Gateway 67
  - Configuring a Route Table 68
- FAQs 69
  - Basic Category 69
  - Technology Category 72
- API Documentation 75
  - Dedicated Line Access(dc) 75
    - version(2018-04-10) 75
      - API overview 75
      - CallingMethod 76
        - signaturev1 76
        - signaturev3 84
        - request 93
        - result 94
        - PublicParameter 97
      - DC-related APIs 99
        - ApproveDirectConnectTunnel 99
        - CreateDirectConnect 101
        - CreateDirectConnectTunnel 103
        - DeleteDirectConnect 106
        - DeleteDirectConnectTunnel 108
        - DescribeAccessPoints 110
        - DescribeCloudBgpAsn 112
        - DescribeDirectConnectPortPrice 114
        - DescribeDirectConnectTunnels 116
        - DescribeDirectConnects 117
        - DescribeIsp 118
        - ModifyDirectConnectAttribute 120
        - ModifyDirectConnectTunnelAttribute 122
        - UpdateVifAssociated 125
      - Data structure 127
      - ErrorCode 133

Product Introduction
Direct Connect Overview

What is Direct Connect?

Direct Connect provides a fast and secure way to connect the cloud platform and the local data center. Users can use a Connection to connect cloud platform computing resources located in multiple regions at one time, achieving flexible and reliable hybrid cloud deployment.

Hybrid Cloud Featuring DC Deployment
Use traditional DC tunnel to connect the user's IDC and the cloud VPC.
If a connection needs to connect multiple VPCs, you need to create DC tunnels with different VLAN IDs to connect multiple VPCs.



Components

DC consists of a Connection, a DC tunnel, and a DC gateway.

- Connection
  The Connection supports dual-line hot standby connection, dual-line connection point power supply, and complete isolation of network pipelines.
- DC Tunnel

A DC tunnel is a network link division of a connection. Users can create DC tunnels connected to different DC gateways to interconnect local data centers with multiple Virtual Private Clouds.

- DC Gateway
- The dedicated traffic entrance of the VPC can be interconnected with multiple different IDCs by connecting with multiple DC tunnels. The DC gateway is implemented in the form of cluster, with no risk of single point failure across the entire route, meeting the requirements of financial-grade network interconnection.
- A DC gateway is a bridge that connects a VPC and a Connection. You can create a DC tunnel in a Connection that is associated with a DC gateway.
- The DC gateway can link DC tunnels from multiple Connections to interconnect with your multiple local data centers.
- Users can create a DC gateway for each VPC in the DC gateway console. Each VPC only supports creating one DC gateway, which can connect with DC tunnel requests from different Connections.

Differences from and Strengths Over IPsec VPN

Strengths	Direct Connect	IPsec VPN
Stable Network Delay	The network latency is reliable and limited to a low level. The connection network is based on a DC. You can use a fixed routing configuration to avoid the latency and instability caused by congestion or fault-triggered detours.	The network connection is based on the Internet. When the network link is blocked during peak hours, it may cause routing detours and unstable latency.
Highly Reliable Disaster Recovery Connect	Both connection devices and network forwarding devices are deployed in a distributed and clustered manner, with full-link high-reliability configuration, supporting dual-line connection with protection, meeting your stringent requirements for availability above 99.95%.	It adopts a dual-machine hot backup configuration, which has high reliability at the gateway layer. However, due to the unreliable Internet network link, it cannot guarantee dedicated line-level network reliability.
Supporting Large Bandwidth	A single line supports a maximum bandwidth connection of 10 Gbps, and can also allow connection with multiple 10 Gbps links for network CLB, with no theoretical upper limit.	A single gateway supports a maximum bandwidth limit of 100 Mbps. VPC supports multiple VPN gateway configurations, which can support VPN connection in a bandwidth of greater than 100 Mbps.
High Security	The network link is dedicated to users, with no risk of data leakage, ensuring high	Network transmission is based on the pre-shared key encryption of the

Strengths	Direct Connect	IPsec VPN
	security and meeting the stringent network connection requirements of the finance, government, and enterprise sectors.	IKE protocol, which can meet most network transmission security requirements.
Supporting Network Address Translation	It supports configuring network address translation services on the gateway, enabling IP mapping at both ends of the DC and IP port mapping at the VPC end, thus resolving address conflicts when multiple networks are interconnected.	Not support.

Product Features

Connection

The physical line connection between the cloud platform and the local data center. You can use a third-party network service provider to establish a network connection between your data center and the cloud platform's dedicated network connection point.

DC Tunnel

- A DC tunnel is a network link division of a connection.
- You can create DC tunnels connected to different DC gateways to interconnect your local data center with multiple VPCs.

Network Address Translation (NAT)

NAT is a solution to the IP conflict problem at both ends of the DC during the connection to a hybrid cloud. You can configure NAT rules on the DC gateway. NAT includes IP translation and IP port translation.

IP Translation

- IP translation refers to translating the original IP to a new IP to achieve mutual network access. It is divided into local IP translation and peer IP translation.
- IP translation does not distinguish between source and destination directions. The mapped IP can actively access the peer end or be actively accessed by the peer end.

Local IP translation

1. Note for Conversion

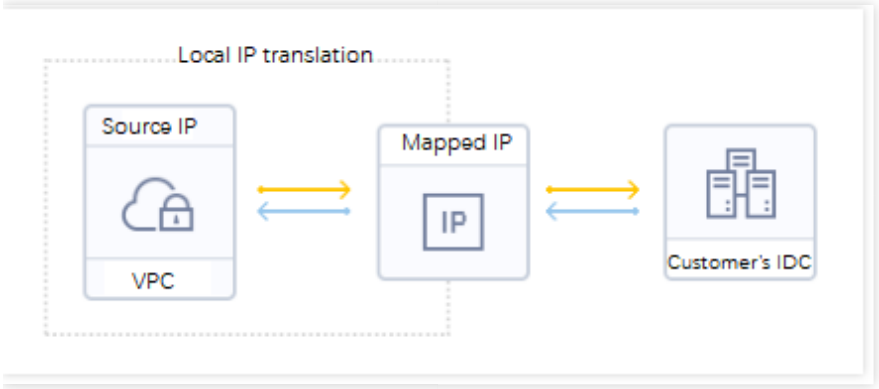
- Local IP translation refers to mapping the original IP in the VPC to a new IP, and using the new IP to communicate with the DC peer.

- You can configure multiple local IP translation rules and configure a network ACL for each local IP translation rule. The network ACL supports configuration of the source port, destination IP, and destination port.

> Note:

> Network address translation rules are effective only for network requests that comply with ACL restrictions.

- The local IP translation does not limit the direction of the network request. It can be the VPC actively accessing the DC peer, or the other way round.



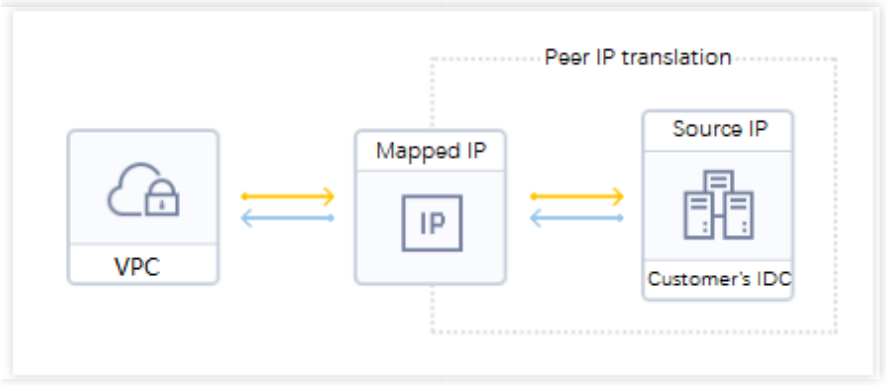
2. Example of Conversion

Inside the VPC, IP A 192.168.0.3 is mapped to IP B 10.100.0.3 , then the source IP for IP A's active access to the DC peer will be automatically modified to 10.100.0.3 , and all network packets accessed by the DC peer 10.100.0.3 will automatically be directed to IP A 192.168.0.3 .

Peer IP translation

1. Note for Conversion

- Peer IP translation means that the original IP in the user's IDC is mapped to a new IP, and the new IP is used to communicate with the IP in the VPC.
- Unlike local IP translation, peer IP translation does not support network ACL restrictions. Therefore, once a peer IP translation rule is configured, it will take effect on all DC tunnel peers.
- The peer IP translation does not limit the direction of the network request. It can be the VPC actively accessing the DC peer, or the other way round.



2. Example of Conversion

Dedicated line peer IP D 10.0.0.3 is mapped to IP C 172.16.0.3 , then IP D 10.0.0.3 actively accesses the source IP of the network packet of the VPC and will be automatically modified to IP C 172.16.0.3 . All the VPC's network packets accessing IP C 172.16.0.3 will automatically be directed to the DC peer IP D 10.0.0.3 .

> Note:
>
> - After the local IP translation and peer IP translation are configured, the DC gateway will only send the translated IP route to the DC peer. Therefore, the original IP that is not configured with the local and peer IP translation will not be able to ping the DC peer. However, DC gateways cannot replace professional network firewalls. If you need advanced network protection, configure security groups and network ACL policies in the VPC and deploy professional physical network firewall devices in your IDC computer room.
> - When the DC gateway is configured with peer IP translation, in the destination IP of the local source IP port translation ACL rule field, you need to fill in the mapped IP of the peer IP translation, instead of the original IP.

IP Port Translation

- IP port translation refers to mapping the original IP port to a new IP port and using the new IP port to achieve network access. IP port translation includes local source IP port translation and local destination IP port translation.
- IP port translation emphasizes directionality. Source IP port translation refers to active outbound access, and destination IP port translation refers to active access by the peer end.

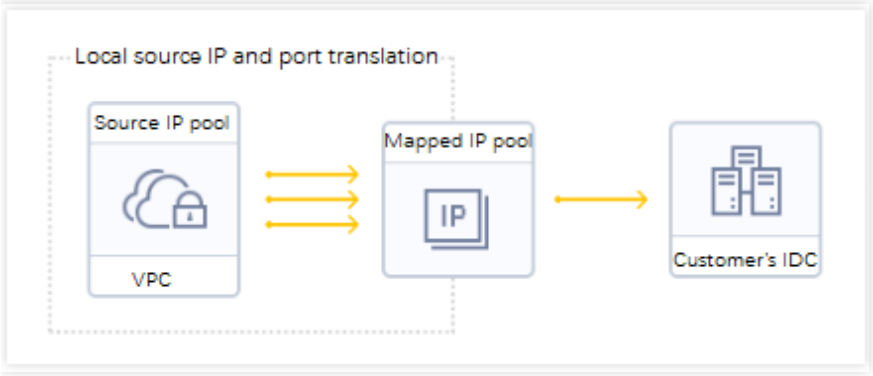
Local Source IP Port Translation

1. Note for Conversion

- Local source IP port translation means that when an IP in a VPC actively accesses a public network through a DC gateway, a random port of a random IP in a specified IP pool is used to access the user

IDC at the DC peer.

- Local source IP port translation supports configuration of ACL rules. Only network outbound access that complies with the ACL rules matches the address pool forwarding rules. By configuring different ACL rules for the address pool, you can flexibly configure network address translation rules for multiple third-party connection.



- The local source IP port translation only supports the network access request initiated by the VPC end. If the DC peer needs to actively access the IP port in the VPC, the local destination IP port translation configuration needs to be additionally configured. The network requests initiated by the local source IP port translation within the VPC are considered stateful connections, thus eliminating the need to address network packet return issues.

2. Example of Conversion

The IP range of VPC C is 172.16.0.0/16 . Third-party banks A and B are connected via a DC, where Bank A's peer IP range is 10.0.0.0/28 , requesting the connecting IP range to be 192.168.0.0/28 ; Bank B's peer IP range is 10.1.0.0/28 , requesting the connecting IP rage to be 192.168.1.0/28 . Then you can configure two local source IP port translations as follows:

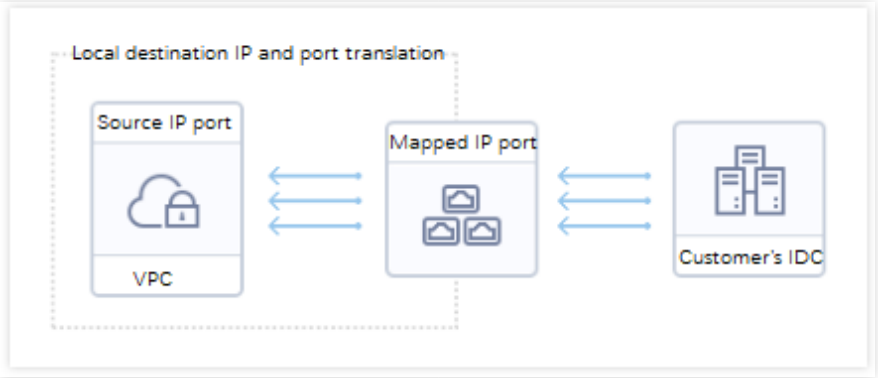
- Address pool A 192.168.0.1 - 192.168.0.15 ; ACL rule A; source IP 172.16.0.0/16 ; destination IP 10.0.0.0/28 ; destination port ALL.
- Address pool B 192.168.1.1 - 192.168.1.15 ; ACL rule B; source IP 172.16.0.0/16 ; destination IP 10.1.0.0/28 ; destination port ALL.
  Then, the network requests that actively access A and B in the VPC are translated into random ports in the corresponding address pools according to ACL rules A and B, and access the corresponding DC tunnels.

Local Destination IP Port Translation

1. Note for Conversion

- The local destination IP port translation is a method for the DC peer to actively access the VPC. The

designated port of the designated IP in the VPC is mapped to a new IP and port. The DC peer can only communicate with the designated IP port in the VPC by accessing the mapped IP port, and other IP ports are not exposed to the DC peer.



- The local destination IP port translation does not support ACL rule adaptation. Therefore, the IP port translation rules will take effect on all DC tunnels connected to the DC gateway. The local destination IP port translation is only effective for the DC tunnel peer to actively access the VPC. If the VPC needs to actively access the DC peer, you can configure the local source IP port translation.

2. Example of Conversion

The IP range of VPC C is 172.16.0.0/16 If you only want to open some ports for active access by the DC peer, you can configure them as follows:

- Mapping A original IP port 172.16.0.1:80 ; Mapping IP port 10.0.0.1:80 .
- Mapping B original IP port 172.16.0.0:8080 ; mapped IP port 10.0.0.1:8080 .
  Then the DC peer can actively access ports 10.0.0.1:80 and 10.0.0.1:8080 , to achieve active access to the two ports 172.16.0.1:80 and 172.16.0.0:8080 in the VPC.

> Note:
>
> - After the local source and destination IP port translation are configured, the DC gateway will only send the translated IP port route to the DC peer. Therefore, the unconfigured local IP port will not be able to actively initiate requests or passively accept requests. However, DC gateways cannot replace professional network firewalls. If you need advanced network protection, configure security groups and network ACL policies in the VPC and deploy professional physical network firewall devices in your IDC computer room.
> - When IP translation and IP port translation are configured at the same time, IP translation is matched first. When there is no matching option for IP translation, IP port translation is matched.
> - When the DC gateway is configured with peer IP translation, in the destination IP of the local source IP port translation ACL rule field, you need to fill in the mapped IP of the peer IP

translation, instead of the original IP.

Use Cases

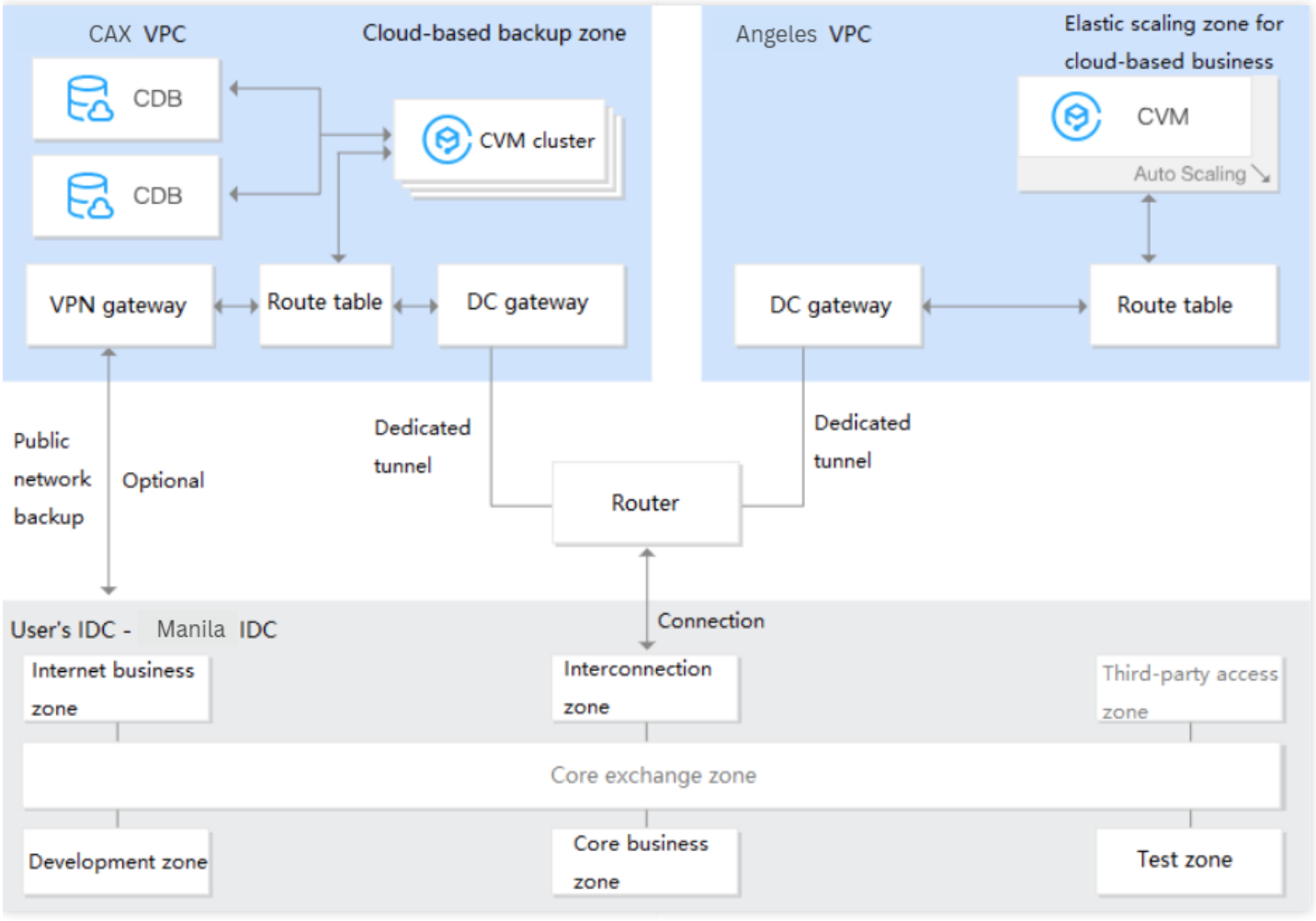
DC can be applied to the following scenarios:

- Data migration, backup, and recovery

DC provides you with fast and reliable connections between your local data center and the cloud network, supporting bandwidth up to 100 Gbps, which is ideal for scenarios such as data migration, disaster recovery, and other high availability policies.

- Flexibly Expand the Computing Power of Local Data Centers

DC is a predictable, high-throughput, reliable connection. Local data centers can leverage the elastic computing capabilities of the cloud to flexibly expand the application layer capabilities of off-cloud data centers, and enjoy the scale and economic benefits of the public cloud without sacrificing network performance.



Limits

Resource limitations

Resources	Restrictions	can request for high quota
Connection/User	10	Yes
DC Tunnel/Connection	5	Yes
DC Gateway/VPC	1	No
Local IP Translation/DC Gateway	100 entries	Yes
Peer IP Translation/DC Gateway	100 entries	Yes
Quantity of IPs Translated at Local Source IP Port/DC Gateway	20	Yes
Local Destination IP Port Translation/DC Gateway	100 entries	Yes
quantity of DC tunnel static route entries	20 entries	No
quantity of DC tunnel BGP routing entries	100 entries	No

Connection Restrictions

Direct Connect

- When you create a new DC gateway, the IP translation and IP port translation contents are empty by default, and both IP translation and IP port translation are ineffective.
- The DC tunnel supports two routing methods: BGP routing and static routing.
- Pay attention to the following restrictions when you publish routes:
  To improve the fine-grained scheduling capabilities of your network, avoid publishing the following routes:

10.0.0.0/8 , 172.16.0.0/12 , 192.168.0.0/16 , 100.64.0.0/10 .
You can split the above large segments into the following for publishing:

- 10.0.0.0/8 Split into: 10.0.0.0/9 + 10.128.0.0/9`.

- 172.16.0.0/12 Split into: 172.16.0.0/13 + 172.24.0.0/13`.
- 192.168.0.0/16 Split into: 192.168.0.0/17 + 192.168.128.0/17`.
- 100.64.0.0/10 Split into: 100.64.0.0/11 + 100.96.0.0/11`.

IP Translation

- The original IP must be within the CIDR range of the VPC.
- The mapped IP cannot be within the CIDR range of the VPC where the DC gateway is located.
- The original IP cannot be repeated, that is, one IP in a VPC can only be mapped to one IP.
- The mapped IP must be unique and cannot be repeated. That is, multiple VPC IP addresses cannot be mapped to the same IP.
- The original IP and mapped IP do not support broadcast address 255.255.255.255 , Class D address 224.0.0.0 - 239.255.255.255 , Class E address 240.0.0.0 - 255.255.255.254 .
- The local IP translation of the DC gateway supports mapping of a maximum of 100 IP addresses, and each IP mapping supports a maximum of 20 ACL rules (if you need to increase the quota, please submit a ticket application).

IP Port Translation

- The mapped IP pool cannot be within the CIDR range of the VPC where the DC gateway is located.
- ACL rules of multiple mapped IP pools cannot overlap, otherwise it causes network address translation conflicts.
- IP addresses in multiple mapped IP pools cannot overlap.
- The mapped IP pool only supports single IP or continuous IP, and the IP range of continuous IPs /24 must be consistent, that is, 192.168.0.1 - 192.168.0.6 is supported but 192.168.0.1 - 192.168.1.2 is not.
- The mapped IP address pool does not support the broadcast address 255.255.255.255 , Class D address 224.0.0.0 - 239.255.255.255 or Class E address 240.0.0.0 - 255.255.255.254 .
- The local source IP port translation supports a maximum of 100 IP pools, and each address pool supports a maximum of 20 ACL rules (if required, you can submit a ticket to request for a quota increase).
- The original IP addresses and the mapped IP addresses cannot be the broadcast address (255.255.255.255), class D addresses (224.0.0.0-239.255.255.255), and class E addresses (240.0.0.0-255.255.255.254).
- The original IP port is unique, that is, the same IP port in a VPC can only be mapped to one IP port.
- The mapped IP port cannot be within the CIDR range of the VPC.
- The mapped IP ports cannot be repeated, that is, one IP port cannot be mapped to multiple VPC IP ports.
- The local destination IP port translation supports up to 100 IP port mappings (if you have any needs, you can submit a ticket to request for a quota increase).

- When you configure IP translation and IP port translation at the same time, if both are matched, IP translation is matched first.
- When you need to switch from IP translation to IP port translation, clear the original IP translation rules and refresh the page to edit the IP port translation rules.

Related products

For relevant products information, see the table below:

Product Name	Relationship with DC
Virtual Private Cloud (VPC)	Connection is available to achieve the integration of the data center in the VPC and the private network of your own IDC.
Network ACL	You can configure multiple local IP translation rules and configure a network ACL for each local IP translation rule.
Routing table	Hybrid cloud deployment requires configuration of the routing table associated with the subnet.

Purchase Guide
Billing Overview

This document lists the billing and pricing instructions for connections, DC tunnels, and DC gateways.

Billing Description

The cost of DC consists of three parts: Connection, DC tunnel, and DC gateway.

Connection

The Connection refers to the channel between the user's local IDC and the DC point. User costs include Connection charges and other parties' charges.

- Connection Charges
  - The fee for using an exclusive port includes: initial installation fee and exclusive port resource occupation fee.
  - For connection to shared partner port resources, you do not need to pay the initial installation fee and exclusive port resource occupation fee.
- Other Parties' Charges
  - Fiber Optic Installation Fee: The cost of laying optical cables between the user's local IDC and the DC point, which is purchased from an operator and paid by the user.
  - In-House Wire (IHW) Rental Fee: The DC point room is generally a neutral IDC room. There may be fiber-to-building or in-house wire rental fees. You need to consult the operator or line provider for detailed information.

DC tunnel

The DC tunnel refers to the private network section between the DC point and the DC gateway on the cloud.

Direct Connect Gateway

A DC gateway is a gateway object on your cloud platform. Traffic passing through the DC gateway is charged.

- Inbound Traffic: Traffic that flows from the user's local data center to the cloud platform data center through the DC channel.
- Outbound Traffic: traffic that flows from the cloud platform data center to the user's local data center through the DC channel.

Quick Start

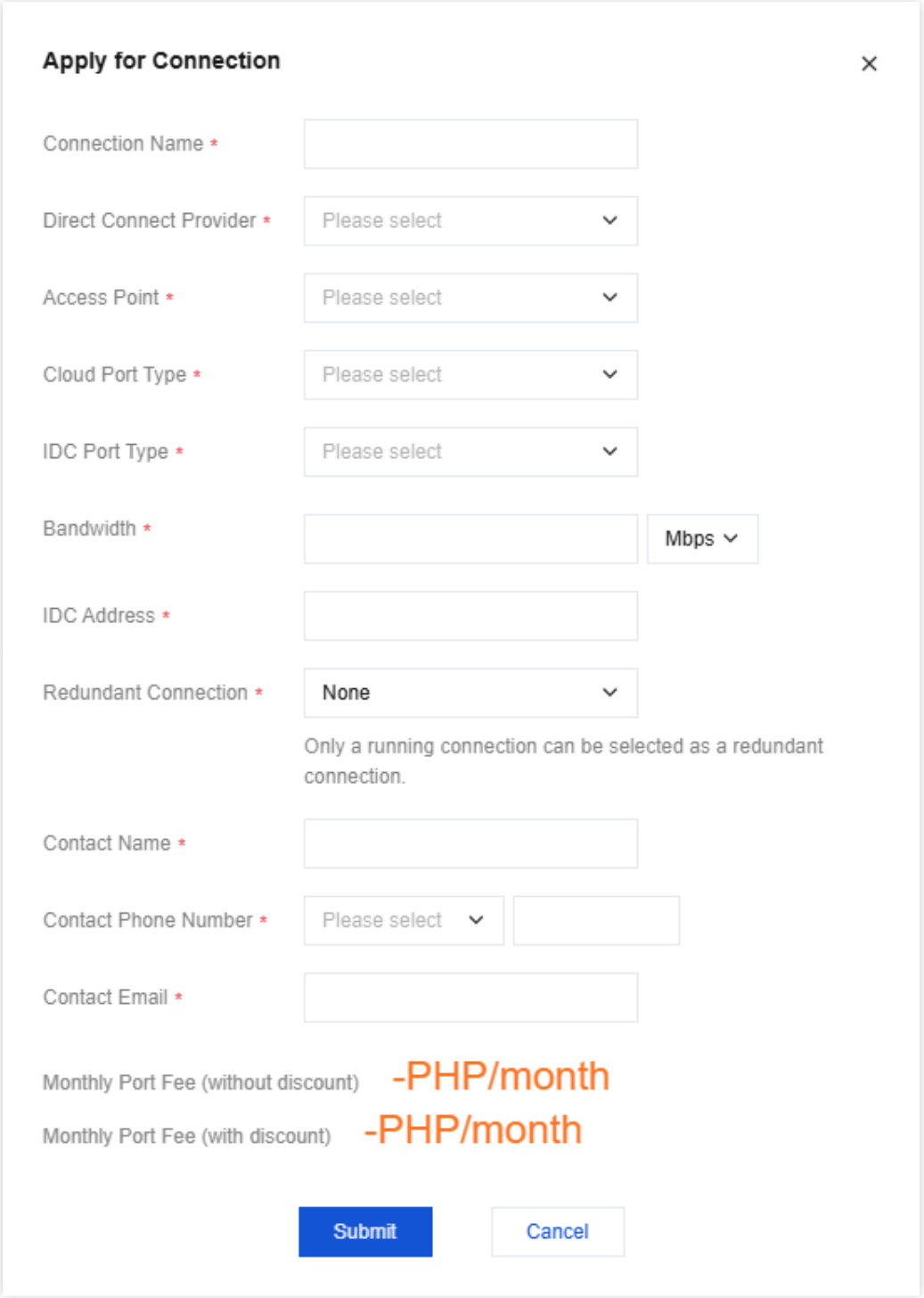
After you purchase the DC service, you can quickly create and log in to the dedicated line instance through visual operations on the console interface.

Step 1: Log in to the DC console

Log in to the Cloud Console, select Cloud Products >Cloud Computing & Networking > Direct Connect to open the DC console.

Step 2: Create a connection

1. In the directory on the left, click Connection to open the management page.
2. On the Connection page, click Create.
3. Please fill in the relevant parameter information according to your dedicated line requirements. After submitting your request, the cloud platform will send a DC manager to verify the detailed information with you as soon as possible.



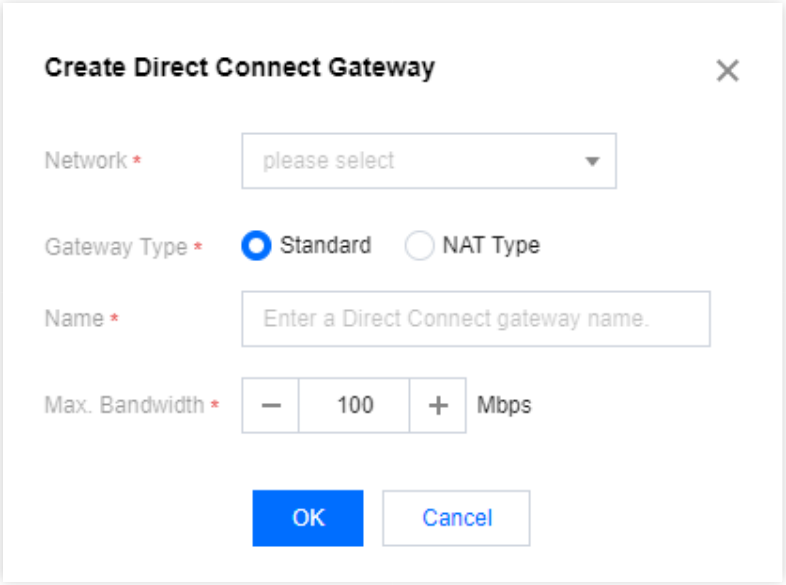
Step 3: Create DC gateway

1. You can log in to the cloud console and select Cloud Products > Cloud Computing & Networking > Virtual Private Cloud to enter the VPC console.

2. In the directory on the left, click Direct Connect Gateway to open the management page.

3. Select a region and network at the top of the page and click Create.

4. In the Create Direct Connect Gateway dialog box that pops up, enter a custom name, select the network type to be associated with, and set the bandwidth limit.

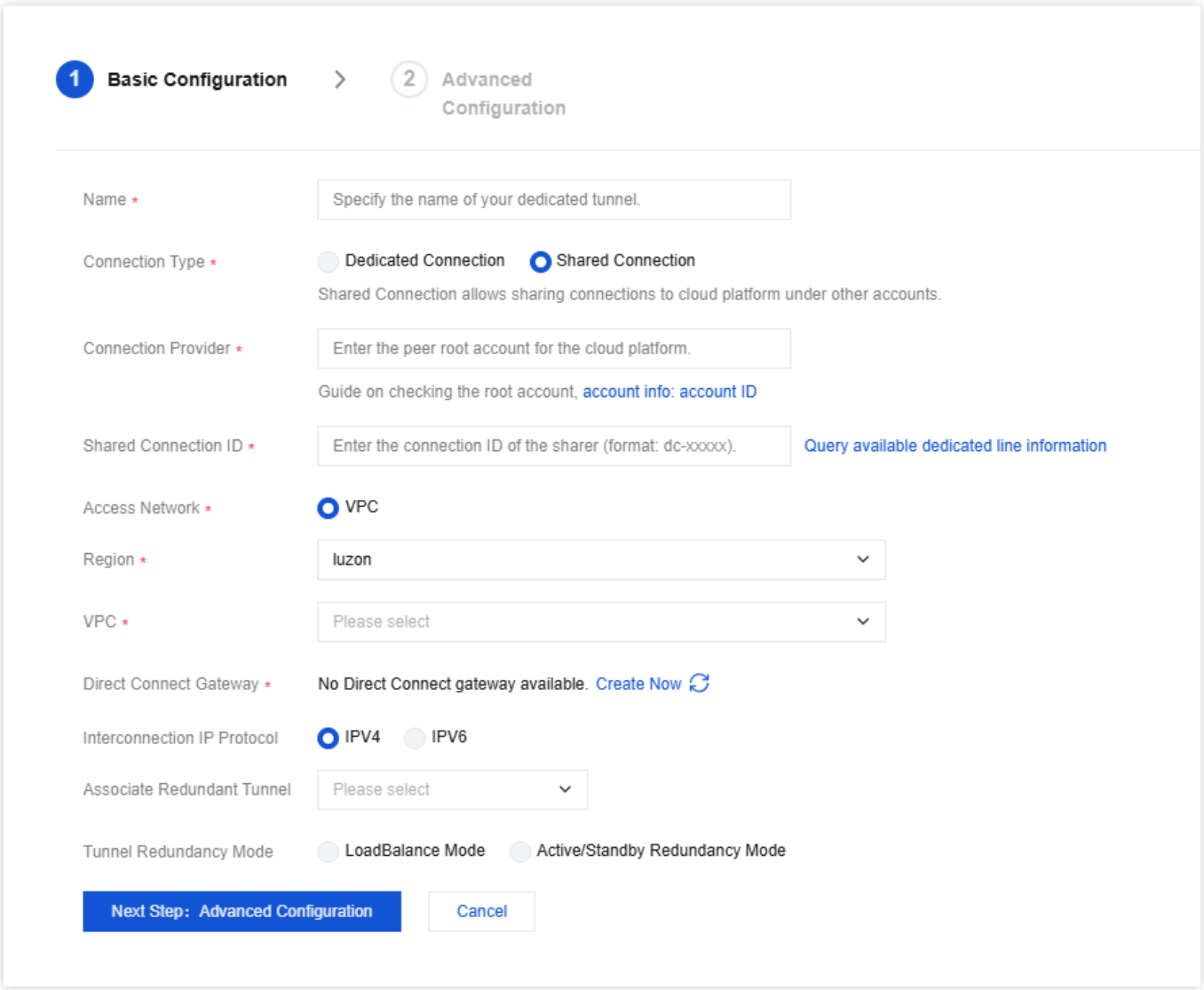


> Note:
>
> If the IP addresses at both ends of the dedicated line conflict, you can create a NAT gateway and configure network address translation rules on the DC gateway.

5. Click OK to complete the creation of the DC gateway.

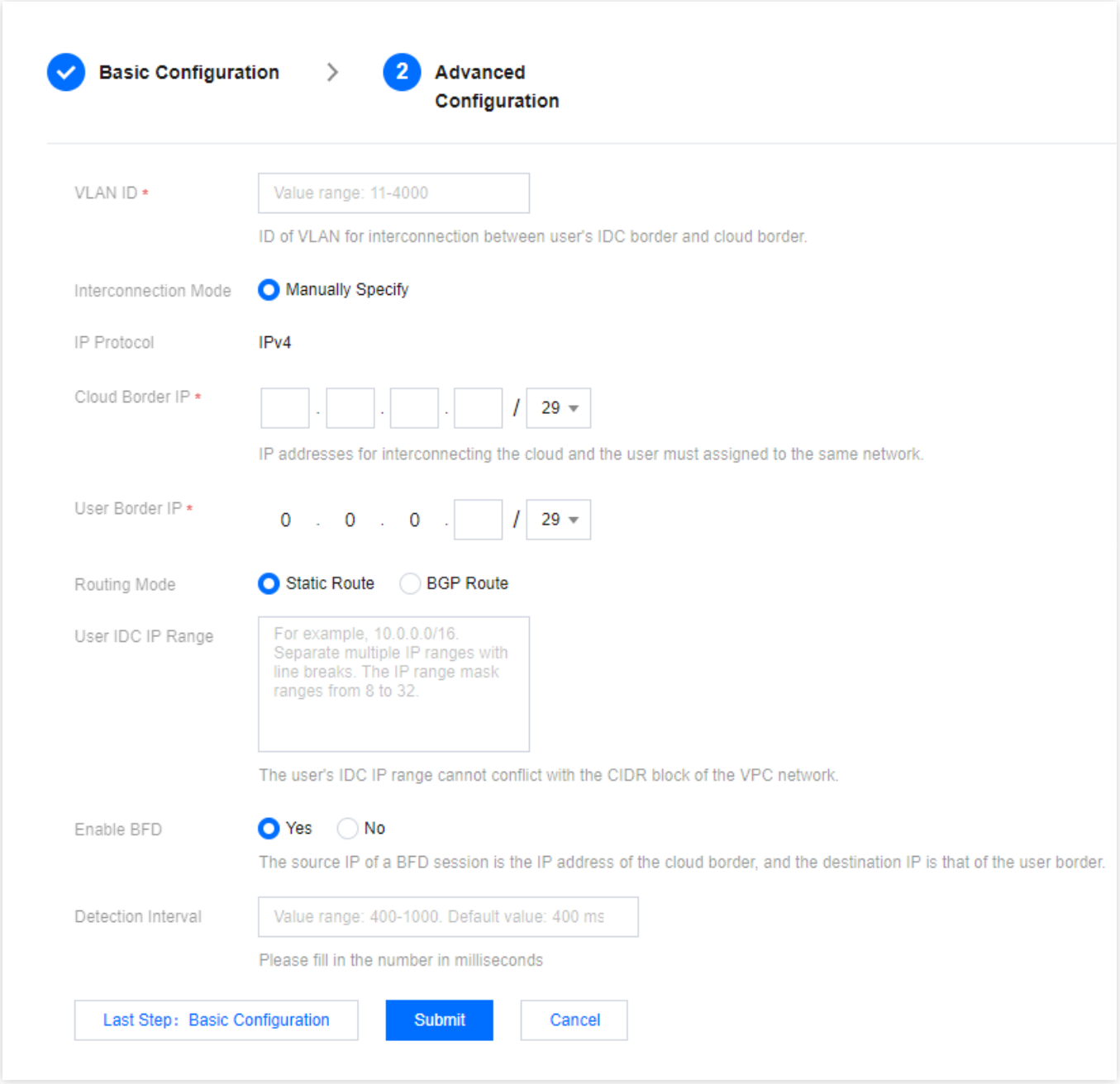
Step 4: Create a Dedicated Tunnel

1. Log in to the Cloud Console, select Cloud Products >Cloud Computing & Networking > Direct Connect to open the DC console.
2. In the directory on the left, click Dedicated Tunnel to open the management page.
3. Click Create.
4. Basic Configuration:



- Name: Create a name for the custom DC tunnel.
- Connection Type: Select a Connection in the running status under your cloud account or a Connection of a shared partner account (obtain Connection information from the partner).
- Access Network: VPC.
- Direct Connect Gateway: Please select the DC gateway under your VPC. If you do not have one, please create a DC gateway according to the prompts on the interface. After the creation is successful, please click the Refresh button to update the gateway list information.

5. Advanced Configuration:

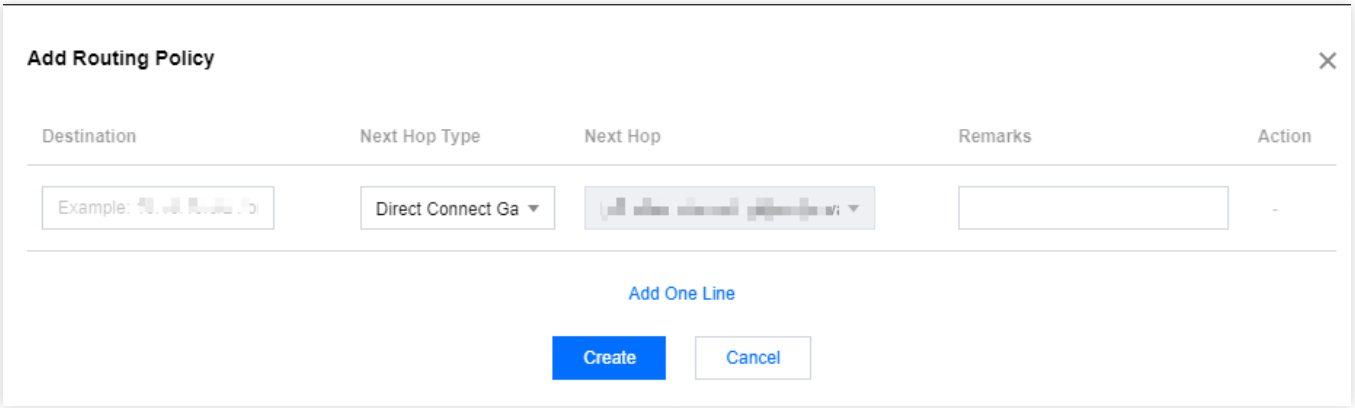


- VLAN ID: If the Connection is provided by a partner, please obtain the VLAN ID from the partner.
- Bandwidth: Set a bandwidth upper limit.
- Border IP: Refers to the interconnection API IP at both ends of the connection (IDC end and cloud connection device).
- Routing Mode: Supports BGP routing and static routing.

6. IDC Device Configuration: The third step in requesting a DC tunnel. You can download the general configuration guide document in the console.
7. Click Submit to complete the creation of the DC tunnel.

Step 5: Configure routing table

1. You can log in to the cloud console and select Cloud Products > Cloud Computing & Networking > Virtual Private Cloud to enter the VPC console.
2. In the directory on the left, you can click Route Table to open the management page.
3. In the list, find the routing table associated with the subnet that requires communication, click its ID, and go to the details page.
4. Click Add Routing Policy, enter the destination IP range, select DC Gateway for the next hop type, and select the gateway name for the next hop.



5. Click OK.

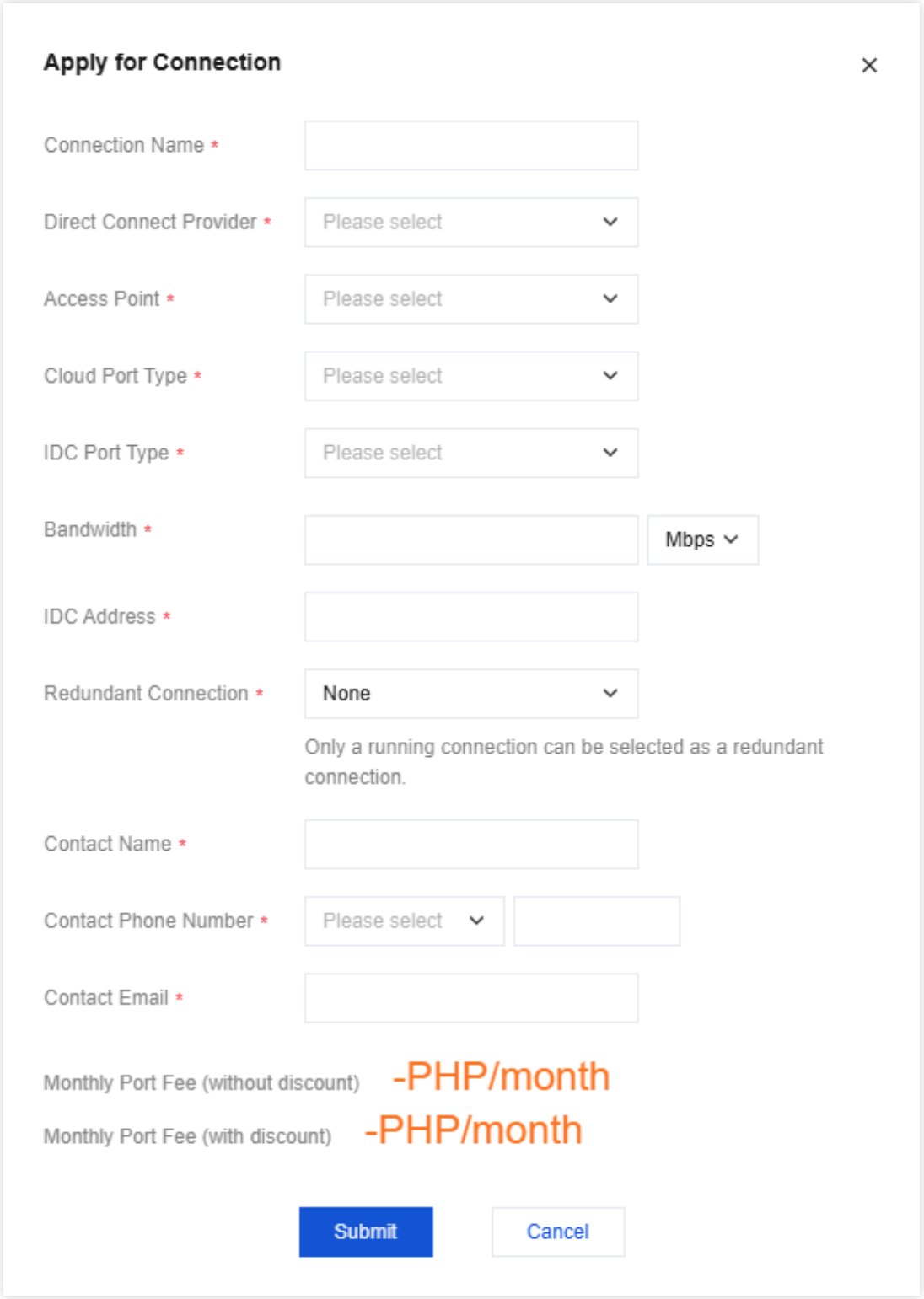
Operation Guide
Managing Connection
Applying for Connection

All connection applications must be initiated and completed in the console.

Console Application

1. Log in to the Direct Connect console.
2. In the left navigation bar, click Connection to enter the physical dedicated line interface.
3. Click Create to apply for a connection.

   To initiate the construction of a connection, users need to fill in the following information: After the construction application is initiated, the connection status will be converted to Application in Progress, and the operational end management staff will evaluate your DC application.



Parameter	Description	Remark
Connection Name	Please customize the name of your connection.	Support changes

Parameter	Description	Remark
Direct Connect Provider	Includes the following options: China Telecom, China Mobile, China Unicom, Others in China (select this option for all domestic dedicated lines other than the three major operators), Others abroad (select this option for all overseas dedicated lines)	-
Access Point	For connections to the cloud platform, it is recommended to choose a nearby connection point.	The city where the connection point is located generally has at least 2 connection points, which can achieve dual-line disaster recovery.
Cloud Port Type	The Cloud port type used to interconnect the connection line with the Converge Cloud connection device	Select the corresponding API type according to bandwidth. You can consult your DC service provider or Converge Cloud architect/after-sales manager for technical support.
IDC Port Type	The IDC port type used to connect the IDC connection to the Converge Cloud connection device	Select the corresponding API type according to bandwidth. You can consult your DC service provider or Converge Cloud architect/after-sales manager for technical support.
IDC Address	Province, city, detailed address	Please provide IDC address details as precisely as possible, including the specific floor.
Bandwidth	Support 2 to 100,000 Mbps	-
Redundant Connection	Select the corresponding connection as the primary and backup relationship to avoid linking two connection lines to the same connection device and ultimately prevent single point failure.	The selection of the primary-backup relationship is mainly to avoid dual-line connection to the same point. The primary-backup relationship of the DC tunnel needs to be applied in the DC tunnel sub-product.
Contact Name	Name of the DC contact person	-
Contact Phone Number	DC contact person's phone number	-

Parameter	Description	Remark
Contact Email	Email of DC contact person	-

Construction acceptance

After the management completes the evaluation and gives the go ahead, they will coordinate relevant resources to assist in building connections. After the connection is built, it will automatically enter the operating status.

Canceling Connections

1. Log in to the Direct Connect console.
2. In the left navigation bar, click Connection to enter the physical dedicated line interface.
3. Click Delete in the Action column to initiate the cancellation of the connection. After the cancellation is initiated, the after-sales manager will contact you and assist you in completing the cancellation process.

Sharing Connection

You can share the connections of other accounts to build DC tunnels, and can also share the connections under your own account with other cloud platform customers.
For details, see Applying for Tunnel.

View Monitoring Information

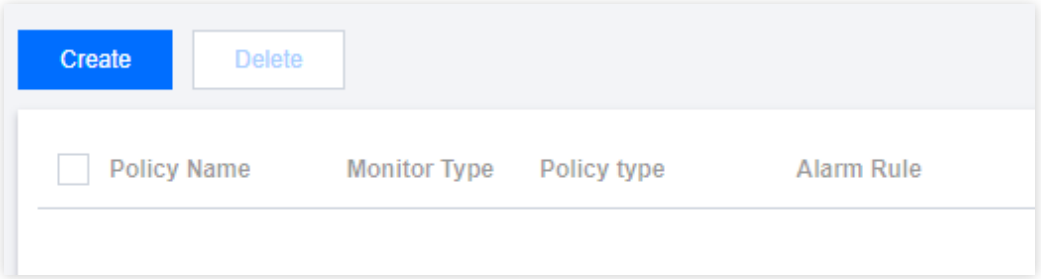
Connection supports the query of monitoring information (network outbound bandwidth, network inbound bandwidth). You can query the monitoring information of connection through the Converge Cloud console. The steps are as follows:

1. Log in to the Direct Connect console.
2. In the left navigation bar, click Connection to enter the physical dedicated line interface.
3. Find the connection you want to view in the list and click the Monitor icon.

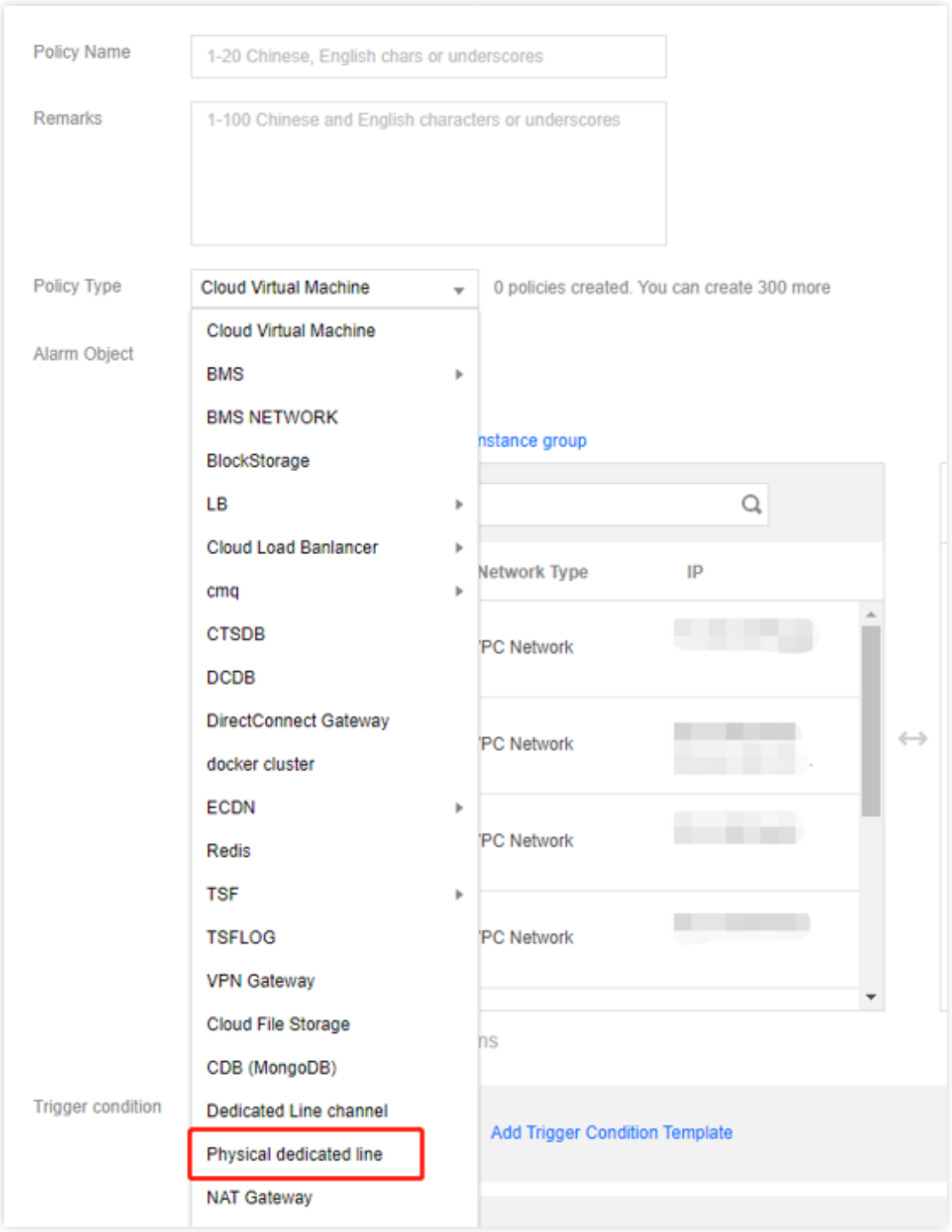
Setting Alarms

Connections support the configuration of monitoring alarms. The configuration steps are as follows:

1. Log in to the Cloud Monitor console.
2. Click Alarm Configuration > Alarm Policy in the left sidebar to open the management page.
3. Click Create.



4. Edit the alarm policy on the new page:
    - Enter the alarm policy name/ID.
    - Select Physical dedicated line for the policy type.
    - Alarm Object: Select the associated DC tunnel.
    - The alarm trigger conditions can be selected as: Outgoing bandwidth, Incoming bandwidth, and Bandwidth usage.
    - Alarm Channel: Set the recipient of the alarm.
    - API Callback: If you need to push the alarm information to a specified address, you can fill in this item. Cloud monitoring will push the alarm information to the address in time.



5. Set the alarm channel and click Finish to complete the configuration of the alarm policy.

After the connection alarm configuration is completed, you can receive system alarms according to the settings of the alarm receiving group.

Managing a DC Tunnel
Applying for Tunnel

Restrictions on the Use of Large IP Ranges

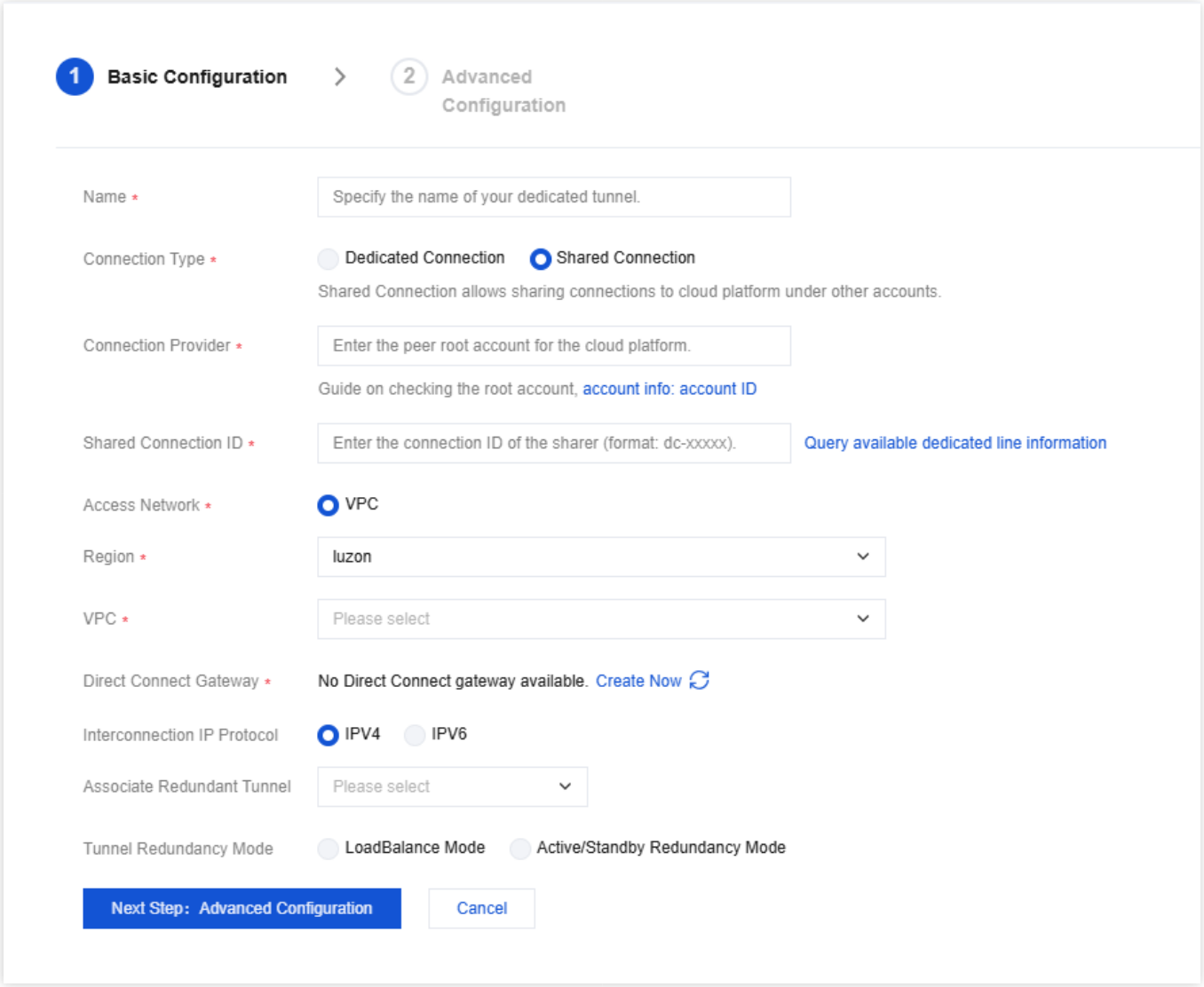
To improve the fine-grained scheduling capabilities of your network, avoid publishing the following routes: 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16, 100.64.0.0/10.
You can split the above large routes into the following sections:

- 10.0.0.0/8 is split into: 10.0.0.0/9 + 10.128.0.0/9.
- 172.16.0.0/12
  is split into: 172.16.0.0/13 + 172.24.0.0/13.
- 192.168.0.0/16
  is split into: 192.168.0.0/17 + 192.168.128.0/17.
- 100.64.0.0/10
  is split into: 100.64.0.0/11 + 100.96.0.0/11.

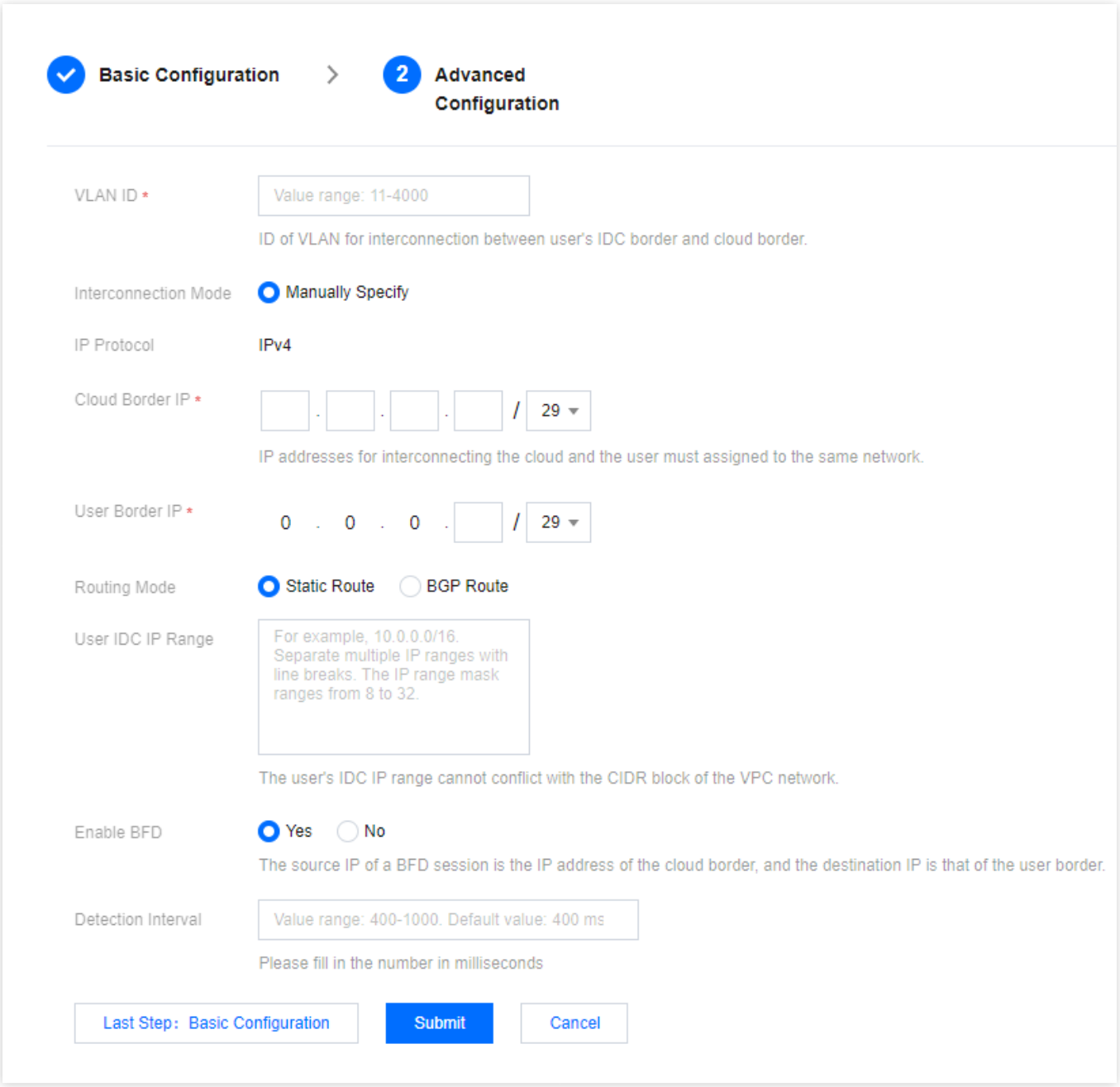
Applying Steps

1. Log in to the Direct Connect console.
2. In the left navigation bar, click Dedicated Tunnel to enter the Dedicated Channel interface.
3. Click Create, refer to the table below to configure the name, dedicated line type, access network, region, associated dedicated line gateway, and other basic configurations. After completion, click Next.

- Assuming your account has a suitable Connection, select Dedicated Connection and enter the relevant information. The application page is as follows:
- Assuming your account does not have a suitable Connection, you can select Shared Connection. The application page is as follows:



4. Advanced Configuration:



Parameter	Description	Remark
Dedicated tunnel name	Create your own DC tunnel name.	-
Connection Type	- Dedicated Connection: Use the Connection of this account. - Shared connection: Use the Connection of another account. Shared connection does not mean sharing the Connection bandwidth, but sharing the Connection port of the cloud platform. In this mode, different tenants are isolated through 802.1q VLANs technology.	To apply for a shared connection, you only need the acceptance by the Connection owner. The intervention of the cloud platform is not needed.

Parameter	Description	Remark
Connection	Dedicated Connection: Select the Connection ID for which you need to establish a DC tunnel.	-
Connection provider	Shared Connection: Enter the account that owns the connection you want to share.	-
Shared connection ID	Shared Connection: Enter the Shared Connection ID for which you want to establish a DC tunnel.	-
Access network	Supports Virtual Private Cloud.	-
VPC	VPC: Select the network instance ID to which the DC tunnel needs to connect.	-
Region	Indicates the region of the DC gateway.	In the Shared Connection mode, you need to obtain the regional information of DCion points from the owner of the Connection.
Direct Connect Gateway	The VPC DC gateway is in the same region as the VPC.	-
VLAN ID	VLAN ID = 0: Indicates that the Connection does not enable a sub-API and can only create one tunnel.	MSTP DC transparent transmission of multiple VLANs requires the operator line to enable the Trunk mode.
Interconnect IP	Supports user customization and random allocation by the cloud platform (you can obtain the randomly allocated address by going to the tunnel details after submitting the application to obtain the interconnected IP address). - Cloud Edge IP: Indicates the edge interconnection IP on the cloud platform side of the Connection. - User Boundary IP: Indicates the interconnection IP on the Connection's user side (or carrier network side), which needs to be configured by the user.	If you choose to publish an Internet IP to a DC gateway, please plan the IP in advance to avoid IP conflicts.
Routing mode	Supports BGP routing and static routing.	Cloud Platform ASN: 45090
BGP ASN	BGP Route: Optional. Please enter the BGP neighbor AS number on the CPE side. If you do not enter this number, the system will randomly assign one.	-

Parameter	Description	Remark
BGP keys	BGP Route: Optional. Enter the MD5 value of the BGP neighbor. Leaving it blank means no BGP key is required.	-
User IDC IP range	Static Route: Enter the IP range of the user-side CPE. In non-NAT mode, make sure it does not conflict with the VPC IP range.	Support Changes: The IP range can be updated later through the Tunnel Change console.
Bandwidth limiting	Set the bandwidth upper limit, which cannot exceed the single line threshold.	-
Health examination	- Yes: Enable BFD health check. - No: No health check is performed.	Currently, only BFD health check is supported.
Detection interval	Enter the BFD health check detection interval.	Unit: milliseconds. Default value: 400 milliseconds. Falls in the range of [400, 1,000].

Connection Status Description

The possible status of a DC tunnel can be one of the following:

- Applying
  The system has received the user's applicatiion for a new tunnel and is ready to initiate a task creation.
- Pending acceptance
  The Connection owner is in the process of approval. Once the Connection owner accepts the tunnel application, the tunnel can be created without approval.
- Configuring
  The system is applying parameter configurations. If the "Configuring" status takes too long, it indicates there's an issue with the system application. Please consult your architect or submit a support ticket.
- Configuration completed
  The system has completed the configuration according to the parameters you entered but has not yet pinged your IDC interconnection address. This status allows deletion.
- Connected
  The system has pinged your IDC device interconnection address, but it does not mean that the service has been successfully connected. Please go to VPC to complete the relevant configuration to achieve connection.
- Deleting
  The system is processing your deletion request. If the "Deleting" status takes too long, it indicates there's an issue with the system deletion. Please consult your architect or submit a support ticket.

Changing a Tunnel

When the Dedicated Tunnel status displays Ready, you can also change channel parameters, modify tunnel bandwidth, and perform other operations in the Direct Connect console.

> Note:
>
> In the Shared Connection mode, the bandwidth change cannot be initiated in the Dedicated Tunnel but must be initiated by the owner of the Connection.

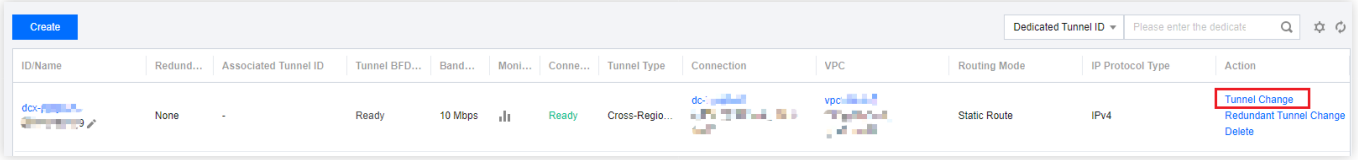
Restrictions on the Use of Large IP Ranges

To enhance the fine-tuned scheduling capability of your network, please avoid publishing the following routes: 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16, 100.64.0.0/10.
You can split the above large segments into the following publications:
10.0.0.0/8
Split into: 10.0.0.0/9 + 10.128.0.0/9.
172.16.0.0/12
Split into: 172.16.0.0/13 + 172.24.0.0/13.
192.168.0.0/16
Split into: 192.168.0.0/17 + 192.168.128.0/17.
100.64.0.0/10
Split into: 100.64.0.0/11 + 100.96.0.0/11.

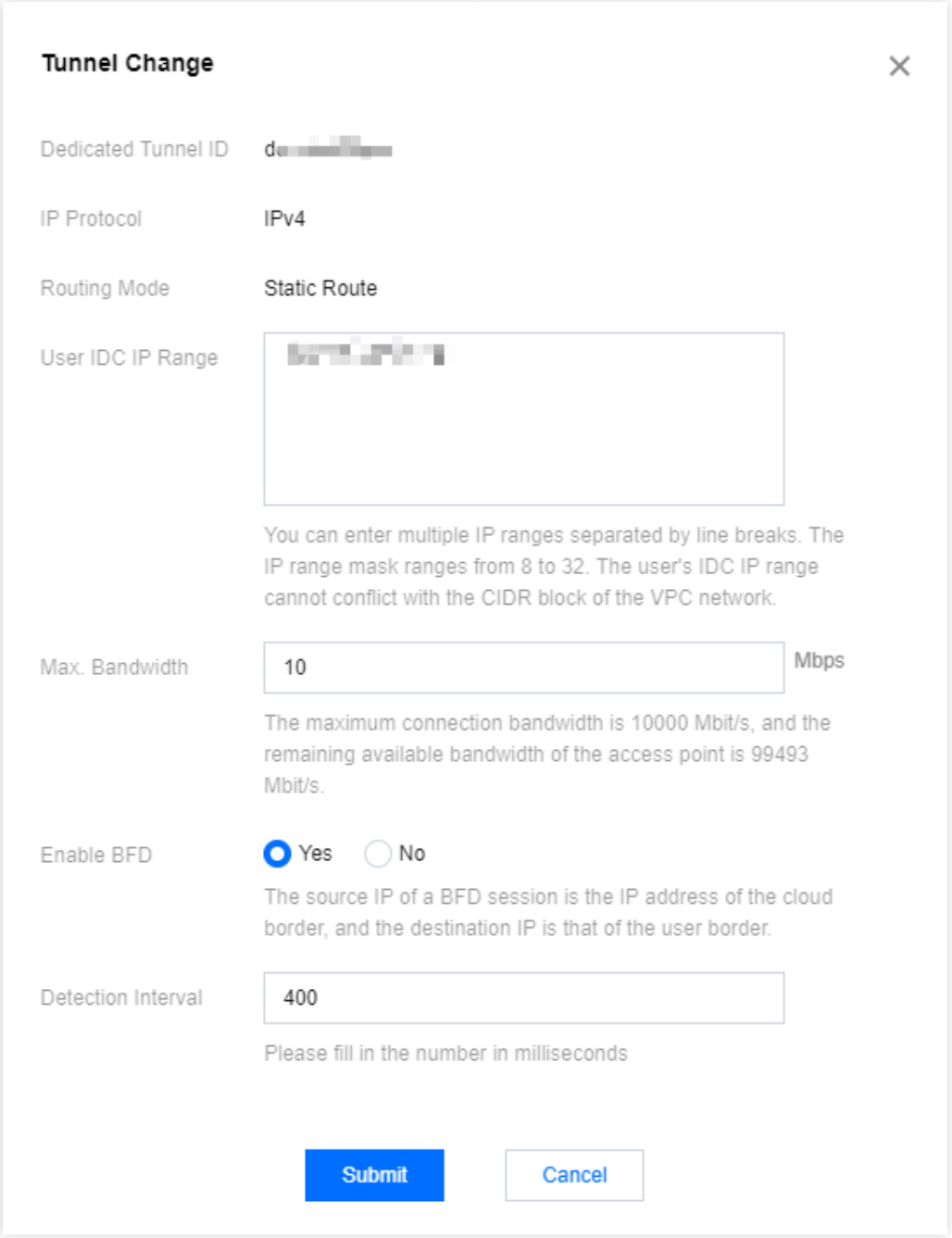
Changing the Tunnel Route

Changing the Dedicated Tunnel of the Static Route

1. Log in to the Direct Connect console.
2. In the left navigation bar, click Dedicated Tunnel to enter the Dedicated Tunnel interface.
3. On the Dedicated Tunnel page, click Tunnel Change in the Operation column to the right of the channel whose parameters need to be changed.

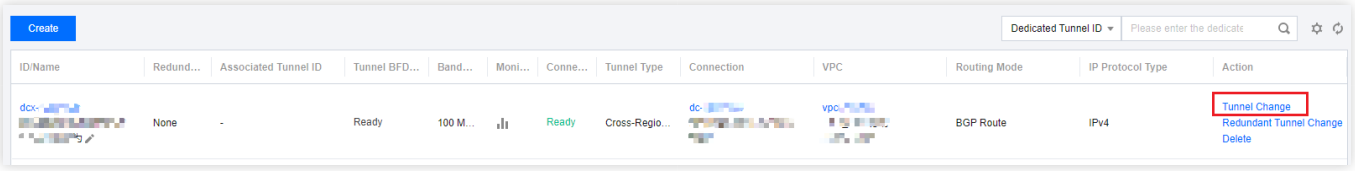


4. On the Tunnel Change Page, follow the interface prompts to make modifications. After completing the changes, click Submit.

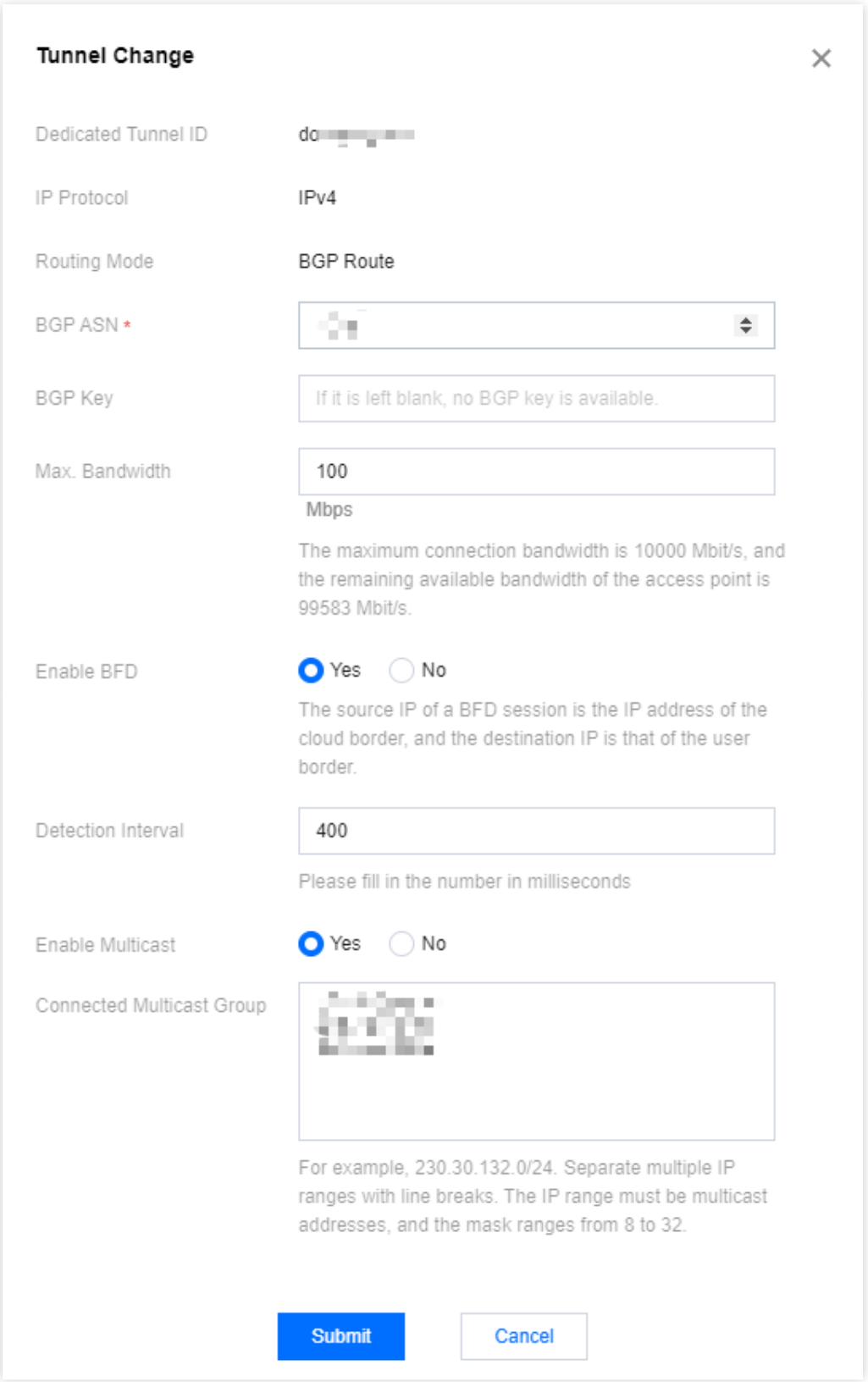


Changing the BGP Routing Dedicated Tunnel

1. On the Dedicated Tunnel page, click Tunnel Change in the Operation column to the right of the channel whose parameters need to be changed.



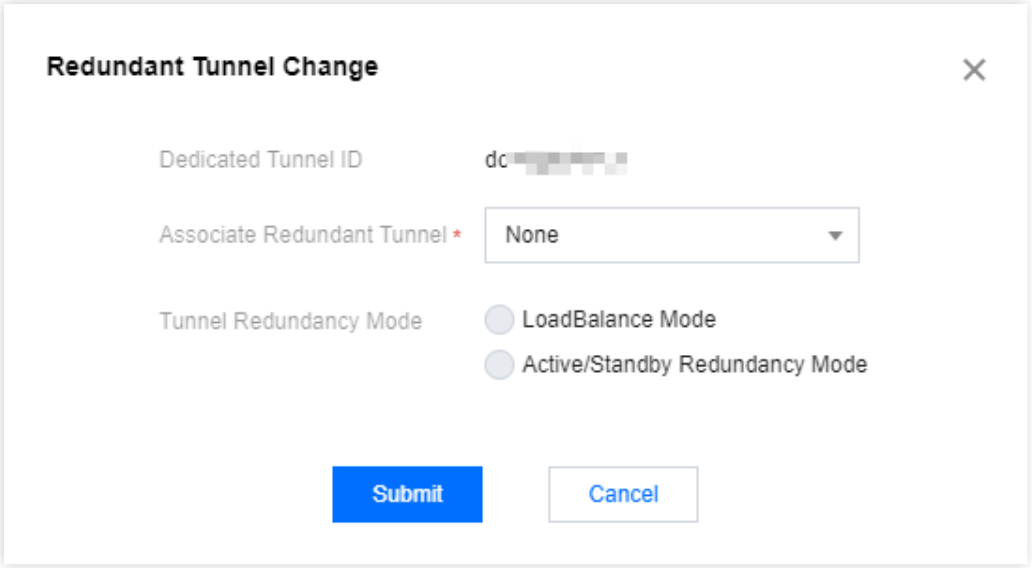
2. On the Tunnel Change Page, follow the interface prompts to make modifications. After completing the changes, click Submit.



Changing the Redundant Tunnel

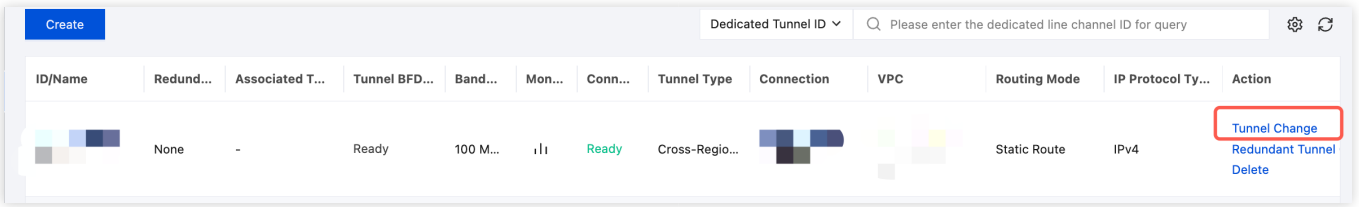
1. On the "Dedicated Tunnel" page, click Redundant Tunnel Change in the "Actions" column to the right of the tunnel for which parameters need to be changed.
2. On the Tunnel Change Page, follow the interface prompts to make modifications. After completing the

changes, click Submit.

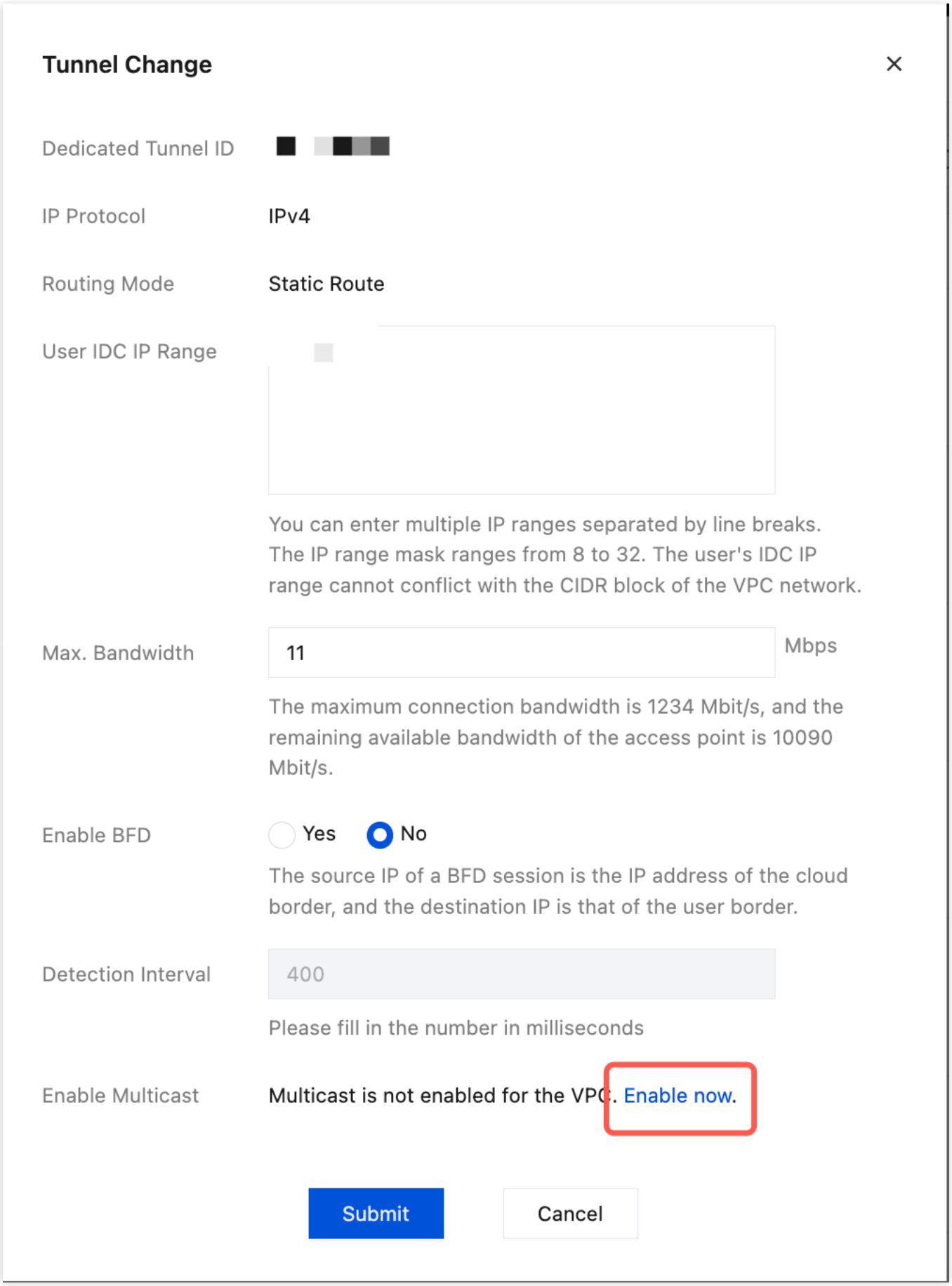


Enabling Multicast

1. On the Dedicated Tunnel page, click Tunnel Change in the Operation column to the right of the channel whose parameters need to be changed.



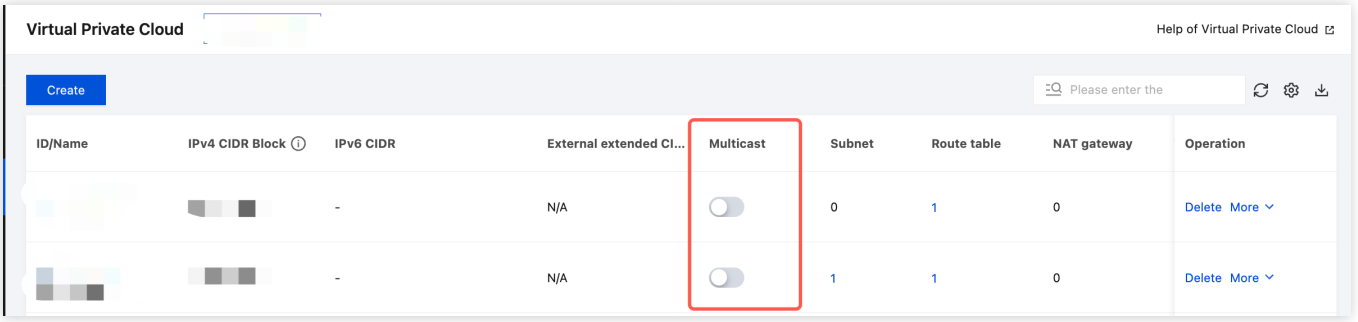
2. If multicast is disabled for your VPC, follow the on-screen prompts to enable it. In the Tunnel Change dialog box, click Enable now to the right of Enable Multicast.



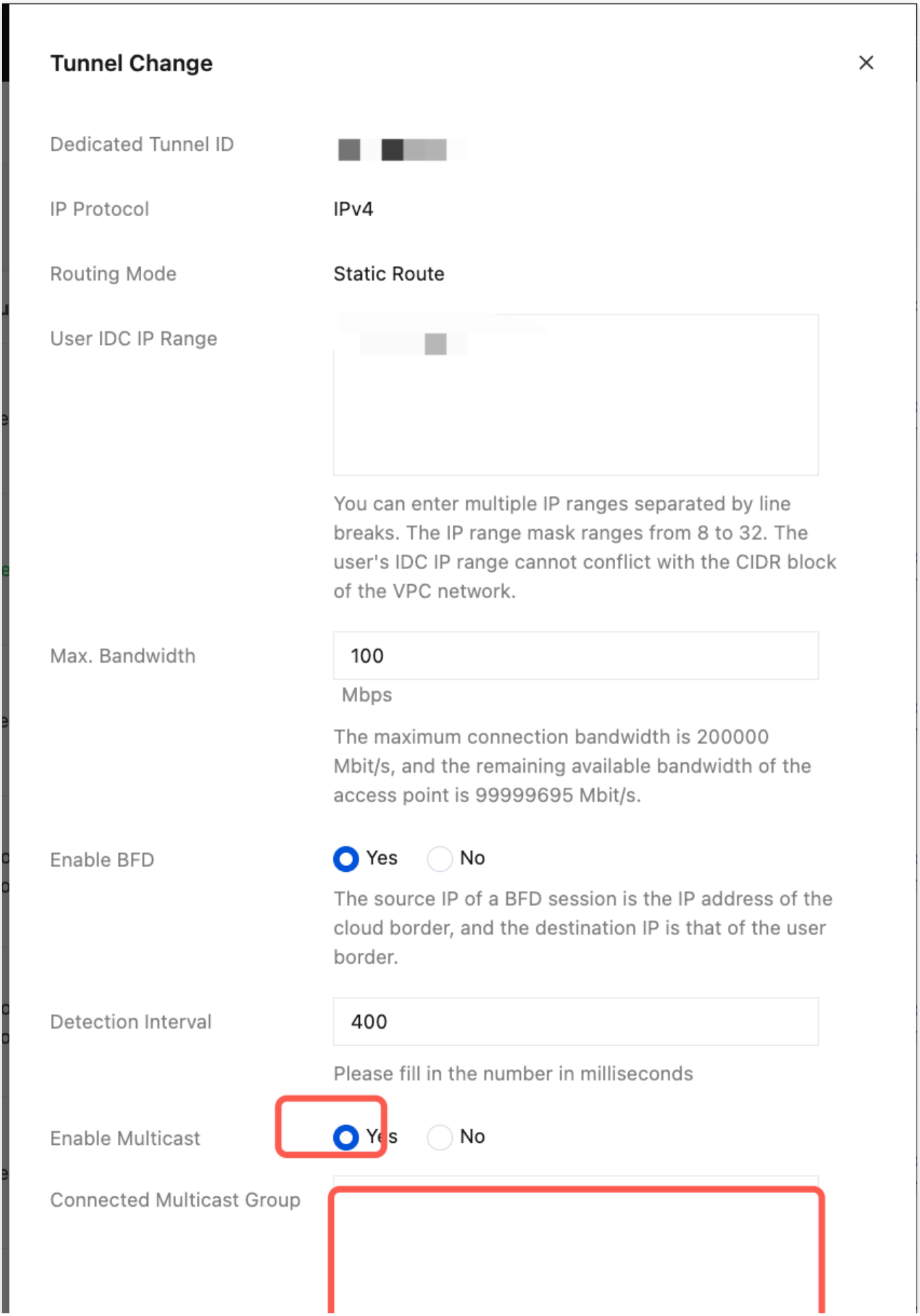
3. Go to the VPC page, select the ID of the VPC that is currently used, and toggle on the switch

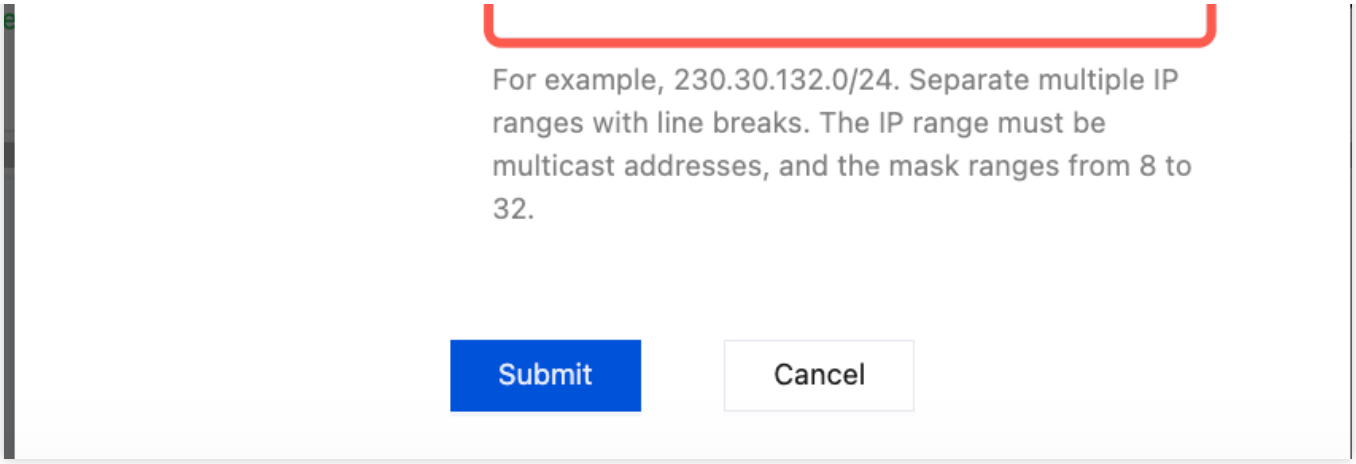


in the Multicast column to enable multicast for the VPC.



4. Go back to the Dedicated Tunnel page and find the tunnel whose parameters need to be changed and click Tunnel Change in the Operation column.
5. In the Tunnel Change dialog box, follow the on-screen prompts to enable multicast. Select Yes for Enable Multicast, set Connected Multicast Group, and click Submit.


Tunnel Change
Dedicated Tunnel ID
IP Protocol
IPv4
Routing Mode
Static Route
User IDC IP Range
You can enter multiple IP ranges separated by line breaks. The IP range mask ranges from 8 to 32. The user's IDC IP range cannot conflict with the CIDR block of the VPC network.
Max. Bandwidth
100
Mbps
The maximum connection bandwidth is 200000 Mbit/s, and the remaining available bandwidth of the access point is 99999695 Mbit/s.
Enable BFD
Yes
No
The source IP of a BFD session is the IP address of the cloud border, and the destination IP is that of the user border.
Detection Interval
400
Please fill in the number in milliseconds
Enable Multicast
Yes
No
Connected Multicast Group



Disabling Multicast

1. On the Dedicated Tunnel page, click Tunnel Change in the Operation column to the right of the channel whose parameters need to be changed.



2. In the Tunnel Change dialog box, follow the on-screen prompts to disable multicast. Select No for Enable Multicast and click Submit.

Tunnel Change

Dedicated Tunnel ID

IP Protocol IPv4

Routing Mode Static Route

User IDC IP Range

You can enter multiple IP ranges separated by line breaks. The IP range mask ranges from 8 to 32. The user's IDC IP range cannot conflict with the CIDR block of the VPC network.

Max. Bandwidth 100 Mbps

The maximum connection bandwidth is 200000 Mbit/s, and the remaining available bandwidth of the access point is 99999695 Mbit/s.

Enable BFD (•) Yes ( ) No

The source IP of a BFD session is the IP address of the cloud border, and the destination IP is that of the user border.

Detection Interval 400

Please fill in the number in milliseconds

Enable Multicast ( ) Yes (•) No

Submit Cancel

Parameter Change Description

The dedicated tunnel supports the following parameter changes:

- BGP ASN
  Changing the BGP ASN will interrupt services.

- Bandwidth

- Changing the bandwidth does not interrupt the business because the system automatically overwrites the configuration.

  > Note:
  >
  > In the Shared Connection mode, the dedicated tunnel cannot request bandwidth changes. Bandwidth changes must be initiated by the Connection owner.

- BGP KEY
  Changing the BGP KEY will not interrupt the services because the system will automatically overwrite the configuration.

- User IDC IP Range
  Supports modification of user IDC IP range, and the system automatically distributes configurations.

- Health Check
  Supports users to customize the BFD dedicated tunnel detection feature to be turned on or off, and supports modifying the detection interval.
  After the channel change request is submitted, the system will complete the device configuration within a few minutes.

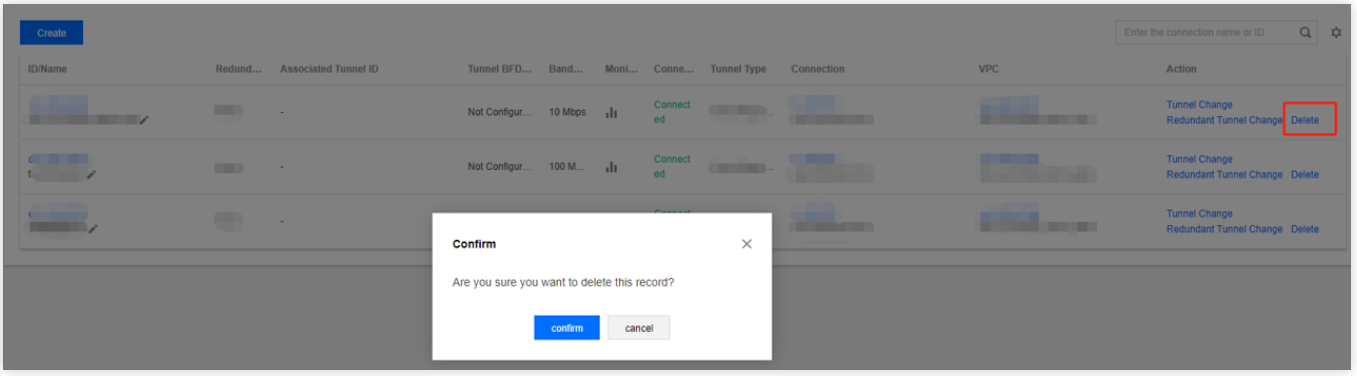
Delete a Channel

> Note:
>
> To protect the normal business of channel users, only the bandwidth of a shared channel can be changed and deletion of the shared channel is not allowed.

1. Log in to the Direct Connect console.

2. In the left navigation bar, click Dedicated Tunnel to enter the Dedicated Channel interface.

3. In the list, find the dedicated tunnel to be deleted, click Delete, and confirm.

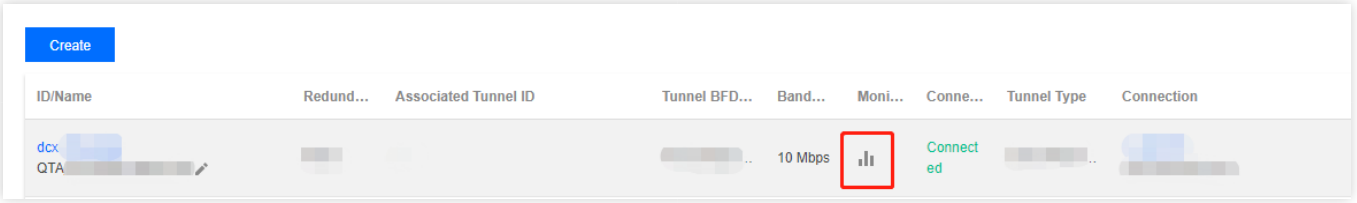


4. If the deletion of a DC tunnel is not completed, a new DC tunnel with the same VLAN ID cannot be created.

View Monitoring Information

DC tunnels support the query of monitoring information (network outbound bandwidth, network inbound bandwidth, outbound packet volume, and inbound packet volume). You can query the monitoring information of Connection through the cloud console. The directions are as follows:

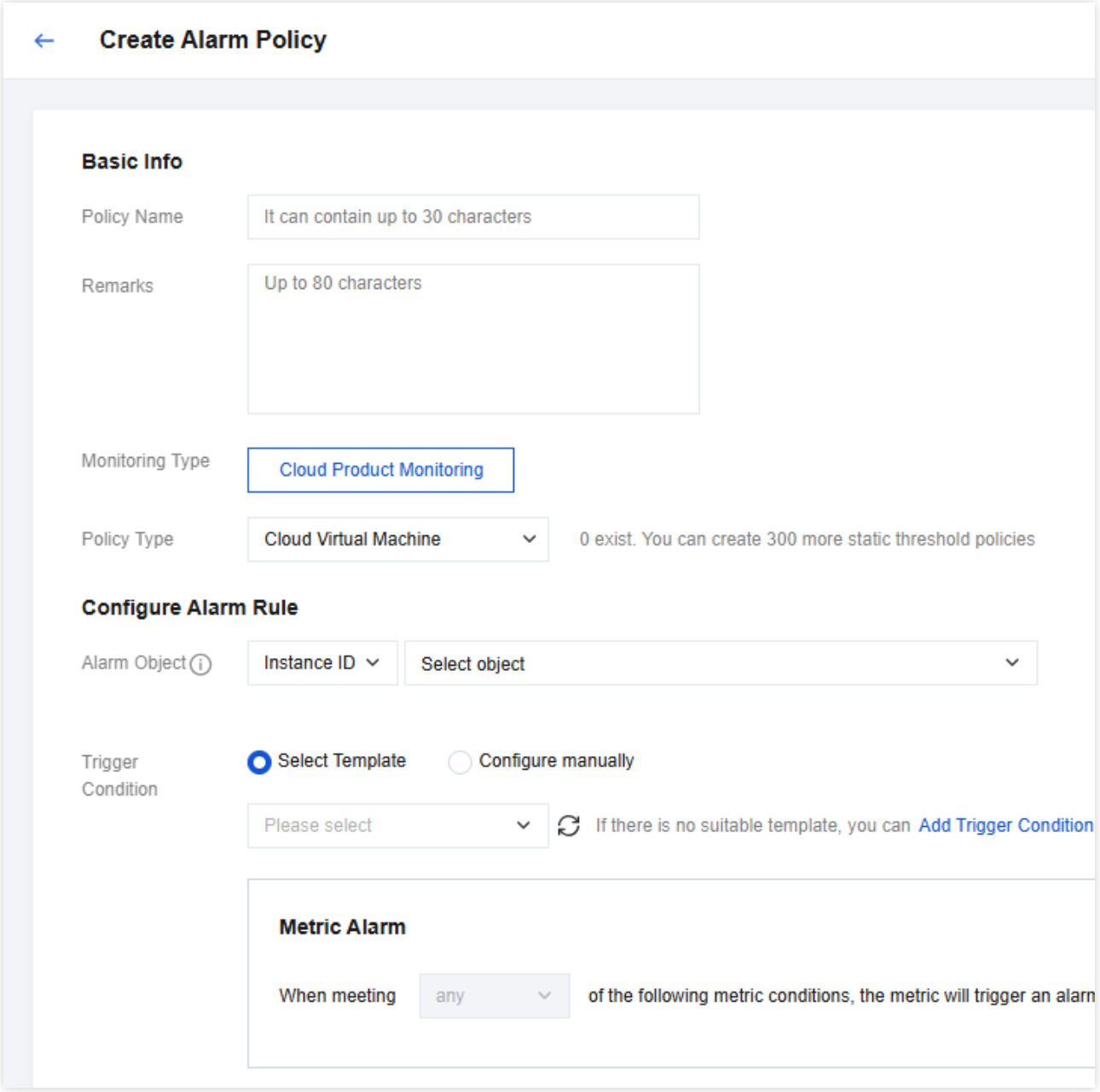
1. Log in to the Direct Connect console.
2. In the left navigation bar, click Dedicated Tunnel to enter the Dedicated Channel interface.
3. In the list, find the dedicated channel you want to view, and click the Monitoring icon.



Setting Alarms

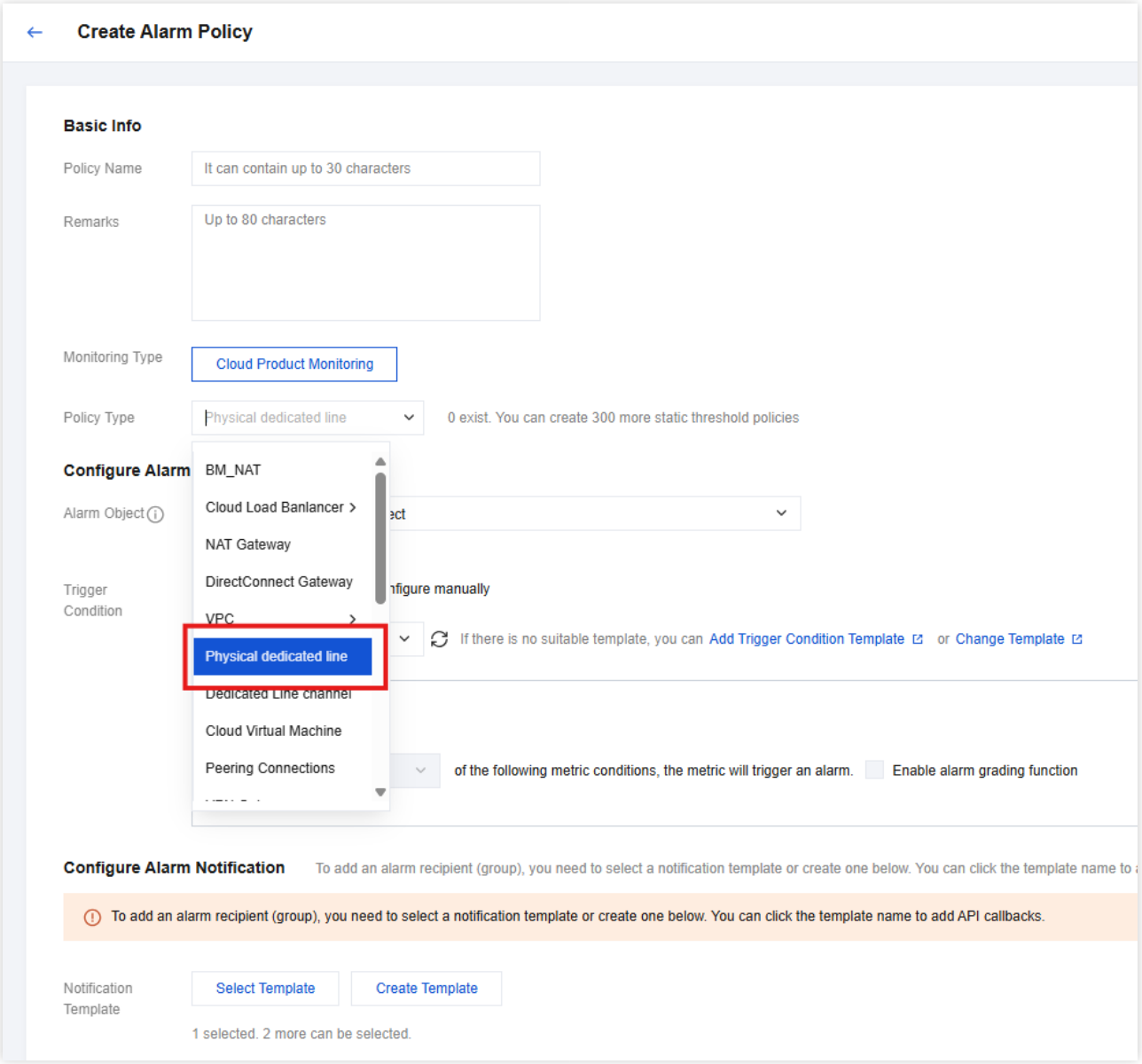
DC tunnels support configuration of monitoring alarms. The configuration steps are as follows:

1. Log in to the Cloud Monitor console.
2. Click Alarm Configuration > Alarm Policy in the left sidebar to open the management page.
3. Click Create.



4. Edit the alarm policy on the new page:
   - Enter the alarm policy name/ID.
   - Select Physical dedicated line for the policy type.
   - Alarm Object: Select the associated DC tunnel.
   - The alarm trigger conditions can be selected as: Outgoing bandwidth, Incoming bandwidth, and Bandwidth usage.

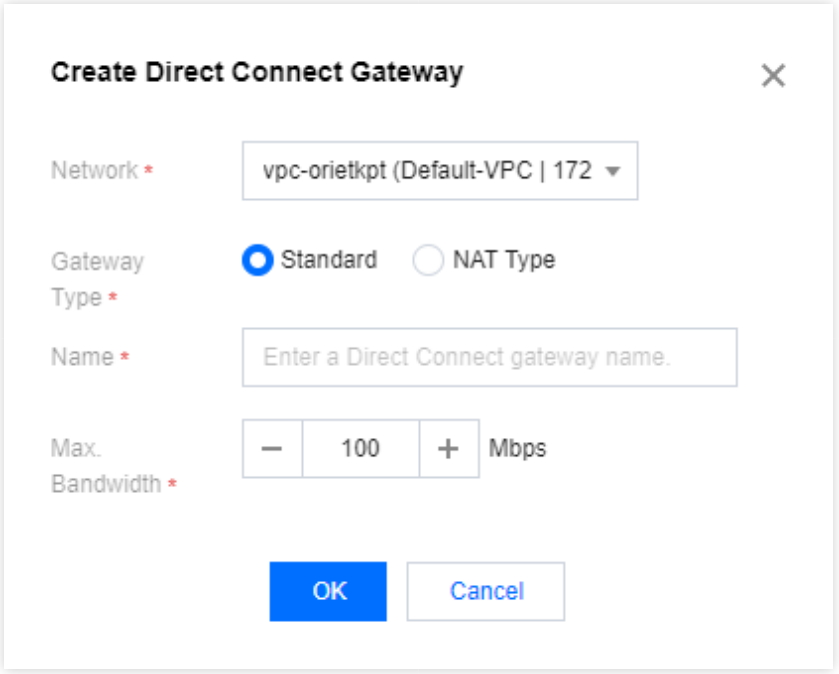
- Alarm Channel: Set the recipient of the alarm.
- API Callback: If you need to push the alarm information to a specified address, you can fill in this item. Cloud monitoring will push the alarm information to the address in time.

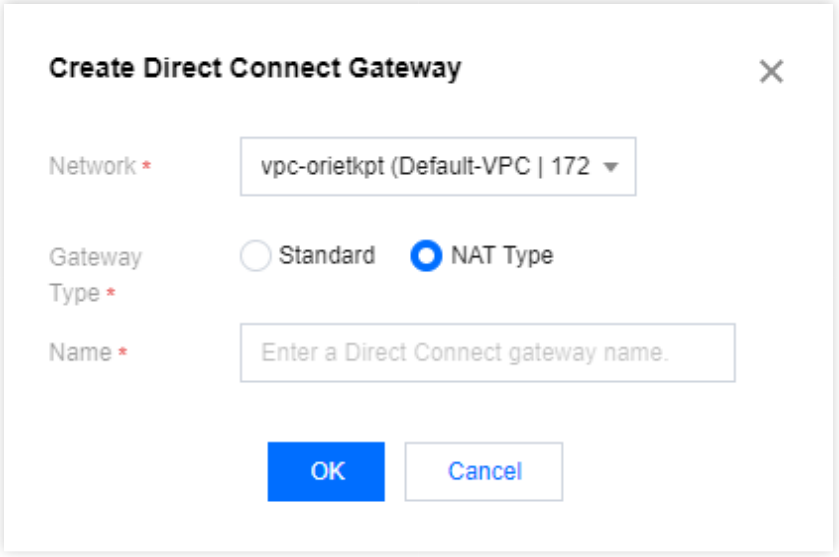


5. Set the alarm channel and click Finish to complete the configuration of the alarm policy.
   After the DC tunnel alarm configuration is completed, you can receive system alarms according to the settings of the alarm receiving group. For more monitoring operations, see Cloud Monitor.

Managing DC Gateway
Creating a Direct Connect Gateway

1. You can log in to the VPC console.
2. In the left sidebar, you can click Direct Connect Gateway to open the management page.
3. Choose Region and VPC, click Create.
4. In the pop-up box, you can fill in the relevant information.





- Network: You can select the created VPC instance.
- Name: The name of the DC gateway.

- Gateway Type: Standard or network address translation (NAT) type.
- Bandwidth Limit: Set the bandwidth limit of the gateway, with the default value being 100 Mbps.

5. After the information is filled in, click OK to complete the creation of the DC gateway.

Configuring Network Address Translation (NAT)

You can configure IP translation and IP port translation for a DC gateway with a NAT type. For details, refer to the following operations:

- Configuring IP Translation
- Configuring IP Port Translation
- Configuration Example

Configuring IP Translation

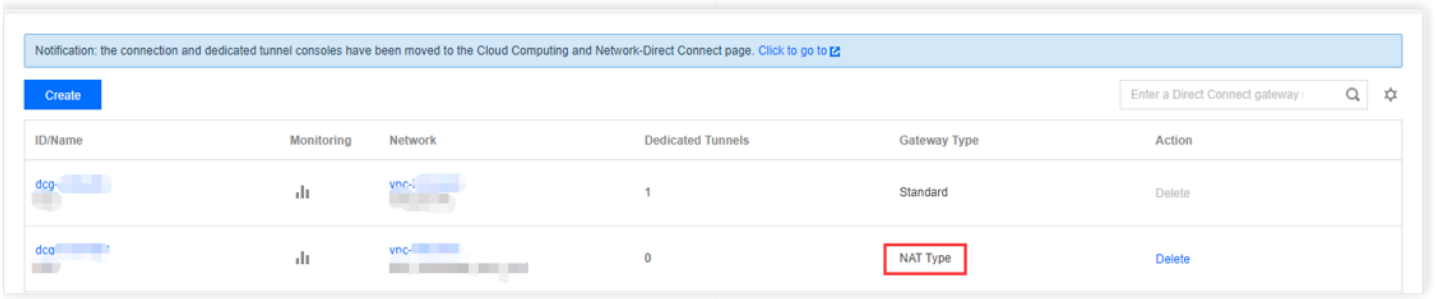
Configuring Local IP Translation

Rules and Restrictions

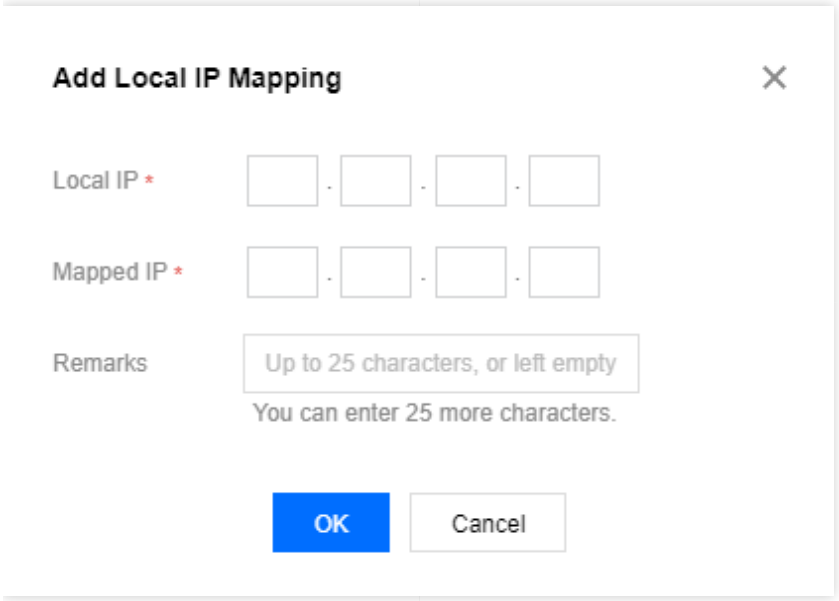
- The original IP must be within the CIDR range of the VPC.
- The mapped IP cannot be within the CIDR range of the VPC where the DC gateway is located.
- The original IP cannot be repeated, that is, one IP in a VPC can only be mapped to one IP.
- The mapped IP must be unique and cannot be repeated. That is, multiple VPC IP addresses cannot be mapped to the same IP.
- The original destination IP cannot be the broadcast address (255.255.255.255), class D addresses (224.0.0.0-239.255.255.255), and class E addresses (240.0.0.0-255.255.255.254).
- The local IP translation of the DC gateway supports mapping of a maximum of 100 IP addresses, and each IP mapping supports a maximum of 20 ACL rules (if you need to increase the quota, please submit a ticket application).

Directions

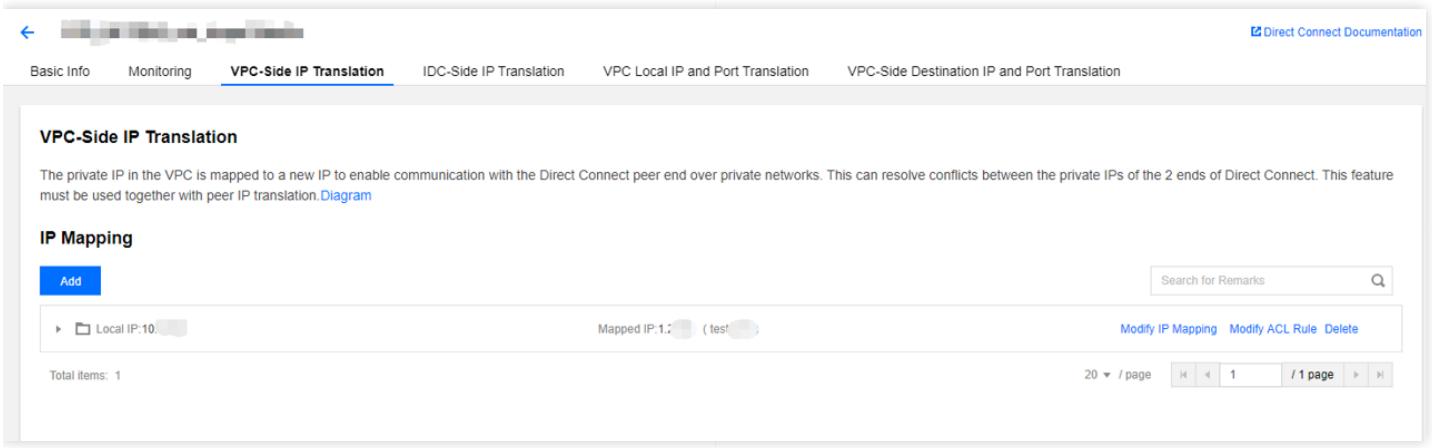
1. You can log in to the VPC console.
2. In the left sidebar, you can click Direct Connect Gateway to open the management page.
3. You can click the DC gateway ID whose gateway type is NAT to open the details page.



4. On the DC Gateway Details page, you can select the VPC IP Translation tab to configure the VPC local IP translation.
5. In the upper left corner of the IP mapping page, you can click Add to add a local IP mapping.
6. In the pop-up Add Local IP Mapping dialog box, you can enter the original IP, mapped IP and remarks.



7. You can click OK to complete the IP mapping settings.



8. (Optional) When you add a local IP mapping, an ACL rule is added by default to allow all inbound and outbound traffic to pass through, that is, the local IP translation is effective for all DC tunnels. You can edit the ACL rule of the local IP translation to change the applicable scope of the local IP translation.

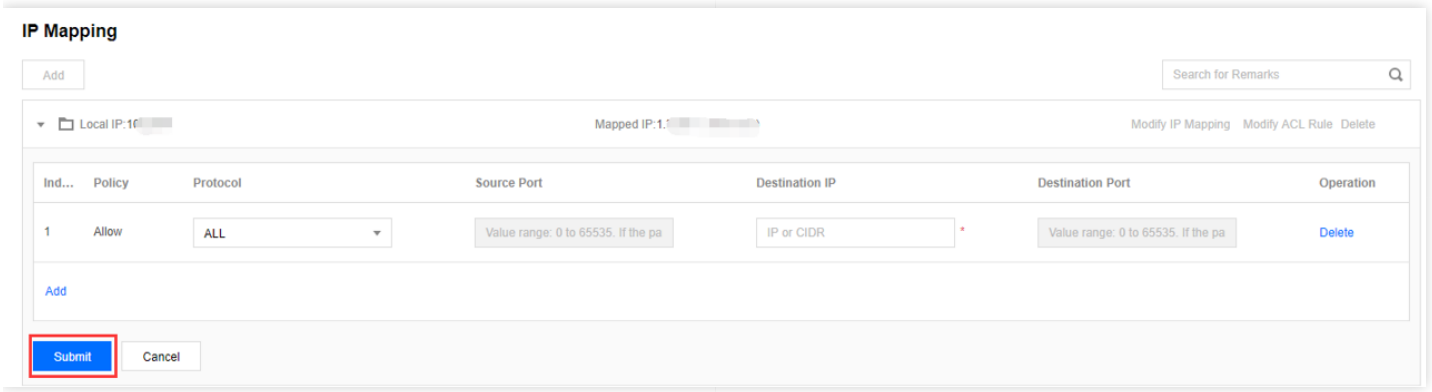
> Note:
>
> - When the DC gateway is configured with peer IP translation at the same time, the mapped IP of the peer IP translation rather than the original IP shall be filled as the destination IP of the local IP translation ACL rules.
> - The local IP translation ACL rule supports the configuration of protocol (TCP or UDP), source port, destination IP, and destination port. If port and IP are not filled in, it means ALL. When ALL is selected for protocol, ALL is selected for port and IP by default.

9. On the IP mapping page, you can click Edit ACL Rules on the right side of the IP mapping row to enter the ACL rule editing status.

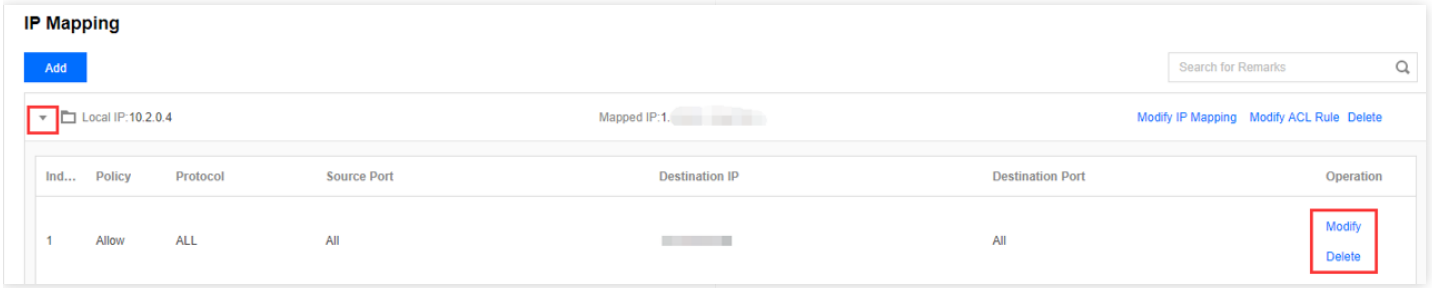


10. At the bottom of the existing ACL rules, you can click Add a New Row. After the ACL rules are added, you can click Submit.

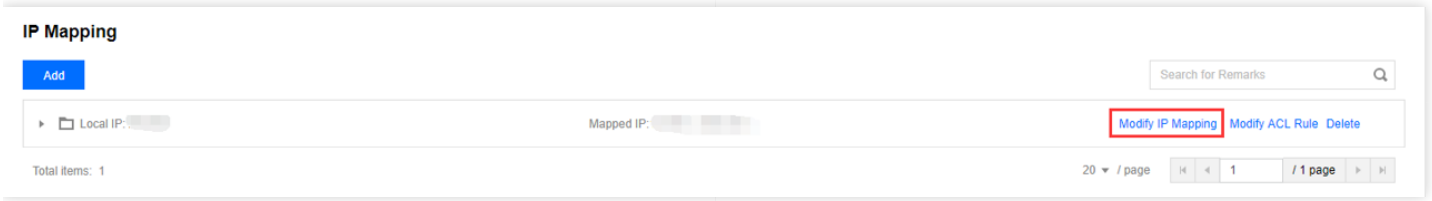
11. (Optional) When you edit ACL rules, you can modify or delete existing ACL rules. After the operation is completed, you can click Save.



12. (Optional) You can also click the Expand icon on the IP mapping page to expand the IP mapping rule, click Modify or Delete on the right side of the rule row, and confirm the operation after it is completed.



13. (Optional) If you need to modify the local IP mapping, you can click Modify IP Mapping on the right side of the IP mapping row on the IP mapping page to modify the original IP, mapped IP, and remarks of the local IP mapping. You can click OK to make the IP mapping take effect.



14. (Optional) If you need to delete the local IP mapping, you can click Delete on the right side of the row where the IP mapping is located on the IP mapping page and confirm the operation. After the IP mapping is deleted, the ACL rules under the IP mapping will be deleted.

Configuring Peer IP Translation

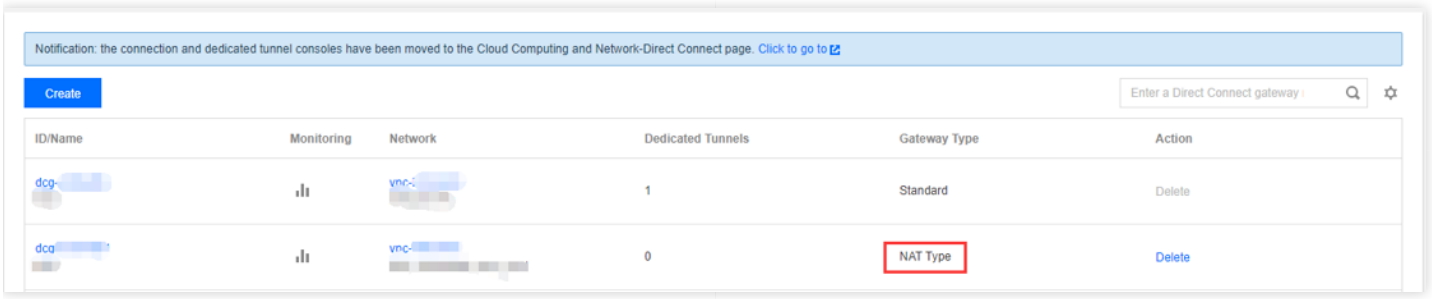
Rules and Restrictions

- The mapped IP cannot be within the CIDR range of the VPC where the DC gateway is located.

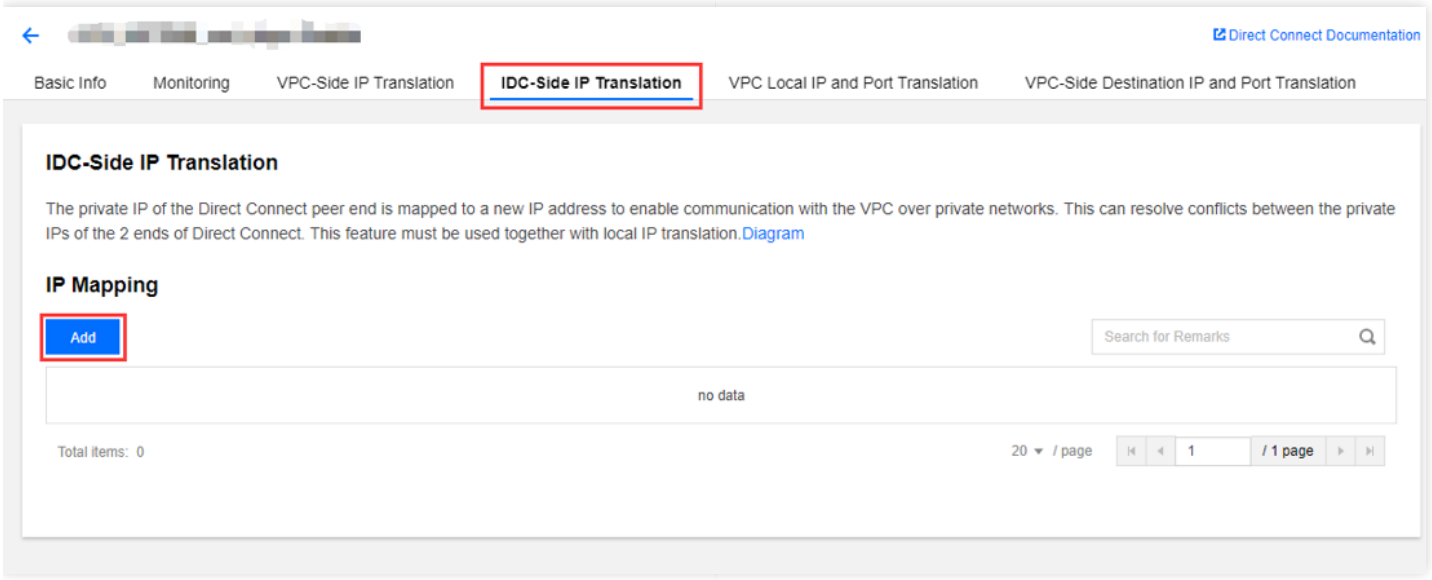
- The original IP cannot be repeated, that is, one peer IP of the DC can only be mapped to one IP.
- The mapped IP must be unique and cannot be repeated. That is, multiple DC peer IP addresses cannot be mapped to the same IP.
- The original destination IP cannot be the broadcast address (255.255.255.255), class D addresses (224.0.0.0-239.255.255.255), and class E addresses (240.0.0.0-255.255.255.254).
- The peer IP translation of the DC gateway supports mapping of a maximum of 100 IP addresses (if you need to increase the quota, please submit a ticket application).

Directions

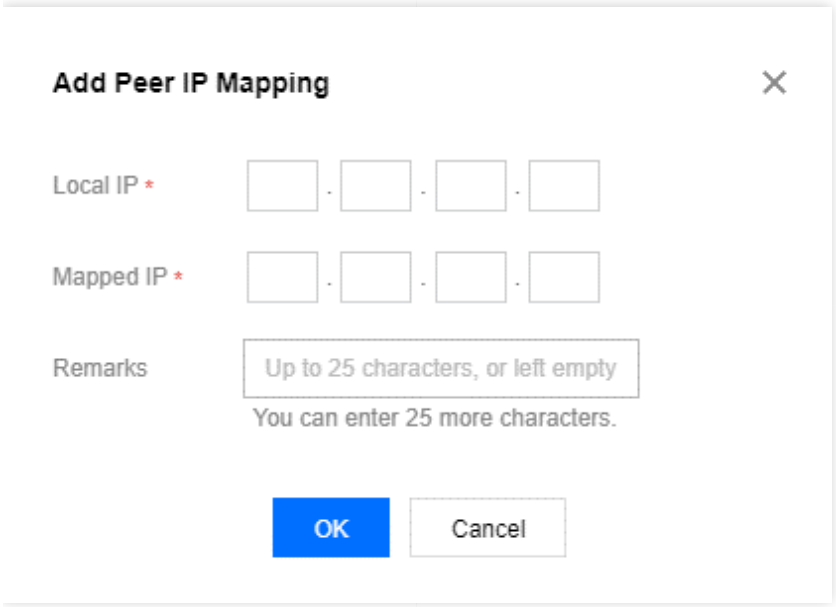
1. You can log in to the VPC console.
2. In the left sidebar, you can click Direct Connect Gateway to open the management page.
3. You can click the DC gateway ID whose gateway type is NAT to open the details page.



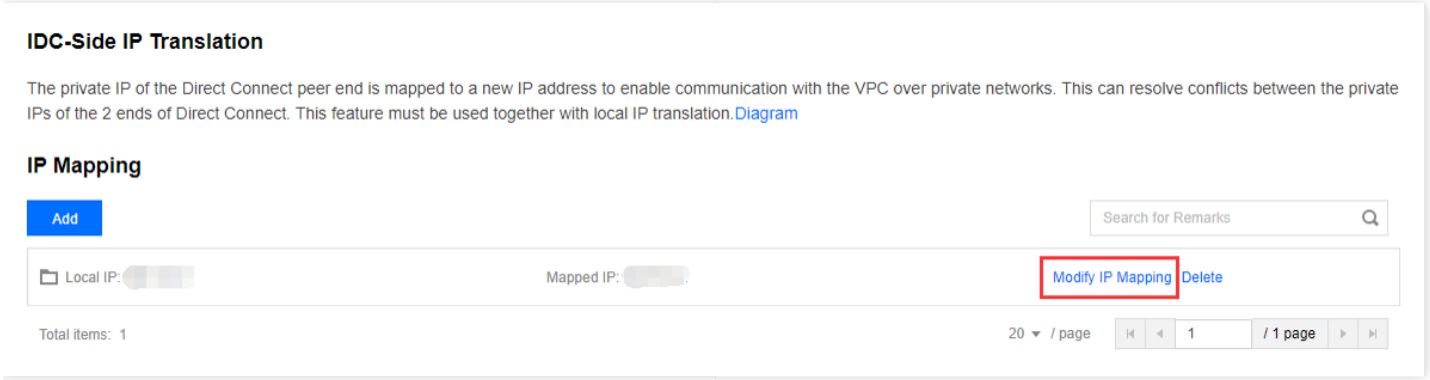
4. On the DC Gateway Details page, you can select the IDC IP Translation tab to configure the peer IP translation.
5. In the upper left corner of the IP mapping page, you can click Add to add a peer IP mapping.



6. In the pop-up Add Peer IP Mapping dialog box, you can enter the original IP, mapped IP and remarks, and click OK.



7. (Optional) If you need to modify the peer IP mapping, you can click Modify IP Mapping on the right side of the IP mapping row on the IP mapping page to modify the original IP, mapped IP, and remarks of the peer IP mapping. You can click OK to make the peer IP mapping take effect.



8. (Optional) If you need to delete the peer IP mapping, on the IP mapping page, you can click Delete on the right side of the row where the IP mapping is located and confirm the operation.

Configuring IP Port Translation

Configuring Local Source IP Port Translation

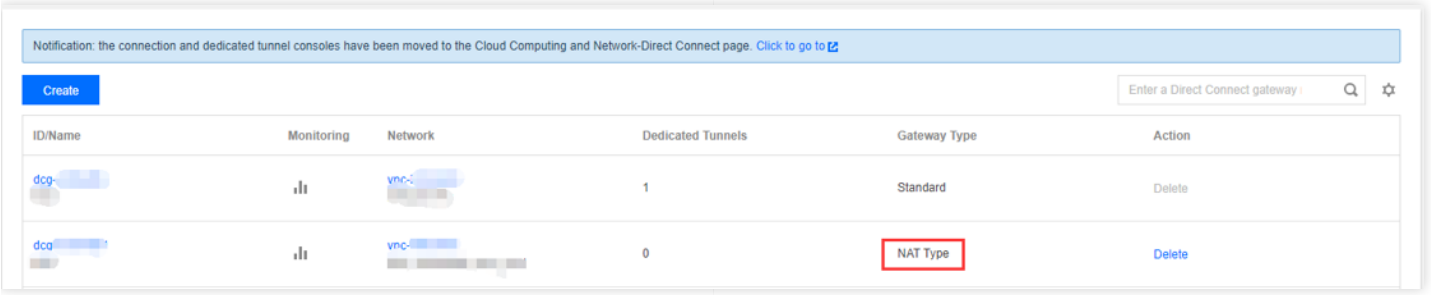
> Note:
>
> When local IP translation and local source IP port translation conflict, the local IP translation takes precedence.

Rules and Restrictions

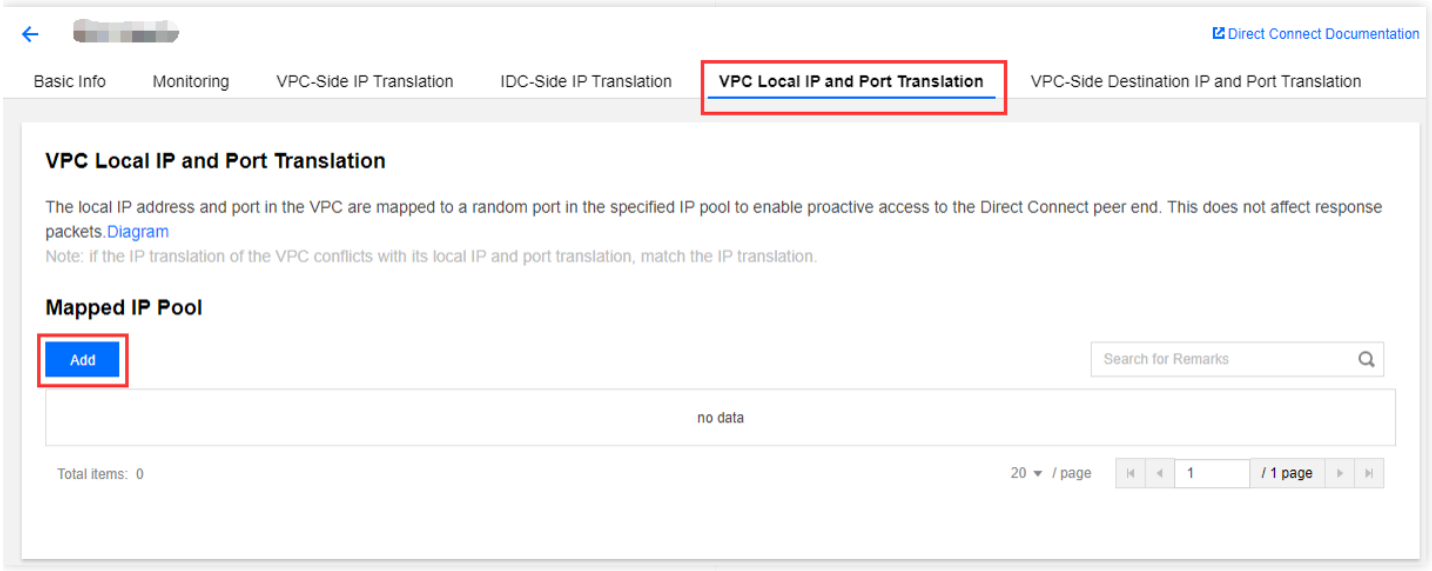
- The mapped IP pool cannot be within the CIDR range of the VPC where the DC gateway is located.
- ACL rules of multiple mapped IP pools cannot overlap, otherwise it causes network address translation conflicts.
- IP addresses in multiple mapped IP pools cannot overlap.
- The mapped IP pool only supports single IP or continuous IP addresses, and the /24 IP range of the continuous IP addresses must be consistent, that is, it supports 192.168.0.1-192.168.0.6 but does not support 192.168.0.1-192.168.1.2.
- The mapped IP pool does not include the broadcast address (255.255.255.255), class D addresses (224.0.0.0-239.255.255.255), and class E addresses (240.0.0.0-255.255.255.254).
- The local source IP port translation supports a maximum of 100 mapped IP pools, and each mapped IP pool supports a maximum of 20 ACL rules (if you need to increase the quota, please submit a ticket application).

Directions

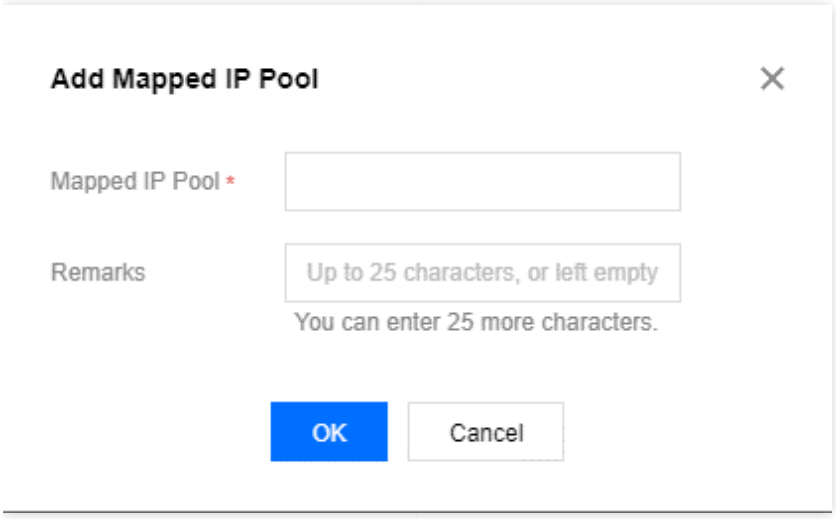
1. You can log in to the VPC console.
2. In the left sidebar, you can click Direct Connect Gateway to open the management page.
3. You can click the DC gateway ID whose gateway type is NAT to open the details page.



4. On the DC Gateway Details page, you can select the VPC Source IP Port Translation tab to configure the local source IP port translation.
5. In the upper left corner of the mapped IP pool page, you can click Add to add a mapped IP pool.



6. In the pop-up Add Mapped IP Pool dialog box, you can enter the mapped IP pool (it supports IP or IP range, and the IP range format is A - B) and remarks, and click OK.



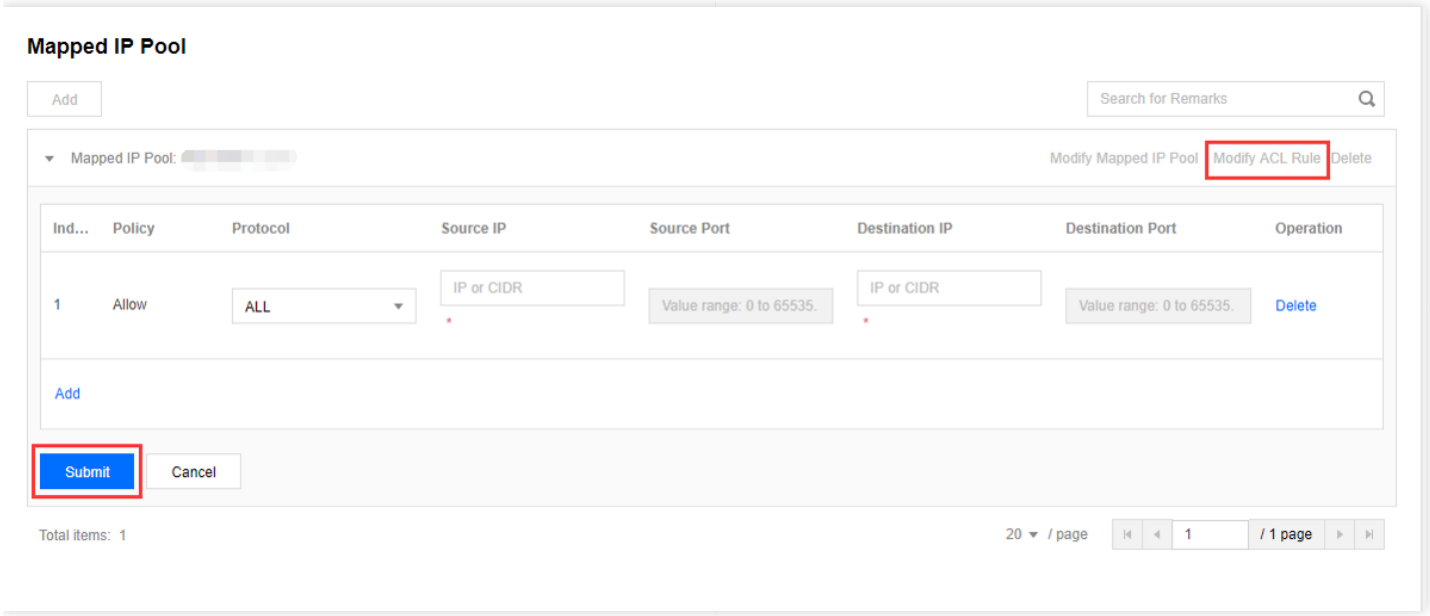
7. The ACL rules for newly added mapped IP pools deny all inbound and outbound traffic. You need to edit the ACL rules to implement network translation.

> Note:
>
> - When the DC gateway is configured with peer IP translation at the same time, the mapped IP of the peer IP translation rather than the original IP shall be filled as the destination IP of the local source IP port translation ACL rules.
> - The local source IP port translation ACL rule supports the configuration of protocol (TCP or UDP), source IP, source port, destination IP, and destination port.

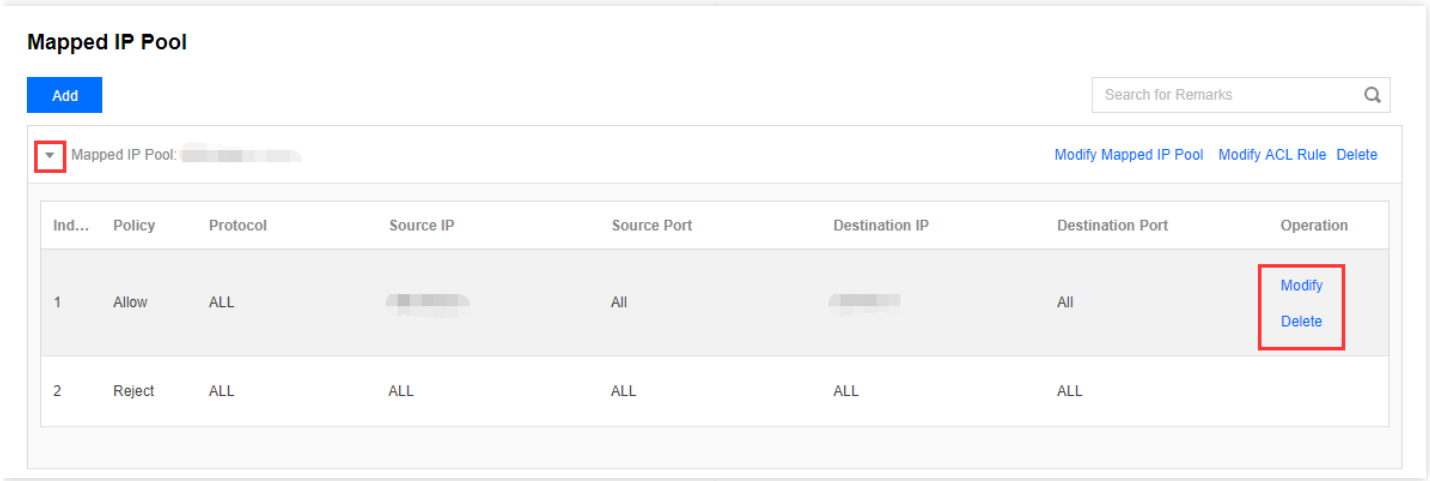
8. On the mapped IP pool page, you can click Edit ACL Rules on the right side of the mapped IP pool to

enter the ACL rule editing status.

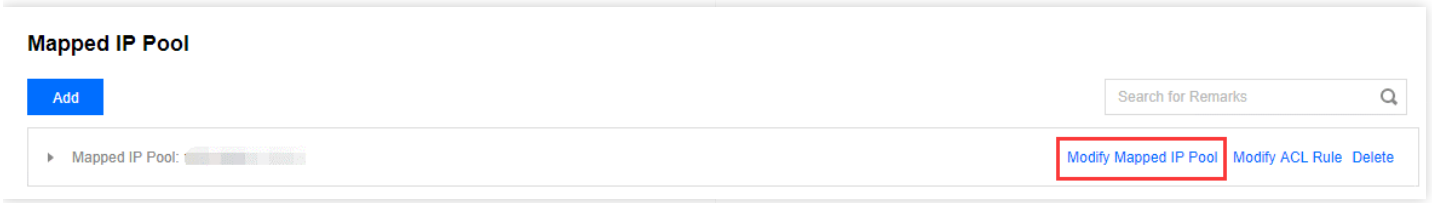
9. At the bottom of the existing ACL rules, you can click Add a New Row. After the ACL rules are added, you can click Submit.



10. (Optional) When you edit ACL rules, you can modify or delete existing ACL rules. After the operation is completed, you can click Save.
11. (Optional) You can also click the following Expand icon on the mapped IP pool page to expand the mapped IP pool rule, click Modify or Delete on the right side of the rule row, and confirm the operation after it is completed.



12. (Optional) If you need to modify the mapped IP pool, on the mapped IP pool page, you can click Modify mapped IP pool on the right side of the row where the mapped IP pool is located to modify the IP and remarks of the mapped IP pool.



13. (Optional) If you need to delete a mapped IP pool, you can click Delete on the right side of the mapped IP pool row on the mapped IP pool page, and confirm the operation to delete the mapped IP pool. After the mapped IP pool is deleted, the ACL rules associated with the mapped IP pool will be automatically deleted.

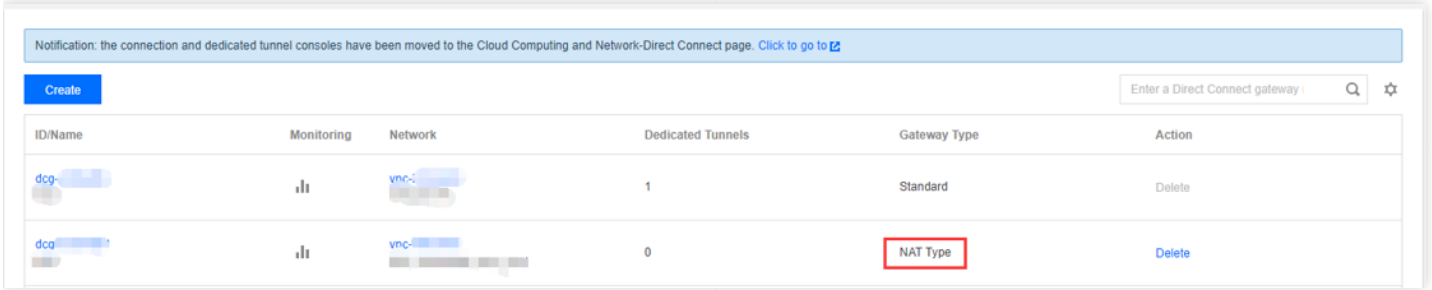
Configuring Local Destination IP Port Translation

Rules and Restrictions

- The original IP must be within the CIDR range of the VPC where the DC gateway is located.
- The same IP port in a VPC can be mapped to multiple different IP ports.
- The mapped IP port cannot be within the CIDR range of the VPC.
- The mapped IP ports cannot be repeated, that is, one IP port cannot be mapped to multiple VPC IP ports.
- The original IP addresses and the mapped IP addresses cannot be the broadcast address (255.255.255.255), class D addresses (224.0.0.0-239.255.255.255), and class E addresses (240.0.0.0-255.255.255.254).
- The local destination IP port translation supports the mapping of a maximum of 100 IP ports (if you need to increase the quota, submit a ticket application).

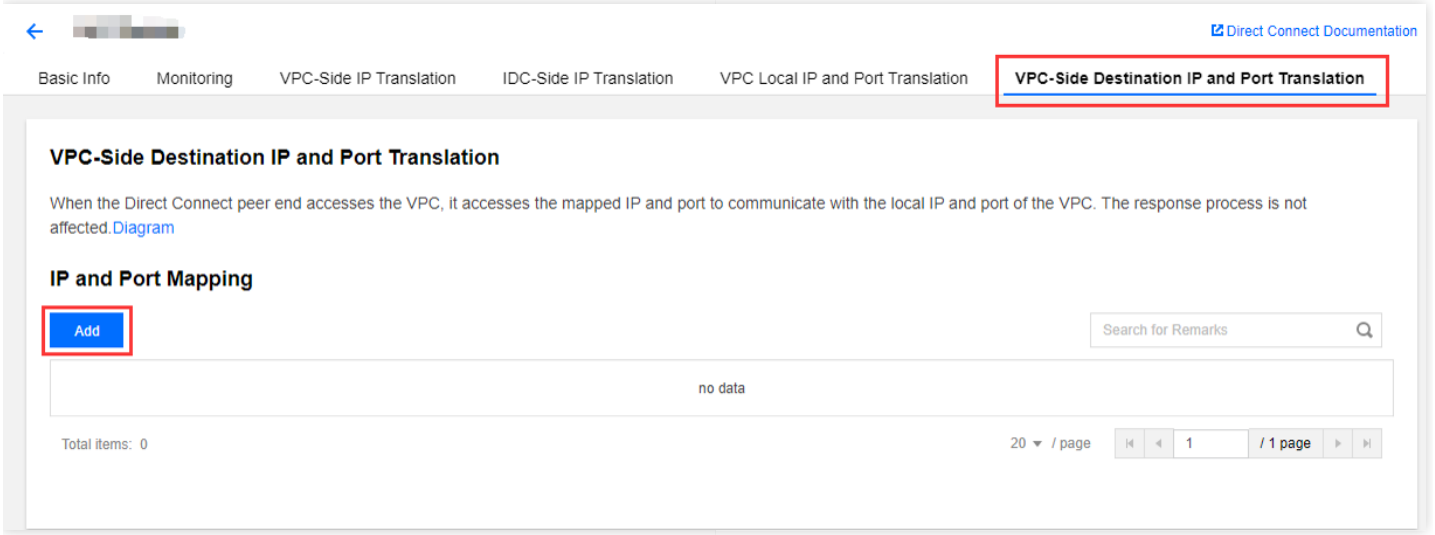
Directions

1. You can log in to the VPC console.
2. In the left sidebar, you can click Direct Connect Gateway to open the management page.
3. You can click the DC gateway ID whose gateway type is NAT to open the details page.

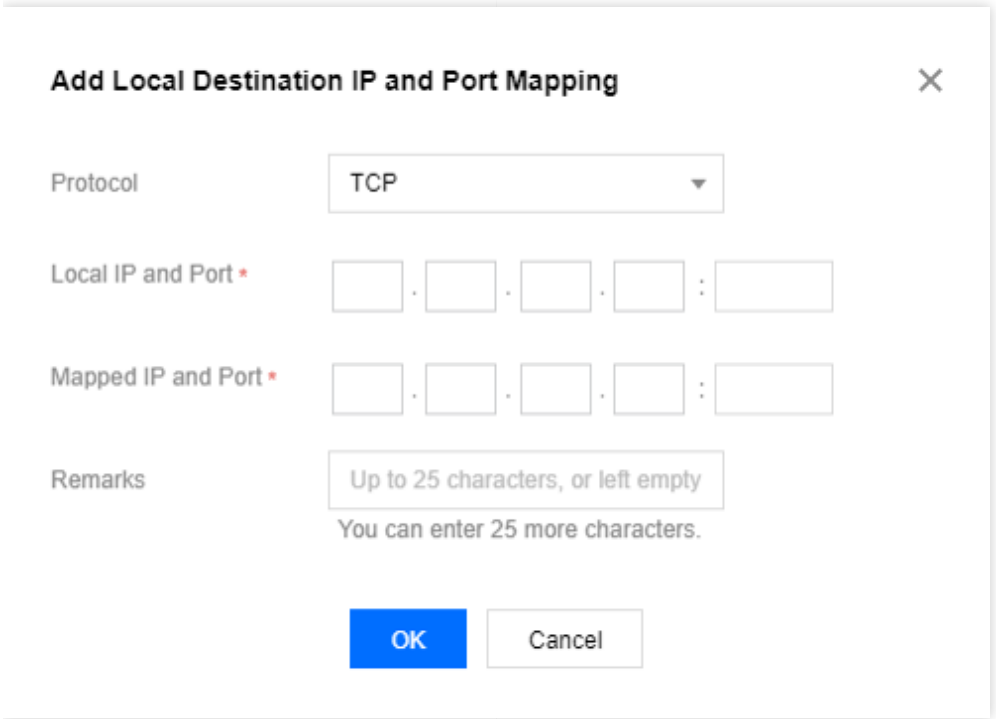


4. On the DC Gateway Details page, you can select the VPC Destination IP Port Translation tab to configure the local destination IP port translation.

5. In the upper left corner of the IP port mapping page, you can click Add to add a local destination IP port mapping.



6. In the pop-up window, you can select the protocol, enter the original IP port, mapped IP port and remarks, and click OK.



7. (Optional) If you need to modify the local destination IP port mapping, you can click Modify IP Port Mapping on the right side of the row where the IP port mapping is located on the IP port mapping page to modify the mapping relationship and remarks of the IP port mapping.

8. (Optional) If you need to delete the local destination IP port mapping, you can click Delete on the right side of the row where the IP port mapping is located on the IP port mapping page and confirm the operation to delete the mapping.

Configuration Example

Examples for Configuring Local IP Translation

If the IP A 192.168.0.3 in the VPC is used as the original IP, it is mapped to the IP B 10.100.0.3 through local IP translation, and:

- The original IP of IP A's active access network packet to the DC peer will be automatically modified to 10.100.0.3 .
- All network packets of 10.100.0.3 accessed by the DC peer will automatically be directed to the IP A 192.168.0.3 .

Examples for Configuring Peer IP Translation

If the IP D 10.0.0.3 of the DC peer is used as the original IP, it is mapped to the IP C 172.16.0.3 through peer IP translation, and:

- The IP D 10.0.0.3 actively accesses the original IP of the network packet of the VPC, which will be automatically modified to the IP C 172.16.0.3 .
- All network packets of the IP C 172.16.0.3 accessed by the VPC will automatically be directed to the DC peer IP D 10.0.0.3 .

Examples for Configuring Local Source IP Port Translation

The IP range of VPC C is 172.16.0.0/16 . Third-party banks A and B are connected via a DC, where Bank A's peer IP range is 10.0.0.0/28 , requesting the connecting IP range to be 192.168.0.0/28 ; Bank B's peer IP range is 10.1.0.0/28 , requesting the connecting IP rage to be 192.168.1.0/28 . Then you can configure two local source IP port translations A and B as follows:

Configuration	Local Source IP Port Translation A	Local Source IP Port Translation B
Mapped IP Pool	192.168.0.1 - 192.168.0.15	192.168.1.1 - 192.168.1.15
ACL Rules - Protocol	ALL	ALL
ACL Rules - Source IP Address	172.16.0.0/16	172.16.0.0/16
ACL Rules - Source Port	—	—

Configuration	Local Source IP Port Translation A	Local Source IP Port Translation B
ACL Rules - Destination IP Address	10.0.0.0/28	10.1.0.0/28
ACL Rules - Destination Port	—	—

After the configuration is completed, the network requests for active access to banks A and B in VPC C will be converted to random ports of the corresponding mapped IP pool according to the corresponding ACL rules to access the corresponding DC tunnels.

Examples for Configuring Local Destination IP Port Translation

The IP range of VPC C is 172.16.0.0/16 . If you only want to open some ports for active access by the DC peer, you can configure the two local destination IP port mappings A and B according to the following scheme:

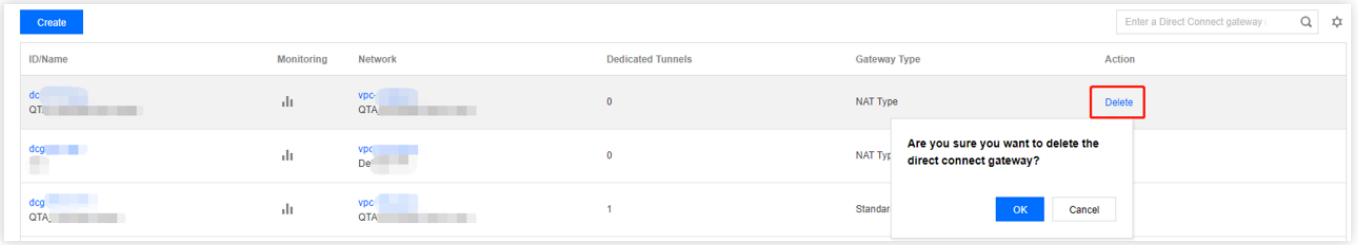
- Local Destination IP Port Mapping A: original IP port 172.16.0.1:80 , and mapped IP port 10.0.0.1:80 .
- Local Destination IP Port Mapping B: original IP port 172.16.0.0:8080 , and mapped IP port 10.0.0.1:8080 .

  After the configuration is completed, the DC peer can actively access ports 10.0.0.1:80 and 10.0.0.1:8080 , to achieve active access to the two ports 172.16.0.1:80 and 172.16.0.0:8080 in the VPC.

Deleting a DC Gateway

If you no longer need a DC gateway, you can delete it. Deleting a DC gateway will also delete the DC tunnel connected to it. Make sure that deleting the DC gateway does not affect your normal service.

1. You can log in to the cloud console and select Cloud Products > Cloud Computing & Networking > Virtual Private Cloud to enter the VPC console.
2. Click Direct Connect Gateway in the left sidebar to open the management page.
   Select the DC gateway to be deleted and click Delete in the action bar.

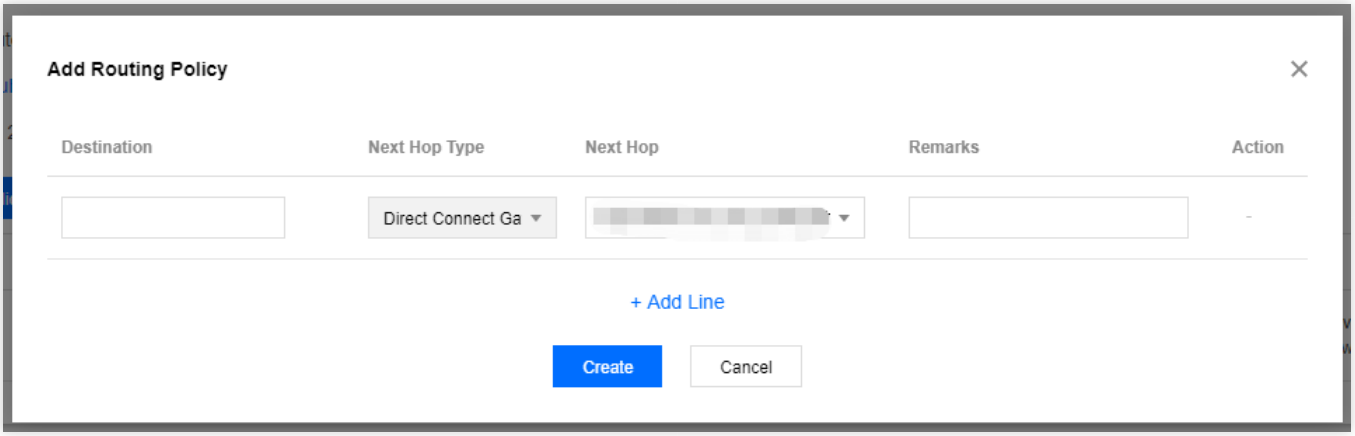


3. Click OK.

Configuring a Route Table

After a DC gateway is created and the construction of a DC tunnel is completed, you can configure the route table of the VPC in the console to direct the traffic that needs to go to the DC to the DC gateway.

1. You can log in to the VPC console.
2. In the directory on the left, you can click Route Table to open the management page.
3. You can click the route table ID that needs to be associated with the DC gateway to open the details page.
4. You can cllick Add Routing Policy.
5. You can enter the destination IP range, select DC Gateway for the next hop type, and select the gateway name for the next hop.



6. Click OK.
   After the above steps is completed, you can direct specific destination traffic to the DC gateway and associate it with your local data center.

FAQs
Basic Category

What is DC?

DC provides a fast way to connect the cloud platform and the local data center. Users can apply for a connection to connect cloud computing resources in multiple regions with your local data center at one time, achieving flexible and reliable hybrid cloud deployment.

What are the Components of DC?

DC consists of connections, DC tunnels, and DC gateways. For details, see Product Overview.

Can the DC be used across accounts?

Connections can be used across accounts. For details, see Sharing Connections.

Can the parameters of a connection be changed after the application is submitted?

After a connection application is submitted, the following parameters can be changed before the cloud platform DC delivery engineer pushes it for backend review: operator, connect point, port type, DC type, etc. If you no longer want this application information, the DC delivery engineer can reject the request and you can reapply for a new one.

Which operators can connect the DC point?

Most connection access points are deployed in the IDCs of neutral IDC operators and can support DC from any DC provider.
For details, log in to the DC console, click Create to create a connection, and select a different operator to display the connection access points that support the operator's connection.

Can a connection support access to cloud resources in multiple regions?

Support. It supports the one-point connection to cloud resources in all regions.

The DC point device supports the 802.1Q VLAN encapsulation technology. The connection supports multiple VLANs in Trunk mode. Different DC tunnels are created through different VLANs to access VPC resources on the cloud in multiple regions.

Why is the status of the connection always Application in Progress?

After you submit your application for a connection, the DC delivery engineer will contact you as soon as possible to confirm your requirements and initiate the corresponding approval and construction process. If the project is urgent, you can contact your DC delivery engineer or submit a ticket to consult for the latest developments.

How long does it take for a connection to take effect after being approved?

1 month. If you do not pay for DC construction within one month, the connect environment has changed and the resources have been recycled. If you still need DC services, you need to reapply for review.

What is the role of connection bandwidth?

The bandwidth of the connection is only for record-keeping and has nothing to do with the speed limit. When the rate of your connection changes, you can contact your DC delivery engineer or submit a ticket to change the bandwidth value of the console for you.

What is the carrier circuit number of a connection?

It is the unique identifier of the circuit provided by the DC provider. Please ensure its accuracy. Subsequent line maintenance relies on the circuit number and the DC provider to locate the line information.

Can the address of connection be changed?

- If your local data center address changes, you need to submit the change request to the DC provider.
- The connect point on the cloud platform side needs to be changed. Please consult your cloud platform DC delivery engineer.

Why is the DC tunnel status always Configuring or Modifying?

Under normal circumstances, it takes several minutes to create or modify the configuration of a DC tunnel. If the process is not completed within 10 minutes, it means that there is a problem with the configuration process. The backend engineer will handle it as soon as possible. You can also obtain the latest developments through your DC delivery engineer.

What are the restrictions on using DC?

DC has resource restrictions and connect restrictions. For details, see Usage Restrictions.

Is there any limit on the amount of data transmitted when using DC?

There is no limit, and users can transfer any amount of data, up to the speed of the DC bandwidth selected by the user.
For other usage restrictions, see Usage Restrictions.

How to configure alarms for a DC?

You can open the console - Cloud Monitor, click New Policy, select DC - Connection or DC - DC Tunnel product as the policy type, and then configure the threshold alarm policy.

What is the difference between DC and IPSec VPN connection?

- VPN connections use a public network and the IPsec protocol to establish an encrypted network connection between your data center and the VPC. VPN gateways can be purchased, validated, and

configured in a few minutes. However, VPN connections may be interrupted by Internet jitter, congestion, and other public network quality issues. When the user's service does not require high network connection quality, it is a fast deployment and cost-effective option.

- DC provides a dedicated network connection solution for you. It takes a long time to build, but can provide high-quality and highly reliable network connection services. When the user's service requires high network quality and security, DC can be selected for deployment.
  For details, see Product Overview.

Technology Category

Does DC support the 802.1Q VLAN encapsulation technology?

Support.

How do DC users use the DC of DC providers?

First, the DC provider needs to establish NNI interconnection with the DC point of the cloud platform. The DC provider needs to go to the DC console and apply for a connection, and the DC delivery engineer will assist in completing the line connection and making NNI interconnection. During this process, there will be a connection ID under the DC provider's cloud platform account, in the format of dc-******* . After it is connected, users use your DC in a shared connection mode:

1. The DC provider needs to prepare its own cloud account ID and connection ID (dc-*******), as well as non-conflicting VLAN IDs and even interconnection IP information, and provide them to its users.
2. The DC user of the DC provider directly opens the cloud platform DC tunnel console , click Create+, select Shared Connection in Connection, enter the DC provider's account ID, connection ID, and VLAN ID in Advanced Configuration, and click Submit.
3. The DC providers need to open a DC tunnel console in the cloud platform account, click Accept in the far right column of the DC tunnel applied for by the user.
4. The cloud platform will automatically create a tunnel within a few minutes.

How can I choose the connection port type?

Confirm with your DC provider. The optical port module supports long-distance/short-distance connections. Confirm the port type again before you submit a connection application to the cloud platform.

Does it support multi-line CLB or active-standby relationship?

Support. DC Tunnel:

- BGP Routing:
- CLB (Active-active): Regardless of whether multiple lines are connected to the same DC point, as long as the local data center under the cloud publishes equal-cost routes to the same DC gateway on the cloud, the traffic sent from the DC gateway on the cloud to the local data center under the cloud will be CLB;
- Primary/Replica (Active-standby): Regardless of whether multiple lines are connected to the same DC point, users need to press multiple AS-PATHs for the replica connects on their own CPE devices to achieve the primary/replica relationship by making the AS-PATH lengths between multiple DC inconsistent.
- Static Routing:

- CLB (Active-active): Regardless of whether multiple lines are connected to the same DC point, as long as equal-cost routes are configured on the DC tunnel configuration of multiple lines, the traffic sent from the DC gateway on the cloud to the local data center under the cloud will be CLB;
- Primary/Replica (Active-standby): It supports the creation of redundant connections and active-standby tunnels under the same connect point.

Where is the interconnect IP actually configured?

The interconnect IP is configured at both ends of connection: the connect device of the DC point and the user's CPE device.

How does the cloud platform isolate different tenants to ensure data security?

The cloud platform private network provides users with an Internet network that uses MPLS_VPN technology. The DC point is equivalent to the PE node of MPLS. The user's DCion to cloud services supports VPC-level VRF technology isolation to ensure the user's data security.

What means are used to trigger the switching of redundant lines?

- Static routes are converged when the bidirectional BFD is configured.
- BGP routing triggers the switching through BGP's own convergence mechanism or when BFD is configured. For the configuration of BFD, you need to submit your request to the DC delivery engineer for backend configuration.
  IPSLA cannot be configured. Reason: The connect point device has many connect lines. Configuring IPSLA will consume the performance of the connect device and may affect the normal use of all customers of the connect point.

Does the cloud platform support link aggregation control protocol (LACP)?

Not support.

Why do DC stress test results not meet expectations?

Reconfirm the created DC bandwidth.
Test the interconnect IP ping to see if there is packet loss. If there is severe packet loss, contact the cloud after-sales team to troubleshoot together.
You can check whether the local DC router is in full duplex mode.
You can use tools such as iPerf to try to initiate multiple processes on multiple clients and cloud servers to test whether the traffic meets expectations and eliminate application problems. If there is no progress in the troubleshooting, contact the cloud after-sales team for assistance.

What should I do if the DC to the cloud platform is interrupted?

- Confirm the interrupt mode:
  The interconnect IP addresses cannot be pinged each other, and the MAC address of the other end

cannot be received. If the DC has exception, the cloud platform after-sales service team receives an automatic alarm message.

- Connect Interruption confirmed:
- If the DC owner is a cloud platform, report the problem to the cloud platform after-sales team as soon as possible. Generally, after an automatic alarm is received, the DC fault after-sales team reports the problem to the operator immediately.
- If the DC owner is a user, the customer needs to report the problem to the operator. If cooperation from the cloud platform is required, contact the after-sales team.

What should I do if the specific IP range of the DC cannot be pinged?

- Confirm whether the network is a newly enabled IP range. If yes, the cloud needs to configure the route.
- You can check whether the route table on the cloud has an inaccessible IP range pointing to the DC gateway and confirm whether the client machine has a route pointing to the DC.
- You can confirm whether the cloud has associated security groups, network ACLs and other security features, and confirm whether the client machine has set security features such as iptables.
- If no exceptions are found during the troubleshooting, provide the troubleshooting information to the after-sales team for follow-up.

What information do I need to provide when I contact customer service to solve a problem?

If you cannot solve the problem yourself, contact us and provide the following information to help improve the troubleshooting efficiency:

- Description of the problem and whether it can be reproduced.
- The source/destination IP pair in question.
- Regional information for DC.
- DC gateway ID.
- Ping/traceroute screenshot during failure.
- Information about iptables, NAT, etc.
- Topology diagram is connected.

API Documentation
Dedicated Line Access(dc)
version(2018-04-10)
API overview

API version

V3

DC-related APIs

Interface name	Interface function
ApproveDirectConnectTunnel	ApproveDirectConnectTunnel
CreateDirectConnect	CreateDirectConnect
CreateDirectConnectTunnel	CreateDirectConnectTunnel
DeleteDirectConnect	DeleteDirectConnect
DeleteDirectConnectTunnel	DeleteDirectConnectTunnel
DescribeAccessPoints	DescribeAccessPoints
DescribeCloudBgpAsn	DescribeCloudBgpAsn
DescribeDirectConnectPortPrice	DescribeDirectConnectPortPrice
DescribeDirectConnectTunnels	DescribeDirectConnectTunnels
DescribeDirectConnects	DescribeDirectConnects
DescribeIsp	DescribeIsp
ModifyDirectConnectAttribute	ModifyDirectConnectAttribute
ModifyDirectConnectTunnelAttribute	ModifyDirectConnectTunnelAttribute
UpdateVifAssociated	UpdateVifAssociated

CallingMethod signaturev1

Converge Cloud authenticates each access request, i.e. each request needs to include authentication information (Signature) in the common parameters to verify the identity of the requester.
The Signature is generated by the security credentials which include SecretId and SecretKey. If you don't have the security credentials yet, go to the API Key page to apply for them; otherwise, you cannot invoke the API.

1. Applying for Security Credentials

Before using the API for the first time, go to the API Key page to apply for security credentials.
Security credentials consist of SecretId and SecretKey:

- SecretId is used to identify the API requester.
- SecretKey is used to encrypt the signature string and verify it on the server.
- You must keep your security credentials private and avoid disclosure.

You can apply for the security credentials through the following steps:

1. Log in to the Converge Cloud Console.
2. Go to the Cloud API Key page.
3. On the API Key Management page, click Create Key to create a SecretId/SecretKey pair.

Note: Each account can have up to two pairs of SecretId/SecretKey.

2. Generating a Signature

With the SecretId and SecretKey, a signature can be generated. The following describes how to generate a signature:

Assume that the SecretId and SecretKey are:

- SecretId: AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE
- SecretKey: Gu5t9xGARNpq86cd98joQYCN3EXAMPLE

Note: This is just an example. For actual operations, please use your own SecretId and SecretKey.

Take the Cloud Virtual Machine's request to view the instance list (DescribeInstances) as an example. When

you invoke this API, the request parameters may be as follows:

Parameter name	Description	Parameter value
Action	Method name	DescribeInstances
SecretId	Key ID	AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE
Timestamp	Current timestamp	1465185768
Nonce	Random positive integer	11886
Region	Region where the instance is located	luzon
InstanceIds.0	ID of the instance to query	ins-09dx96dg
Offset	Offset	0
Limit	Allowed maximum output	20
Version	API version number	2017-03-12

2.1. Sorting Parameters

First, sort all the request parameters in an ascending lexicographical order (ASCII code) by their names. Notes: (1) Parameters are sorted by their names instead of their values; (2) The parameters are sorted based on ASCII code, not in an alphabetical order or by values. For example, InstanceIds.2 should be arranged after InstanceIds.12. You can complete the sorting process using a sorting function in a programming language, such as the ksort function in PHP. The parameters in the example are sorted as follows:

```
{
    'Action' : 'DescribeInstances',
    'InstanceIds.0' : 'ins-09dx96dg',
    'Limit' : 20,
    'Nonce' : 11886,
    'Offset' : 0,
    'Region' : 'luzon',
    'SecretId' : 'AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE',
    'Timestamp' : 1465185768,
    'Version': '2017-03-12',
}
```

When developing in another programming language, you can sort these sample parameters and it will work as long as you obtain the same results.

2.2. Concatenating a Request String

This step generates a request string.
Format the request parameters sorted in the previous step into the form of "parameter name"="parameter value". For example, for the Action parameter, its parameter name is "Action" and its parameter value is "DescribeInstances", so it will become Action=DescribeInstances after formatted.
Note: The "parameter value" is the original value but not the value after URL encoding.

Then, concatenate the formatted parameters with "&". The resulting request string is as follows:

```
Action=DescribeInstances&InstanceIds.0=ins-09dx96dg&Limit=20&Nonce=11886&Offset=0&Region=luzon&SecretId=AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE&Timestamp=1465185768&Version=2017-03-12
```

2.3. Concatenating the Signature Original String

This step generates a signature original string.
The signature original string consists of the following parameters:

1. HTTP method: POST and GET modes are supported, and GET is used here for the request. Please note that the method name should be in all capital letters.
2. Request host: the domain name of the request to view the list of instances (DescribeInstances) is cvm.convergecloud.com. The actual request domain name varies by the module to which the API belongs. For more information, see the instructions of the specific API.
3. Request path: The request path in the current version of Cloud API is fixed to / .
4. Request string: the request string generated in the previous step.

The concatenation rule of the signature original string is: Request method + request host + request path + ? + request string

The concatenation result of the example is:

```
GETcvm.convergecloud.com/?Action=DescribeInstances&InstanceIds.0=ins-09dx96dg&Limit=20&Nonce=11886&Offset=0&Region=luzon&SecretId=AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE&Timestamp=1465185768&Version=2017-03-12
```

2.4. Generating a Signature String

This step generates a signature string.
First, use the HMAC-SHA1 algorithm to sign thesignature original stringobtained in the previous step, and then encode the generated signature using Base64 to obtain the final signature.

The specific code is as follows with the PHP language being used as an example:

```
$secretKey = 'Gu5t9xGARNpq86cd98joQYCN3EXAMPLE';
$srcStr = 'GETcvm.convergecloud.com/?Action=DescribeInstances&InstanceIds.0=ins-09dx96dg&Limit
=20&Nonce=11886&Offset=0&Region=luzon&SecretId=AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPL
E&Timestamp=1465185768&Version=2017-03-12';
$signStr = base64_encode(hash_hmac('sha1', $srcStr, $secretKey, true));
echo $signStr;
```

The final signature is:

```
EliP9YW3pW28FpsEdkXt/+WcGeI=
```

When developing in another programming language, you can sign and verify the original in the example above and it works as long as you get the same results.

3. Encoding a Signature String

The generated signature string cannot be directly used as a request parameter and must be URL encoded.

For example, if the signature string generated in the previous step is EliP9YW3pW28FpsEdkXt/+WcGeI= , the final signature string request parameter (Signature) is EliP9YW3pW28FpsEdkXt%2f%2bWcGeI%3d, which will be used to generate the final request URL.

**Note: If your request method is GET, or the request method is POST and the Content-Type is application/x-www-form-urlencoded, then all the request parameter values need to be URL encoded (except the parameter key and the symbol of =) when sending the request. Non-ASCII characters need to be encoded with UTF-8 before URL encoding. **

Note: The network libraries of some programming languages automatically URL encode all parameters, in which case there is no need to URL encode the signature string; otherwise, two rounds of URL encoding will cause the signature to fail.

Note: Other parameter values also need to be encoded using RFC 3986. Use %XY in percent-encoding for special characters such as Chinese characters, where "X" and "Y" are hexadecimal characters (0-9 and uppercase A-F), and using lowercase will cause an error.

4. Signature Failure

The following situational error codes for signature failure may occur. Please resolve the errors accordingly.

Error code	Error description
AuthFailure.SignatureExpire	The signature is expired

Error code	Error description
AuthFailure.SecretIdNotFound	The key does not exist
AuthFailure.SignatureFailure	Signature error
AuthFailure.TokenFailure	Token error
AuthFailure.InvalidSecretId	Invalid key (not a Cloud API key type)

5. Signature Demo

When calling API 3.0, you are recommended to use the corresponding Converge Cloud SDK 3.0, Swhich encapsulates the signature process, enabling you to focus on only the specific APIs provided by the product when developing. See SDK Center for more information. Currently, the following programming languages are supported:

- Python
- Java
- PHP
- Go
- Node

To further explain the signing process, we will use a programming language to implement the process described above. The request domain name, API and parameter values in the sample are used here. This goal of this example is only to provide additional clarification for the signature process, please see the SDK for actual usage.

The final output URL might be: https://cvm.convergecloud.com/?Action=DescribeInstances&InstanceIds.0=ins-09dx96dg&Limit=20&Nonce=11886&Offset=0&Region=luzon&SecretId=AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE&Signature=EliP9YW3pW28FpsEdkXt%2F%2BWcGeI%3D&Timestamp=1465185768&Version=2017-03-12

Note: The key in the example is fictitious, and the timestamp is not the current time of the system, so if this URL is opened in the browser or called using commands such as curl, an authentication error will be returned: Signature expired. In order to get a URL that can work properly, you need to replace the SecretId and SecretKey in the example with your real credentials and use the current time of the system as the Timestamp.

Note: In the example below, even if you use the same programming language, the order of the parameters in the URL may be different for each execution. However, the order does not matter, as long as all the parameters are included in the URL and the signature is calculated correctly.

Note: The following code is only applicable to API 3.0. It cannot be directly used in other signature processes. Even with an older API, signature calculation errors may occur due to the differences in details. Please refer to the corresponding documentation.

Java

```
import java.io.UnsupportedEncodingException;
import java.net.URLEncoder;
import java.util.Random;
import java.util.TreeMap;
import javax.crypto.Mac;
import javax.crypto.spec.SecretKeySpec;
import javax.xml.bind.DatatypeConverter;

public class CloudAPIDemo {
    private final static String CHARSET = "UTF-8";

    public static String sign(String s, String key, String method) throws Exception {
        Mac mac = Mac.getInstance(method);
        SecretKeySpec secretKeySpec = new SecretKeySpec(key.getBytes(CHARSET), mac.getAlgorithm());
        mac.init(secretKeySpec);
        byte[] hash = mac.doFinal(s.getBytes(CHARSET));
        return DatatypeConverter.printBase64Binary(hash);
    }

    public static String getStringToSign(TreeMap<String, Object> params) {
        StringBuilder s2s = new StringBuilder("GETcvm.convergecloud.com/?");
        // When signing, the parameters need to be sorted in lexicographical order. TreeMap is used here
to guarantee the correct order.
        for (String k : params.keySet()) {
            s2s.append(k).append("=").append(params.get(k).toString()).append("&");
        }
        return s2s.toString().substring(0, s2s.length() - 1);
    }

    public static String getUrl(TreeMap<String, Object> params) throws UnsupportedEncodingException
{
        StringBuilder url = new StringBuilder("https://cvm.convergecloud.com/?");
        // There is no requirement for the order of the parameters in the actual request URL.
        for (String k : params.keySet()) {
            // The request string needs to be URL encoded. As the Key is all in English letters, only the valu
e is URL encoded here.
            url.append(k).append("=").append(URLEncoder.encode(params.get(k).toString(), CHARSET)).app
end("&");
        }
        return url.toString().substring(0, url.length() - 1);
```

```
    }

    public static void main(String[] args) throws Exception {
        TreeMap<String, Object> params = new TreeMap<String, Object>(); // TreeMap enables automati
c sorting
        // A random number should be used when actually calling, for example: params.put("Nonce", new
Random().nextInt(java.lang.Integer.MAX_VALUE));
        params.put("Nonce", 11886); // Common parameter
        // The current time of the system should be used when actually calling, for example:   params.put
("Timestamp", System.currentTimeMillis() / 1000);
        params.put("Timestamp", 1465185768); // Common parameter
        params.put("SecretId", "AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE"); // Common parameter
        params.put("Action", "DescribeInstances"); // Common parameter
        params.put("Version", "2017-03-12"); // Common parameter
        params.put("Region", "luzon"); // Common parameter
        params.put("Limit", 20); // Business parameter
        params.put("Offset", 0); // Business parameter
        params.put("InstanceIds.0", "ins-09dx96dg"); // Business parameter
        params.put("Signature", sign(getStringToSign(params), "Gu5t9xGARNpq86cd98joQYCN3EXAMPLE
", "HmacSHA1")); // Common parameter
        System.out.println(getUrl(params));
    }
}
```

Python

Note: If running in a Python 2 environment, the following requests dependency package must be installed first: pip install requests .

```
# -*- coding: utf8 -*-
import base64
import hashlib
import hmac
import time

import requests

secret_id = "AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE"
secret_key = "Gu5t9xGARNpq86cd98joQYCN3EXAMPLE"

def get_string_to_sign(method, endpoint, params):
    s = method + endpoint + "/?"
    query_str = "&".join("%s=%s" % (k, params[k]) for k in sorted(params))
    return s + query_str

def sign_str(key, s, method):
```

```
    hmac_str = hmac.new(key.encode("utf8"), s.encode("utf8"), method).digest()
    return base64.b64encode(hmac_str)

if __name__ == '__main__':
    endpoint = "cvm.convergecloud.com"
    data = {
        'Action' : 'DescribeInstances',
        'InstanceIds.0' : 'ins-09dx96dg',
        'Limit' : 20,
        'Nonce' : 11886,
        'Offset' : 0,
        'Region' : 'luzon',
        'SecretId' : secret_id,
        'Timestamp' : 1465185768, # int(time.time())
        'Version': '2017-03-12'
    }
    s = get_string_to_sign("GET", endpoint, data)
    data["Signature"] = sign_str(secret_key, s, hashlib.sha1)
    print(data["Signature"])
    # n actual invocation would occur here, which may incur fees after success
    # resp = requests.get("https://" + endpoint, params=data)
    # print(resp.url)
```

signaturev3

Converge Cloud The API will authenticate each access request, meaning that each request must include signature information (Signature) in the public request parameters to verify the requester's identity.
The signature information is generated by the security credentials, which include SecretId and SecretKey . If the user does not have security credentials, please apply for them on the Cloud API Key page, otherwise they cannot call the Cloud API interfaces.

1. Apply for security credentials.

Before using the Cloud API for the first time, please go to the Cloud API Key page to apply for a security credential.
Security credentials include SecretId and SecretKey:

- SecretId The security credentials are used to identify the identity of the API caller.
- SecretKey The secret key is used to encrypt and sign the string for server-side verification of the signature.
- Users must strictly protect their security credentials and avoid disclosure them.

The specific steps to apply for security credentials are as follows:

1. Log in to Converge Cloud Administration Center Console
2. Go to the console page for cloud API keys
3. On the Cloud API Key page, click New to create a pair of SecretId/SecretKey

Note: Developer accounts can have up to two pairs SecretId / SecretKey.

2. TC3-HMAC-SHA256 signature method

Note: For GET method, only Content-Type: application/x-www-form-urlencoded protocol format is supported. For POST method, Content-Type: application/json and Content-Type: multipart/form-data are currently supported. By default, all business interfaces are supported in json format. Only specific business interfaces are supported in multipart format. In this case, the interface cannot be called in json format. Refer to the specific business interface document description.

The following takes Cloud Virtual Machine querying Region-1 instance list as an example to introduce the signature calculation process step by step. We only use two parameters for the query instance list: Limit and Offset, called using the GET method.

Assume that the SecretId and SecretKey of the user are AKIDz 8krbsJ 5yKBZQpn 74WFkmLPx 3EXAMPLE and Gu 5t9xGARNpq 86cd 98joQYCN3EXAMPLE, respectively.

2.1. splice specification request string

Concatenate CanonicalRequest strings in the following format:

```
CanonicalRequest =
  HTTPRequestMethod + '\n' +
  CanonicalURI + '\n' +
  CanonicalQueryString + '\n' +
  CanonicalHeaders + '\n' +
  SignedHeaders + '\n' +
  HashedRequestPayload
```

- HTTPRequestMethod: HTTP request methods (GET, POST), GET in this example;
- CanonicalURI: URI parameter, API 3.0 fixed to forward slash (/);
- CanonicalQueryString: Query string in the URL that initiates the HTTP request. For POST requests, it is fixed as an empty string. For GET requests, it is the question mark (?) in the URL. The following string content, this example value is: Limit=10&Offset=0. Note: CanonicalQueryString needs to be URL encoded.
- CanonicalHeaders: The header information of participating signature, at least including host and content-type, can also be added with customized header to improve the uniqueness and security of its own request. Splicing rules: 1) head key and value are uniformly converted to lowercase, and the first and last spaces are removed, and spliced according to the format of key:value\n;2) multiple heads are spliced according to the dictionary sorting of head key (lowercase). In this example: content-type: application/x-www-form-urlencoded\nhost: cvm.convergecloud.com\n
- SignedHeaders: The header information involved in the signature indicates which headers participate in the signature of this request, and the header content contained in CanonicalHeaders is one-to-one corresponding. content-type and host are required headers. constructed as: 1) The head key is uniformly converted to lowercase; 2) Multiple header keys (lowercase) are concatenated according to dictionary sorting and separated by semicolons (;). In this case: content-type;host
- HashedRequestPayload: The hash value of the request body, calculated as Lowercase(HexEncode(Hash.SHA256(RequestPayload))), SHA256 hash the entire payload of the HTTP request body, then hexadecimal encoding, and finally converting the encoding string to lowercase letters. Note: For GET requests, RequestPayload is fixed as an empty string. For POST requests, RequestPayload is the payload of the HTTP request body.

According to the above rules, the resulting canonical request string in the example is as follows (for clarity, \nnewlines are replaced by a new line printed separately):

```
GET
```

```
/
Limit=10&Offset=0
content-type:application/x-www-form-urlencoded
host:cvm.convergecloud.com

content-type;host
e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855
```

2.2. Concatenate the string to be signed

Concatenate the string to be signed in the following format:

```
StringToSign =
  Algorithm + \n +
  RequestTimestamp + \n +
  CredentialScope + \n +
  HashedCanonicalRequest
```

- Algorithm: Signature algorithm, currently fixed as TC3-HMAC-SHA256;
- RequestTimestamp: Request timestamp, i.e. the X-TC-Timestamp value of the request header. The request in the example above is 1539084154;
- CredentialScope: Credential range in the format Date/service/tc3_request, containing date, requested service and termination string (tc3_request). **Date is the date of UTC standard time, the value needs to be consistent with UTC standard time converted by common parameter X-TC-Timestamp **;service is the product name, which must be consistent with the product domain name called, such as cvm. The above example request, the value is 2018-10-09/cvm/tc3_request;
- HashedCanonicalRequest: The hash value of the canonical request string obtained by concatenating the above steps is calculated by Lowercase(HexEncode(Hash.SHA256(CanonicalRequest))).

note:

> 1. Date must be calculated from timestamp X-TC-Timestamp and time zone UTC+0. Adding local time zone information to the system, such as East Zone 8, will cause calls to succeed during the day and night, but calls to fail in the early hours of the morning. Assuming the timestamp is 1551113065, the time in the East Eight District is 2019-02-26 00:44:25, but the calculated Date with UTC+0 should be 2019-02-25 instead of 2019-02-26.
> 2. Timestamp must be the current system time and ensure that the system time and standard time are synchronized. If the difference exceeds five minutes, it will fail. If it is not synchronized with the standard time for a long time, it may cause the request to fail after running for a period of time (return signature expiration error).

According to the above rules, the string to be signed in the example is as follows (for clarity,\nnewlines are

replaced by new lines printed):

```
TC3-HMAC-SHA256
1539084154
2018-10-09/cvm/tc3_request
91c9c192c14460df6c1ffc69e34e6c5e90708de2a6d282cccf957dbf1aa7f3a7
```

2.3. calculate the signature

1. Compute the derived signature key, pseudocode as follows

```
SecretKey = "Gu5t9xGARNpq86cd98joQYCN3EXAMPLE"
SecretDate = HMAC_SHA256("TC3" + SecretKey, Date)
SecretService = HMAC_SHA256(SecretDate, Service)
SecretSigning = HMAC_SHA256(SecretService, "tc3_request")
```

- SecretKey: Original SecretKey;
- Date: That is, the Date field information in Credential, as shown in the example above, is 2018-10-09.;
- Service: That is, the Service field information in Credential, as shown in the example above, is cvm;

2. Calculate the signature, pseudocode as follows

```
Signature = HexEncode(HMAC_SHA256(SecretSigning, StringToSign))
```

- SecretSigning: That is, the derivative signature key calculated above;
- StringToSign: That is, the character string to be signed calculated in step 2;

2.4. Splicing Authorization

Splice as follows Authorization:

```
Authorization =
    Algorithm + ' ' +
    'Credential=' + SecretId + '/' + CredentialScope + ', ' +
    'SignedHeaders=' + SignedHeaders + ', '
    'Signature=' + Signature
```

- Algorithm: Signature method, fixed as TC3-HMAC-SHA256;
- SecretId: SecretId in key pair;
- CredentialScope: See above, Scope of Voucher;
- SignedHeaders: See above, header information for participating signatures;
- Signature: signature value

According to the above rules, the values obtained in the example are:

```
TC3-HMAC-SHA256 Credential=AKIDEXAMPLE/Date/service/tc3_request, SignedHeaders=content-type;host, Signature=5da7a33f6993f0614b047e5df4582db9e9bf4672ba50567dba16c6ccf174c474
```

The final complete invocation information is as follows:

```
https://cvm.convergecloud.com/?Limit=10&Offset=0

Authorization: TC3-HMAC-SHA256 Credential=AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE/2018-10-09/cvm/tc3_request, SignedHeaders=content-type;host, Signature=5da7a33f6993f0614b047e5df4582db9e9bf4672ba50567dba16c6ccf174c474
Content-Type: application/x-www-form-urlencoded
Host: cvm.convergecloud.com
X-TC-Action: DescribeInstances
X-TC-Version: 2017-03-12
X-TC-Timestamp: 1539084154
X-TC-Region: luzon
```

3. signing failed

According to the actual situation, there are the following signature failure error codes, please handle according to the actual situation

error code	error description
AuthFailure.SignatureExpire	signature expiration
AuthFailure.SecretIdNotFound	key is not present
AuthFailure.SignatureFailure	signature error
AuthFailure.TokenFailure	token error
AuthFailure.InvalidSecretId	Illegal key (not cloud API key type)

4. Signature Demo

Java

```
import java.io.BufferedReader;
import java.io.InputStream;
```

```
import java.io.InputStreamReader;
import java.net.URL;
import java.text.SimpleDateFormat;
import java.util.Date;
import java.util.Map;
import java.util.TimeZone;
import java.util.TreeMap;
import javax.crypto.Mac;
import javax.crypto.spec.SecretKeySpec;
import javax.net.ssl.HttpsURLConnection;
import javax.xml.bind.DatatypeConverter;

import org.apache.commons.codec.digest.DigestUtils;

public class CloudAPITC3Demo {
    private final static String CHARSET = "UTF-8";
    private final static String ENDPOINT = "cvm.convergecloud.com";
    private final static String PATH = "/";
    private final static String SECRET_ID = "AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE";
    private final static String SECRET_KEY = "Gu5t9xGARNpq86cd98joQYCN3EXAMPLE";
    private final static String CT_X_WWW_FORM_URLENCODED = "application/x-www-form-urlencode
d";
    private final static String CT_JSON = "application/json";
    private final static String CT_FORM_DATA = "multipart/form-data";

    public static byte[] sign256(byte[] key, String msg) throws Exception {
        Mac mac = Mac.getInstance("HmacSHA256");
        SecretKeySpec secretKeySpec = new SecretKeySpec(key, mac.getAlgorithm());
        mac.init(secretKeySpec);
        return mac.doFinal(msg.getBytes(CHARSET));
    }

    public static void main(String[] args) throws Exception {
        String service = "cvm";
        String host = "cvm.convergecloud.com";
        String region = "luzon";
        String action = "DescribeInstances";
        String version = "2017-03-12";
        String algorithm = "TC3-HMAC-SHA256";
        String timestamp = "1539084154";
        //String timestamp = String.valueOf(System.currentTimeMillis() / 1000);
        SimpleDateFormat sdf = new SimpleDateFormat("yyyy-MM-dd");
        // Pay attention to the time zone, otherwise it is easy to make mistakes.
        sdf.setTimeZone(TimeZone.getTimeZone("UTC"));
        String date = sdf.format(new Date(Long.valueOf(timestamp + "000")));

        // ************* Step 1: Assemble the specification request string *************
```

```
        String httpRequestMethod = "GET";
        String canonicalUri = "/";
        String canonicalQueryString = "Limit=10&Offset=0";
        String canonicalHeaders = "content-type:application/x-www-form-urlencoded\n" + "host:" + host
+ "\n";
        String signedHeaders = "content-type;host";
        String hashedRequestPayload = DigestUtils.sha256Hex("");
        String canonicalRequest = httpRequestMethod + "\n" + canonicalUri + "\n" + canonicalQueryStri
ng + "\n"
                + canonicalHeaders + "\n" + signedHeaders + "\n" + hashedRequestPayload;
        System.out.println(canonicalRequest);

        // ************* Step 2: Stitching the string to be signed *************
        String credentialScope = date + "/" + service + "/" + "tc3_request";
        String hashedCanonicalRequest = DigestUtils.sha256Hex(canonicalRequest.getBytes(CHARSET));
        String stringToSign = algorithm + "\n" + timestamp + "\n" + credentialScope + "\n" + hashedCan
onicalRequest;
        System.out.println(stringToSign);

        // ************* Step 3: Calculate the signature *************
        byte[] secretDate = sign256(("TC3" + SECRET_KEY).getBytes(CHARSET), date);
        byte[] secretService = sign256(secretDate, service);
        byte[] secretSigning = sign256(secretService, "tc3_request");
        String signature = DatatypeConverter.printHexBinary(sign256(secretSigning, stringToSign)).toLow
erCase();
        System.out.println(signature);

        // ************* Step 4: Splicing Authorization *************
        String authorization = algorithm + " " + "Credential=" + SECRET_ID + "/" + credentialScope + ", "
                + "SignedHeaders=" + signedHeaders + ", " + "Signature=" + signature;
        System.out.println(authorization);

        TreeMap<String, String> headers = new TreeMap<String, String>();
        headers.put("Authorization", authorization);
        headers.put("Host", host);
        headers.put("Content-Type", CT_X_WWW_FORM_URLENCODED);
        headers.put("X-TC-Action", action);
        headers.put("X-TC-Timestamp", timestamp);
        headers.put("X-TC-Version", version);
        headers.put("X-TC-Region", region);
    }
}
```

Python

```
# -*- coding: utf-8 -*-
```

```
import hashlib, hmac, json, os, sys, time
from datetime import datetime

# key parameters
secret_id = "AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE"
secret_key = "Gu5t9xGARNpq86cd98joQYCN3EXAMPLE"

service = "cvm"
host = "cvm.convergecloud.com"
endpoint = "https://" + host
region = "luzon"
action = "DescribeInstances"
version = "2017-03-12"
algorithm = "TC3-HMAC-SHA256"
timestamp = 1539084154
date = datetime.utcfromtimestamp(timestamp).strftime("%Y-%m-%d")
params = {"Limit": 10, "Offset": 0}

# ************* Step 1: Assemble the specification request string *************
http_request_method = "GET"
canonical_uri = "/"
canonical_querystring = "Limit=10&Offset=0"
ct = "x-www-form-urlencoded"
payload = ""
if http_request_method == "POST":
    canonical_querystring = ""
    ct = "json"
    payload = json.dumps(params)
canonical_headers = "content-type:application/%s\nhost:%s\n" % (ct, host)
signed_headers = "content-type;host"
hashed_request_payload = hashlib.sha256(payload.encode("utf-8")).hexdigest()
canonical_request = (http_request_method + "\n" +
                     canonical_uri + "\n" +
                     canonical_querystring + "\n" +
                     canonical_headers + "\n" +
                     signed_headers + "\n" +
                     hashed_request_payload)
print(canonical_request)

# ************* Step 2: Stitching the string to be signed *************
credential_scope = date + "/" + service + "/" + "tc3_request"
hashed_canonical_request = hashlib.sha256(canonical_request.encode("utf-8")).hexdigest()
string_to_sign = (algorithm + "\n" +
                  str(timestamp) + "\n" +
                  credential_scope + "\n" +
                  hashed_canonical_request)
print(string_to_sign)
```

```
# ************* Step 3: Calculate the signature *************
# Compute signature digest function
def sign(key, msg):
    return hmac.new(key, msg.encode("utf-8"), hashlib.sha256).digest()
secret_date = sign(("TC3" + secret_key).encode("utf-8"), date)
secret_service = sign(secret_date, service)
secret_signing = sign(secret_service, "tc3_request")
signature = hmac.new(secret_signing, string_to_sign.encode("utf-8"), hashlib.sha256).hexdigest()
print(signature)

# ************* Step 4: Splicing Authorization *************
authorization = (algorithm + " " +
                 "Credential=" + secret_id + "/" + credential_scope + ", " +
                 "SignedHeaders=" + signed_headers + ", " +
                 "Signature=" + signature)
print(authorization)

# Common parameters added to request header
headers = {
    "Authorization": authorization,
    "Host": host,
    "Content-Type": "application/%s" % ct,
    "X-TC-Action": action,
    "X-TC-Timestamp": str(timestamp),
    "X-TC-Version": version,
    "X-TC-Region": region,
}
```

request

1. Service Address

Region refers to the geographical area of a physical data center. Converge Cloud ensures complete isolation between different regions, providing maximum stability and fault tolerance. To reduce access latency and improve download speed, it is recommended to choose the region closest to your customers.

You can view the complete region list by using the API interface "DescribeRegions".

2. Communications Protocol

All the Converge Cloud APIs communicate via HTTPS, providing highly secure communication tunnels.

3. Request Methods

Supported HTTP request methods:

- POST (recommended)
- GET

PThe Content-Type types supported by POST requests:

- application/json (recommended). The TC3-HMAC-SHA256 signature algorithm must be used.
- application/x-www-form-urlencoded. The HmacSHA1 or HmacSHA256 signature algorithm must be used.
- multipart/form-data (only supported by certain APIs). You must use TC3-HMAC-SHA256 to calculate the signature.

The size of a GET request packet is up to 32 KB. The size of a POST request is up to 1 MB when the HmacSHA1 or HmacSHA256 signature algorithm is used, and up to 10 MB when TC3-HMAC-SHA256 is used.

4. Character Encoding

Only UTF-8 encoding is used.

result

Response for Successful Requests

For example, when calling CAM API (version: 2017-03-12) to view the status of instances (DescribeInstancesStatus), if the request has succeeded, you may see the response as shown below:

```
{
    "Response": {
        "TotalCount": 0,
        "InstanceStatusSet": [],
        "RequestId": "b5b41468-520d-4192-b42f-595cc34b6c1c"
    }
}
```

- The API will return Response, which contains RequestId, as long as it processes the request. It does not matter if the request is successful or not.
- RequestId is the unique ID of an API request. Contact us with this ID when an exception occurs.
- Except for the fixed fields, all fields are action-specified. For the definitions of action-specified fields, see the corresponding API documentation. In this example, TotalCount and InstanceStatusSet are the fields specified by the API DescribeInstancesStatus. 0 TotalCount means that the requester owns 0 CVM instance so the InstanceStatusSet is empty.

Response for Failed Requests

If the request has failed, you may see the response as shown below:

```
{
    "Response": {
        "Error": {
            "Code": "AuthFailure.SignatureFailure",
            "Message": "The provided credentials could not be validated. Please check your signature is cor
rect."
        },
        "RequestId": "ed93f3cb-f35e-473f-b9f3-0d451b8b79c6"
    }
}
```

- The presence of the Error field indicates that the request has failed. A response for a failed request will include Error, Code and Message fields.

- Code is the code of the error that helps you identify the cause and solution. There are two types of error codes so you may find the code in either common error codes or API-specified error codes.
- Message explains the cause of the error. Note that the returned messages are subject to service updates. The information the messages provide may not be up-to-date and should not be the only source of reference.
- RequestId is the unique ID of an API request. Contact us with this ID when an exception occurs.

Common Error Codes

If there is an Error field in the response, it means that the API call failed. The Code field in Error indicates the error code. The following table lists the common error codes that all actions can return.

Error Code	Description
AuthFailure.InvalidSecretId	Invalid key (not a API key type).
AuthFailure.MFAFailure	MFA failed.
AuthFailure.SecretIdNotFound	The key does not exist.
AuthFailure.SignatureExpire	Signature expired.
AuthFailure.SignatureFailure	Signature error.
AuthFailure.TokenFailure	Token error.
AuthFailure.UnauthorizedOperation	The request does not have CAM authorization.
DryRunOperation	DryRun Operation. It means that the request would have succeeded, but the DryRun parameter was used.
FailedOperation	Operation failed.
InternalError	Internal error.
InvalidAction	The API does not exist.
InvalidParameter	Incorrect parameter.
InvalidParameterValue	Invalid parameter value.
LimitExceeded	Quota limit exceeded.
MissingParameter	A parameter is missing.
NoSuchVersion	The API version does not exist.

Error Code	Description
RequestLimitExceeded	The number of requests exceeds the frequency limit.
ResourceInUse	Resource is in use.
ResourceInsufficient	Insufficient resource.
ResourceNotFound	The resource does not exist.
ResourceUnavailable	Resource is unavailable.
UnauthorizedOperation	Unauthorized operation.
UnknownParameter	Unknown parameter.
UnsupportedOperation	Unsupported operation.
UnsupportedProtocol	hHTTPS request method error. Only GET and POST requests are supported.
UnsupportedRegion	API does not support the requested region.

PublicParameter

Common parameters are parameters used to identify users and interface authentication purposes. If not necessary, these parameters are not described in the separate interface document of each interface, but these parameters need to be carried in each request before the request can be normally initiated.

signature method v3

When using TC3-HMAC-SHA256 signature method, the common parameters need to be uniformly placed in the HTTP Header request header, as follows:

parameter name	type	required	described
X-TC-Action	String	Yes	The name of the operation interface. Refer to the description of the public parameter Action in the input parameters of the interface documentation for the value. For example, the value for the query instance list interface of the cloud server is DescribeInstances.
X-TC-Region	String	Yes	region parameters, Data used to identify which region you wish to operate on. The region value accepted by the interface refers to the description of the input parameter common parameter Region in the interface document. Note: Some interfaces do not need to pass this parameter, which is specifically stated in the interface documentation. In this case, even passing this parameter will not take effect.
X-TC-Timestamp	Integer	Yes	The current UNIX timestamp, which records the time when the API request was initiated. for example 1529223702. Note: If the time difference from the server exceeds 5 minutes, it will cause a signature expiration error.
X-TC-Version	String	Yes	Version of API for operation. Refer to the description of the public parameter Version in the interface document for the value. For example, the version of the cloud server. 2017-03-12.
Authorization	String	Yes	HTTP The standard authentication header field is "Authorization". For example: TC3-HMAC-SHA256 Credential=AKIDEXAMPLE/Date/service/tc3_request, SignedHeaders=content-type;host, Signature=fe5f80f77d5fa3beca038a248ff027d0445342fe2855ddc963176630326f1024 Here, - TC3-HMAC-SHA256: Signature method, currently fixed as this value, - Credential: Credential: Signature credential; AKIDEXAMPLE is the SecretId; Date is a date in UTC time, and this value must match the value of X-TC-Timestamp (a common parameter) in UTC time format; service is the name of the product/service, and is generally a domain name prefix. For example,cvm; - SignedHeaders: The headers that contains the authentication information; content-type and host are the required headers; - Signature: Signature digest.
X-TC-Token	String	No	The token used for temporary certificates needs to be used in conjunction with a temporary key. Temporary keys and tokens need to be obtained by calling the access management service interface. Long-term keys do not require tokens.

signature method v1

When using HmacSHA1 and HmacSHA256 signature methods, common parameters need to be placed uniformly in the request string, as follows

parameter name	type	required	described
Action	String	Yes	The name of the interface to be operated. The value refers to the explanation of the public parameter Action in the interface documentation. For example, for the cloud server's query instance list interface, the value is DescribeInstances .
Region	String	Yes	The region parameter is used to identify which region's data you want to operate on. The region value accepted by the interface is specified in the input parameter of the public parameter Region in the interface documentation. Note: Some interfaces do not require this parameter to be passed, which will be specifically mentioned in the interface documentation. Even if this parameter is passed, it will not take effect in this case.
Timestamp	Integer	Yes	The current UNIX timestamp, which can record the time when the API request is initiated. For example, 1529223702. If the difference between the current time is too large, it will cause a signature expiration error.
Nonce	Integer	Yes	A random positive integer combined with Timestamp is used to prevent replay attacks.
SecretId	String	Yes	The SecretId is an identifier applied for the cloud API key to identify the user's identity. A SecretId corresponds to a unique SecretKey , and the SecretKey is used to generate the request signature Signature .
Signature	String	Yes	Request signature is used to verify the legitimacy of this request. Users need to calculate it based on the actual input parameters. The specific calculation method can be found in the interface authentication documentation.
Version	String	Yes	The version of the API being operated on. The value refers to the description of the public parameter Version in the interface documentation. For example, the version of the cloud server. 2017-03-12.
SignatureMethod	String	No	Signature method, currently supports HmacSHA256 and HmacSHA1. HmacSHA256 algorithm is used to verify signatures only if this parameter is specified as HmacSHA 256, otherwise HmacSHA1 is used to verify signatures.
Token	String	No	Token used for temporary certificate needs to be used together with temporary key. The temporary key and Token need to be obtained from the Access Management service invocation interface. Long-term keys do not require tokens.

zone list

A region (Region) refers to the geographical area of a physical data center. Converge Cloud Translation: To deliver verification that completely isolates different regions, ensuring maximum stability and fault tolerance between regions. In order to reduce access latency and improve download speed, it is recommended that you choose the region closest to your customers.

You can view the complete region list by using the API interface Query Region List.

DC-related APIs
ApproveDirectConnectTunnel

1. Interface Description

Interface request domain name: dc.api3.convergecloud.com.

The DC owner approves shared channel application.

Default interface request rate limit: 20 times per second.

Interface update time: 2025-08-22 00:40:59.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ApproveDirectConnectTunnel
Version	Yes	No	String	Public parameter, The value of this interface: 2018-04-10
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
DirectConnectTunnelId	Yes	No	String	Private Channel ID Example: dcx-2j1x1udk
DirectConnectTunnelName	Yes	No	String	Private Channel Name Example: dc_name
Approved	Yes	No	Bool	Approval result: True: Approved; and False: Not approved. Example: True
Comments	No	No	String	Remarks Example: Comments

3. Output Parameters

Parameter name	Type	Description

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error
InvalidParameter	Wrong parameter.
InvalidParameter.DcResourceNotFound	The direct connection resource does not exist.

CreateDirectConnect

1. Interface Description

Interface request domain name: dc.api3.convergecloud.com.

Apply for physical DC access.

Default interface request rate limit: 20 times per second.

Interface update time: 2025-08-22 00:55:12.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: CreateDirectConnect
Version	Yes	No	String	Public parameter, The value of this interface: 2018-04-10
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
DirectConnectName	Yes	No	String	Physical DC Name Example: Local Hangxin Connection 1
AccessPointId	Yes	No	String	Access point for physical DC. You can access the region ID by calling the DescribeAccessPoints interface. The selected access point must exist and be in an accessible state. Example: ap-cn-place-hx
LineOperator	Yes	No	String	ISPs providing access connection. Telecom: CTCC; Mobile: CMCC; Unicom: CUCC; In-houseWiring: in-house wiring; Other: others; InternationalOperator: others mainland. Example: Mobile
Location	Yes	No	String	Geographical location of the local data center. Example: 14th Floor, Sigma A Building, Haidian District, Local City
CloudPortType	Yes	No	String	Physical DC port type, values: 100 Base-T: Fast Ethernet port, 1000 Base-T (default value): Gigabit Ethernet port, 1000 Base-LX: Gigabit single-mode fiber port (10 km), 10 GBase-T: 10 Gigabit Ethernet port, 10 GBase-LR: 10 Gigabit single-mode fiber port (10 km), default value, Gigabit single-mode fiber port (10 km). Example: 100Base-T
Bandwidth	Yes	No	Int64	Physical DC interface bandwidth, in a unit of Mbps, with a default value of 1000, and a value range of [2, 10240]. Example: 1000
RedundantDirectConnectId	No	No	String	Redundant physical DC ID. Example: dc-12345678
CustomerName	Yes	No	String	Name of physical DC applicant, obtained from account system by default. Example: John Doe
CustomerContactMail	Yes	No	String	E-mail address of physical DC applicant, obtained from account system by default. Example: 12345@mail.com
CustomerContactNumber	Yes	No	String	Contact number of physical DC applicant, obtained from account system by default. Example: 110
IdcPortType	Yes	No	String	Physical DC IDC side port type, values: 100 Base-T: Fast Ethernet port, 1000 Base-T (default value): Gigabit Ethernet port, 1000 Base-LX: Gigabit single-mode fiber port (10 km), 10 GBase-T: 10 Gigabit Ethernet port, 10 GBase-LR: 10 Gigabit single-mode fiber port (10 km), default value, Gigabit single-mode fiber port (10 km). Example: 100Base-T
IdcCity	Yes	No	String	City Where Data Center Locates Example: place

3. Output Parameters

Parameter name	Type	Description
DirectConnectIdSet	Array of String	Physical DC ID Example: ["dc-abcdefgh"]
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error
LimitExceeded	Exceeded quota limit

Error Code	Description
UnsupportedOperation	Operation unsupported.
ResourceNotFound	The resource does not exist.
LimitExceeded.DirectConnectLimitExceeded	Number of physical DCs has reached a limit.
UnauthorizedOperation	Unauthorized operation
InvalidParameter.PortBandwidthMismatch	Port bandwidths of the cloud side and the IDC side mismatch.
InvalidParameter.DcBandwidthOutOfRange	Physical DC bandwidth is out of range. Physical DC bandwidth is required to be greater than 1, not less than the maximum bandwidth of the private channel, not greater than the port bandwidth, and not less than a sum of private channel bandwidths in a non-overselling mode.

CreateDirectConnectTunnel

1. Interface Description

Interface request domain name: dc.api3.convergecloud.com.

API for Creating Dedicated Channel

Default interface request rate limit: 20 times per second.

Interface update time: 2025-08-22 01:15:19.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: CreateDirectConnectTunnel
Version	Yes	No	String	Public parameter, The value of this interface: 2018-04-10
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
DirectConnectId	Yes	No	String	DC ID, for example, dc-kd7d06of. Example: dc-abcdefgh
DirectConnectTunnelName	Yes	No	String	Tunnel name Example: dc_name
DirectConnectOwnerAccount	No	No	String	Physical DC owner, which is the current customer (physical DC owner) by default. For a shared DC, the developer account ID of the shared DC needs to be entered here. Example: 110000000163
VpcName	Yes	No	String	VPC Unified ID or CPM Network Unified ID Example: vpc-r8ztdfrd
DirectConnectGatewayId	Yes	No	String	DC gateway ID, for example, dcg-d545ddf. Example: dcg-abcdefgh
Bandwidth	Yes	No	Int64	DC Bandwidth, unit: Mbps Default is the bandwidth value of the physical DC. Example: 100
RouteType	Yes	No	String	BGP: BGP routing STATIC: Static routing Default is BGP routing. Example: BGP
BgpPeer	No	No	BgpPeer	BgpPeer, user-side BGP information, including ASN and AuthKey. Example:View
IdcRoutes	No	No	String	Static Routing, User IDC Subnet Address Example: 10.0.0.0/16
Vlan	Yes	No	Int64	VLAN, in a range of 11-4000, needing to match VLAN ID of the user side. Example: 100
CloudAddress	Yes	No	String	Cloud-Side Interconnect IP Example: 10.10.10.10
CustomerAddress	Yes	No	String	CustomerAddress, user-side interconnect IP. Example: 192.168.1.1/30

Parameter name	Required	Allow NULL	Type	Description
RelatedDirectConnectTunnelId	No	No	String	Associated Redundancy Channel ID Example: dcx-2j1x1udk
LoadMode	Yes	No	String	Channel CLB modes: None: Non-redundancy mode LoadBalance: CLB MasterSlave: Primary and secondary Example: LoadBalance
VpcId	Yes	No	Int64	VPC Digital ID Example: 65535
EnableBfd	Yes	No	Bool	Whether to Enable BFD Example: True
BfdInterval	No	No	Int64	BFD Protocol Interval Configuration Example: 100
ConnectSubnetMask	Yes	No	Uint64	Interconnection Address Mask Example: 16
NetworkRegion	Yes	No	String	Region Where VPC Locates Example: ap-test
IpType	No	No	String	Channel IP Protocol Type Example: v4

3. Output Parameters

Parameter name	Type	Description
DirectConnectTunnelIdSet	Array of String	Dedicated Channel ID Example: ["dcx-abcdefgh"]
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
MissingParameter	Parameter missing
InternalError	Internal error
InvalidParameter	Wrong parameter.
InvalidParameterValue	Incorrect parameter value
InvalidParameterValue.VlanConfLict	VLAN Conflict
LimitExceeded.DirectConnectTunnelLimitExceeded	Number of dedicated channels for the physical DC has reached a limit.
InvalidParameter.UinIsNotExist	This account ID does not exist.
LimitExceeded	Exceeded quota limit
ResourceUnavailable.InsufficientBalance	Sorry, your account is overdue. Products cannot be activated in an overdue status. Please recharge first.
UnsupportedOperation	Operation unsupported.
InvalidParameter.AddressError	Interconnect IP Error

Error Code	Description
ResourceInUse.DcVpcIsExist	The VPC for the physical DC already exists.
UnsupportedOperation.CrossBorderDirectConnectTunnel	Creating cross-border dedicated channels is not allowed. Please contact us.
InvalidParameter.DirectConnectIdIsNotUin	The physical DC does not belong to this account.
LimitExceeded.DirectConnectLimitExceeded	Number of physical DCs has reached a limit.
InvalidParameter.DcxBandwidthOutOfRange	Physical DC bandwidth is out of range. Private channel bandwidth is required to be greater than 1, and not greater than the physical DC bandwidth, and a sum of private channel bandwidths is not greater than the physical DC bandwidth in a non-overselling mode.
InvalidParameter.ArAvailBandwidthNotEnough	The available bandwidth is insufficient at the DC access point.

DeleteDirectConnect

1. Interface Description

Interface request domain name: dc.api3.convergecloud.com.

Delete physical DC.

Default interface request rate limit: 20 times per second.

Interface update time: 2022-11-29 23:51:50.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DeleteDirectConnect
Version	Yes	No	String	Public parameter, The value of this interface: 2018-04-10
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
DirectConnectId	Yes	No	String	Physical DC ID Example: dc-2j1x1udk

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error
InvalidParameter	Wrong parameter.
InvalidParameterValue	Incorrect parameter value
UnsupportedOperation	Operation unsupported.
ResourceNotFound	The resource does not exist.
FailedOperation	Operation Failed
InvalidParameter.DirectConnectIdIsNotUin	The physical DC does not belong to this account.
UnauthorizedOperation	Unauthorized operation
LimitExceeded.DirectConnectTunnelLimitExceeded	Number of dedicated channels for the physical DC has reached a limit.
InvalidParameter.DcResourceNotFound	The direct connection resource does not exist.

DeleteDirectConnectTunnel

1. Interface Description

Interface request domain name: dc.api3.convergecloud.com.

Delete tunnel

Default interface request rate limit: 20 times per second.

Interface update time: 2022-11-29 23:52:28.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DeleteDirectConnectTunnel
Version	Yes	No	String	Public parameter, The value of this interface: 2018-04-10
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
DirectConnectTunnelId	Yes	No	String	Dedicated Channel ID Example: dcx-2j1x1udk

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error
InvalidParameter	Wrong parameter.
UnsupportedOperation.StateConfLict	Status Conflict
UnsupportedOperation	Operation unsupported.
ResourceNotFound	The resource does not exist.
ResourceNotFound.DirectConnectTunnelIdIsNotExist	Dedicated channel does not exist.
InvalidParameter.DcResourceNotFound	The direct connection resource does not exist.

DescribeAccessPoints

1. Interface Description

Interface request domain name: dc.api3.convergecloud.com.

Query access point of physical DC.

Default interface request rate limit: 20 times per second.

Interface update time: 2022-11-29 23:52:45.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeAccessPoints
Version	Yes	No	String	Public parameter, The value of this interface: 2018-04-10
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
Offset	No	No	Int64	Offset, with a default value of 0. Example: 0
Limit	No	No	Int64	Number of returns, with a default value of 20, and a maximum value of 100. Example: 100
Filters	No	No	Array of Filter	Filter Parameters, supporting filtering based on an array of access point IDs (AccessPointId) Example:View

3. Output Parameters

Parameter name	Type	Description
AccessPointSet	Array of AccessPoint	Access Point Information Example:View
TotalCount	Uint64	Number of Access Points Example: 100
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
MissingParameter	Parameter missing
ResourceUnavailable	Resource unavailable
InternalError	Internal error
InvalidParameter	Wrong parameter.
InvalidParameterValue	Incorrect parameter value
UnsupportedOperation	Operation unsupported.
ResourceNotFound	The resource does not exist.
UnauthorizedOperation	Unauthorized operation

DescribeCloudBgpAsn

1. Interface Description

Interface request domain name: dc.api3.convergecloud.com.

Access BGP ASN used in BGP-type channel cloud.

Default interface request rate limit: 20 times per second.

Interface update time: 2024-10-24 04:26:06.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeCloudBgpAsn
Version	Yes	No	String	Public parameter, The value of this interface: 2018-04-10
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface

3. Output Parameters

Parameter name	Type	Description
CloudBgpAsn	Int64	BGP ASN used in the BGP-type channel cloud Example: 100
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error

DescribeDirectConnectPortPrice

1. Interface Description

Interface request domain name: dc.api3.convergecloud.com.

Query monthly rental price of a DC port, namely port inquiry.

Default interface request rate limit: 20 times per second.

Interface update time: 2025-08-22 01:17:46.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeDirectConnectPortPrice
Version	Yes	No	String	Public parameter, The value of this interface: 2018-04-10
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
PortType	Yes	No	String	Port Type for Inquiry Example: trunk

3. Output Parameters

Parameter name	Type	Description
PortType	String	Port type Example: 100Base-T

Parameter name	Type	Description
TotalCost	Float	Monthly Rental Price of Port Example: 300.1
RealTotalCost	Float	Monthly Rental Price of Port, price after discount. Example: 300.1
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error

DescribeDirectConnectTunnels

1. Interface Description

Interface request domain name: dc.api3.convergecloud.com.

Used for querying dedicated channel list.

Default interface request rate limit: 20 times per second.

Interface update time: 2022-11-29 23:48:27.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeDirectConnectTunnels
Version	Yes	No	String	Public parameter, The value of this interface: 2018-04-10
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
Offset	No	No	Int64	Offset, with a default value of 0. Example: 0
Limit	No	No	Int64	Number of returns, with a default value of 20, and a maximum value of 100. Example: 20
Filters	No	No	Array of Filter	Filter criteria. Filtering by state, dedicated tunnel ID or name, connection ID, Direct Connect gateway ID, associated tunnel, redundant tunnel ID, or IP address type is supported. Example:View

3. Output Parameters

Parameter name	Type	Description
DirectConnectTunnelSet	Array of DirectConnectTunnel	Dedicated Channel List Example:View
TotalCount	Int64	Total Number of Channels Meeting Conditions Example: 100
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error
ResourceNotFound	The resource does not exist.
ResourceNotFound.DirectConnectTunnelIdIsNotExist	Dedicated channel does not exist.

DescribeDirectConnects

1. Interface Description

Interface request domain name: dc.api3.convergecloud.com.

Query physical DC list.

Default interface request rate limit: 20 times per second.

Interface update time: 2024-11-21 01:28:36.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeDirectConnects
Version	Yes	No	String	Public parameter, The value of this interface: 2018-04-10
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
Offset	No	No	Int64	Offset, with a default value of 0. Example: 0
Limit	No	No	Int64	Number of returns, with a default value of 20, and a maximum value of 100. Example: 100
Filters	No	No	Array of Filter	Filter criteria. Filtering by state, Direct Connect ID, Direct Connect name, AppId, Direct Connect owner UIN, or whether it is a shared Direct Connect is supported. Example:View
DirectConnectIds	No	No	Array of String	Connection ID Example: dc-m6t1txpp

3. Output Parameters

Parameter name	Type	Description
DirectConnectSet	Array of DirectConnect	Physical DC List Example:View
TotalCount	Int64	Conform to the number of physical DC lists. Example: 100
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
UnauthorizedOperation	Unauthorized operation
UnsupportedOperation	Operation unsupported.
InternalError	Internal error
InvalidParameterValue	Incorrect parameter value
ResourceNotFound	The resource does not exist.
InvalidParameter	Wrong parameter.

DescribeIsp

1. Interface Description

Interface request domain name: dc.api3.convergecloud.com.

Obtains dedicated line ISP information

Default interface request rate limit: 20 times per second.

Interface update time: 2025-08-22 01:23:34.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeIsp
Version	Yes	No	String	Public parameter, The value of this interface: 2018-04-10
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface

3. Output Parameters

Parameter name	Type	Description
IspList	Array of IspInfo	ISP detailed information list Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
MissingParameter	Parameter missing
ResourceUnavailable	Resource unavailable
InternalError	Internal error
InvalidParameter	Wrong parameter.
InvalidParameterValue	Incorrect parameter value
UnsupportedOperation	Operation unsupported.
ResourceNotFound	The resource does not exist.
UnauthorizedOperation	Unauthorized operation

ModifyDirectConnectAttribute

1. Interface Description

Interface request domain name: dc.api3.convergecloud.com.

Modify properties of physical DC.

Default interface request rate limit: 20 times per second.

Interface update time: 2025-08-02 01:27:33.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ModifyDirectConnectAttribute
Version	Yes	No	String	Public parameter, The value of this interface: 2018-04-10
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
DirectConnectId	Yes	No	String	Physical DC ID Example: dcx-abcdefgh
DirectConnectName	Yes	No	String	Physical DC Name Example: mock_dc
CustomerContactMail	Yes	No	String	E-mail address of physical DC applicant, obtained from account system by default. Example: 12345@mail.com
CustomerName	Yes	No	String	Name of physical DC applicant, obtained from account system by default. Example: John Doe
CustomerContactNumber	Yes	No	String	Contact number of physical DC applicant, obtained from account system by default. Example: 18812345678
Bandwidth	No	No	Uint64	Physical DC Bandwidth Example: 1000
IsShare	No	No	Bool	Whether to share. Example: True

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
UnauthorizedOperation	Unauthorized operation
UnsupportedOperation	Operation unsupported.
InternalError	Internal error
InvalidParameterValue	Incorrect parameter value
ResourceNotFound	The resource does not exist.
ResourceUnavailable.InsufficientBalance	Sorry, your account is overdue. Products cannot be activated in an overdue status. Please recharge first.
InvalidParameter.DirectConnectIdIsNotUin	The physical DC does not belong to this account.
InvalidParameter	Wrong parameter.
InvalidParameter.DcBandwidthOutOfRange	Physical DC bandwidth is out of range. Physical DC bandwidth is required to be greater than 1, not less than the maximum bandwidth of the private channel, not greater than the port bandwidth, and not less than a sum of private channel bandwidths in a non-overselling mode.
InvalidParameter.DcResourceNotFound	The direct connection resource does not exist.

ModifyDirectConnectTunnelAttribute

1. Interface Description

Interface request domain name: dc.api3.convergecloud.com.

Modify properties of dedicated channel.

Default interface request rate limit: 20 times per second.

Interface update time: 2025-08-02 01:36:20.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ModifyDirectConnectTunnelAttribute
Version	Yes	No	String	Public parameter, The value of this interface: 2018-04-10
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
DirectConnectTunnelId	Yes	No	String	Dedicated Channel ID Example: dcx-2j1x1udk
DirectConnectTunnelName	No	No	String	Tunnel name Example: dc_name
IdcRoutes	No	No	String	User-Side Network Segment Address Example: 10.0.0.0/16
Bandwidth	No	No	Int64	Dedicated channel bandwidth value, in a unit of M. Example: 100
Comments	No	No	String	Channel Remarks Example: Comments
EnableBfd	No	No	Bool	Whether to Enable BFD Example: True

Parameter name	Required	Allow NULL	Type	Description
BfdInterval	No	No	Int64	BFD Packet Interval Time Example: 30
EnableMulticast	No	No	Bool	Whether to Enable Multicast Example: True
MulticastGroups	No	No	String	Channel Multicast Group Address Example: 224.0.2.2
BgpPeer	No	No	BgpPeer	BGP ASN and PASSWORD Example:View

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
ResourceNotFound.DirectConnectTunnelIdIsNotExist	Dedicated channel does not exist.
InternalError	Internal error
InvalidParameter	Wrong parameter.
UnsupportedOperation.StateConfLict	Status Conflict
FailedOperation	Operation Failed
MissingParameter	Parameter missing
InvalidParameter.DcxBandwidthOutOfRange	Physical DC bandwidth is out of range. Private channel bandwidth is required to be greater than 1, and not greater than the physical DC bandwidth, and a sum of private channel bandwidths is not greater than the physical DC bandwidth in a non-overselling mode.
InvalidParameter.DcResourceNotFound	The direct connection resource does not exist.

Error Code	Description
InvalidParameter.InvalidIpMulticastConfig	An error in IP multicast configuration occurs.

UpdateVifAssociated

1. Interface Description

Interface request domain name: dc.api3.convergecloud.com.

Update channel redundancy mode.

Default interface request rate limit: 20 times per second.

Interface update time: 2025-08-22 01:25:05.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: UpdateVifAssociated
Version	Yes	No	String	Public parameter, The value of this interface: 2018-04-10
Region	No	No	String	Public parameter,Regional information A list of supported geographies is available through the DescribeRegions interface
DirectConnectTunnelId	Yes	No	String	Private channel ID, for example, dcx-nsurd338 Example: dcx-2j1x1udk
LoadMode	Yes	No	String	Channel CLB modes: None: Non-redundancy mode LoadBalance: CLB MasterSlave: Primary and secondary Example: LoadBalance
RelatedDirectConnectTunnelId	No	No	String	Associated private channel ID, for example, dcx-nsurd338. Example: dcx-2j1x1udk

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
FailedOperation	Operation Failed
InternalError	Internal error
InvalidParameter	Wrong parameter.

Data structure

DirectConnect

Physical Leased Line Information List

Referenced by the following interfaces: DescribeDirectConnects

name	required	NULL allowed	type	description
DirectConnectId	yes	no	String	Physical DC ID Example: dc-psjiehij
DirectConnectName	yes	no	String	Physical DC Name Example: mock_dc
AccessPointId	yes	no	String	Access Point ID of Physical DC Example: ap-place-c-jxq
State	yes	no	String	Physical DC Status Applying: PENDING Application rejected: REJECTED Under construction: ALLOCATED Activated: AVAILABLE Deleting: DELETING Deleted: DELETED. Example: PENDINGPAY
CreatedTime	yes	no	String	Creation Time For Physical DC Example: 2020-12-08 16:57:43
EnabledTime	yes	no	String	Enablement Time for Physical DC Example: 2021-01-06 10:39:41
LineOperator	yes	no	String	ISPs providing access connection. Telecom: CTCC; Mobile: CMCC; Unicom: CUCC; In-houseWiring: in- house wiring; Other: others; InternationalOperator: others mainland. Example: In-houseWiring
Location	yes	no	String	Geographical Location of Local Data Center Example: UK
Bandwidth	yes	no	Int64	Physical DC interface bandwidth, in a unit of Mbps. Example: 1000
RedundantDirectConnectId	yes	no	String	Redundant Physical DC ID Example: dc-1234
CustomerName	yes	no	String	Name of physical DC applicant, obtained from account system by default. Example: Tom
CustomerContactMail	yes	no	String	E-mail address of physical DC applicant, obtained from account system by default. Example: 274907341@mail.com
CustomerContactNumber	yes	no	String	Contact number of physical DC applicant, obtained from account system by default. Example: 15802738654
FaultReportContactPerson	yes	no	String	Fault Contact Example: Tom
FaultReportContactNumber	yes	yes	String	Fault Reporting Contact Number Example: 15802738654
IdcCity	yes	no	String	City Where IDC Locates Example: place

name	required	NULL allowed	type	description
CloudPortType	yes	no	String	Cloud Side Port Type Example: 100Base-T
ApplyId	yes	no	Uint64	Application ID Example: 130000000301
IsShare	no	no	Bool	Whether to Share Example: True
DcOwnerUin	no	no	String	DC Provider Account Example: 130000000301
TunnelCount	no	no	Uint64	Private Channel Quantity Example: 100
AppId	no	no	Uint64	DC AppId Example: 130000000301

AccessPoint

Access Point Information

Referenced by the following interfaces: DescribeAccessPoints

name	required	NULL allowed	type	description
AccessPointName	yes	no	String	Access Point Name Example: Central-A-West Region
AccessPointId	yes	no	Int64	Unique ID of Access Point Example: 100
State	yes	no	String	Access point status: AVAILABLE and UNAVAILABLE. Example: AVAILABLE
Location	yes	no	String	Address of Data Center Where Access Point Locates Example: Central Telecom West Region 803DC
LineOperator	yes	no	Array of String	List of Access Point Supported ISPs Example: ["Telecom"]
AvailableBandwidthRatio	yes	no	Uint64	Bandwidth Percentage Available for Access Point Example: 100
CurrentBandwidth	yes	no	Uint64	Current used bandwidth, unit: MBytes. Example: 100
NotifyBandwidthRatio	yes	no	Uint64	Bandwidth Alarm Ratio Example: 100
TotalBandwidth	yes	no	Uint64	Total bandwidth of access points, unit: MBytes. Example: 100
City	yes	no	String	City Where IDC Locates Example: place
CloudPortType	yes	no	Array of String	User-side access port type of the physical DC, values: 100 Base-T: Fast Ethernet, 1000 Base-T (default value): Gigabit Ethernet, 1000 Base-LX: Gigabit Single-Mode Fiber (10 km), 10 GBase-T: 10 Gigabit Ethernet 10 GBase-LR: 10 Gigabit Single-Mode Fiber (10 km), default value, Gigabit Single-Mode Fiber (10 km). Example: 100Base-T

name	required	NULL allowed	type	description
IdcPortType	yes	no	Array of String	Physical DC IDC side access port type, values: 100 Base-T: Fast Ethernet, 1000 Base-T (default value): Gigabit Ethernet, 1000 Base-LX: Gigabit single-mode fiber (10 km), 10 GBase-T: 10 Gigabit Ethernet 10 GBase-LR: 10 Gigabit single-mode fiber (10 km), default value, Gigabit single-mode fiber (10 km). Example: 100Base-T
Region	yes	no	String	Region Example: 50001000

DirectConnectTunnel

Private Channel Information List

Referenced by the following interfaces: DescribeDirectConnectTunnels

name	required	NULL allowed	type	description
DirectConnectTunnelId	yes	no	String	Private Channel ID Example: dcx-r3sml04o
DirectConnectId	yes	no	String	Connection ID Example: dc-9s5kpgyp
State	yes	no	String	Private Channel Status AVAILABLE: Ready APPLYING: Applying ALLOCATING: Configuration in progress ALLOCATED: Configuration completed ALTERING: Modifying DELETING: Deleting DELETED: Deletion completed PENDING: Pending acceptance REJECTED: Rejected Example: PENDING
DirectConnectOwnerAppId	yes	no	Int64	DC owner, developer account ID. Example: 130000000301
NetworkType	yes	no	String	Network type. VPC: Virtual Private Cloud. Example: VPC
VpcId	yes	no	String	Unified VPC ID. Example: vpc-aipqhdez
DirectConnectGatewayId	yes	no	String	Direct connect gateway ID Example: dcg-r70hz833
RouteType	yes	no	String	BGP: BGP routing; STATIC: Static. Example: STATIC
IdcRoutes	yes	yes	Array of String	User-Side Network Segment Address Example: 10.0.0.0/16
Vlan	yes	no	Int64	VLAN of Private Channel Example: 100
CloudAddress	yes	no	String	Cloud-Side Interconnect IP Example: 10.10.10.10
CustomerAddress	yes	no	String	User-Side Interconnect IP Example: 169.254.64.2/29
DirectConnectTunnelName	yes	no	String	Private Channel Name Example: dc_name

name	required	NULL allowed	type	description
CreatedTime	yes	no	String	Private Channel Creation Time Example: 2018-06-01 14:59:16
Bandwidth	yes	no	Int64	Bandwidth Value of Private Channel Example: 1000
NetDetectId	yes	yes	String	Associated Network Custom Probe ID Example: 100
NatType	yes	yes	Bool	Whether it is a Nat channel. Example: True
VpcRegion	yes	yes	String	Region Where VPC Connected by Channel Locates Example: gz
BfdState	yes	yes	String	BFD status: DISABLED: Off ENABLE: On UP: Healthy DOWN: Abnormal Example: 0
DirectConnectGatewayName	yes	yes	String	Direct Connect Gateway Name Example: Test gateway.
VpcName	yes	yes	String	VPC Name Example: Test VPC.
EnableMulticast	yes	yes	Bool	True: Enabled; False: Disabled. Example: True
MulticastGroups	yes	yes	String	Multicast Group Supported Under Channel Example: 224.0.2.2
AppId	yes	no	Int64	Private channel owner, developer account ID. Example: 130000000301
LoadMode	yes	no	String	Channel CLB modes: 0: None; 1: LoadBalance; and 2: MasterSlave. Example: LoadBalance
ConnectSubnetMask	yes	no	Uint64	Interconnection Address Mask Example: 16
DirectConnectOwnerUin	yes	no	Int64	Leased Line Owner Account UIN Example: 130000000301
BfdInterval	yes	no	Uint64	Interval Field Value in BFD Protocol Example: 100
RelatedDirectConnectTunnelId	yes	yes	String	Associated Channel ID Example: dcx-2j1x1udk
Comments	yes	yes	String	Channel Remarks Example: Comments
MasterStatus	no	yes	Bool	In a primary/secondary mode, whether the channel is primary. Example: True
RegionStatus	yes	yes	Int64	Used for determining same region, across regions within mainland, cross-border Example: 0

name	required	NULL allowed	type	description
SupportBfd	yes	yes	Bool	Whether to Support BFD Example: True
DirectConnectTunnelOwnerUin	yes	yes	Int64	Private Channel Owner Account UIN Example: 130000000301
BgpPeer	no	yes	BgpPeer	BgpPeer, user-side BGP information, including ASN and AuthKey. Example:View
IpType	no	no	String	Channel IP Protocol Type Example: v4
ShareMode	yes	no	Bool	Whether it is a shared channel. Example: True
AccessPointId	yes	no	String	DC Point ID Example: 100
DirectConnectName	no	no	String	Physical Leased Line Name Example: dc-dfas

Filter

Used for conditional filtering queries.

Referenced by the following interfaces: DescribeAccessPoints, DescribeDirectConnectTunnels, DescribeDirectConnects

name	required	NULL allowed	type	description
Name	yes	no	String	Field Needing To Be Filtered Example: Name
Values	yes	no	Array of String	Filter Value of Field Example: mock_name

BgpPeer

BGP Parameters, including ASN, AuthKey.

Referenced by the following interfaces: CreateDirectConnectTunnel, DescribeDirectConnectTunnels, ModifyDirectConnectTunnelAttribute

name	required	NULL allowed	type	description
Asn	no	no	Int64	User side, BGP ASN. Example: 100
AuthKey	no	no	String	User-Side BGP Key Example: bgp_key

IspInfo

ISP details

Referenced by the following interfaces: DescribeIsp

name	required	NULL allowed	type	description
IspId	no	no	Int64	ISP ID Example: 100
IspName	no	no	String	ISP Other name Example: place

name	required	NULL allowed	type	description
IspInternationalName	no	no	String	ISP English name Example: place

ErrorCode

Feature Description

If there is an Error field in the response, it means that the API call failed. For example:

```
{
    "Response": {
        "Error": {
            "Code": "AuthFailure.SignatureFailure",
            "Message": "The provided credentials could not be validated. Please check your signature is cor
rect."
        },
        "RequestId": "ed93f3cb-f35e-473f-b9f3-0d451b8b79c6"
    }
}
```

Code in Error indicates the error code, and Message indicates the specific information of the error.

Error Code List

Common Error Codes

Error codes	Description
AuthFailure.InvalidSecretId	Invalid key (not a Cloud API key type).
AuthFailure.MFAFailure	MFA failed.
AuthFailure.SecretIdNotFound	Key does not exist. Check if the key has been deleted or disabled in the console, and if not, check if the key is correctly entered. Note that whitespaces should not exist before or after the key.
AuthFailure.SignatureExpire	Signature expired. Timestamp and server time cannot differ by more than five minutes. Please ensure your current local time matches the standard time.
AuthFailure.SignatureFailure	Invalid signature. Signature calculation error. Please ensure you've followed the signature calculation process described in the Signature API documentation.
AuthFailure.TokenFailure	Token error.

Error codes	Description
AuthFailure.UnauthorizedOperation	The request does not have CAM authorization.
DryRunOperation	DryRun Operation. It means that the request would have succeeded, but the DryRun parameter was used.
FailedOperation	Operation failed.
InternalError	Internal error.
InvalidAction	The API does not exist.
InvalidParameter	Incorrect parameter.
InvalidParameterValue	Invalid parameter value.
LimitExceeded	Quota limit exceeded.
MissingParameter	A parameter is missing.
NoSuchVersion	The API version does not exist.
RequestLimitExceeded	The number of requests exceeds the frequency limit.
ResourceInUse	Resource is in use.
ResourceInsufficient	Insufficient resource.
ResourceNotFound	The resource does not exist.
ResourceUnavailable	Resource is unavailable.
UnauthorizedOperation	Unauthorized operation.
UnknownParameter	Unknown parameter.
UnsupportedOperation	Unsupported operation.
UnsupportedProtocol	HTTPS request method error. Only GET and POST requests are supported.
UnsupportedRegion	API does not support the requested region.

Service Error Codes

Error codes	Description
InvalidParameter.ArAvailBandwidthNotEnough	The available bandwidth is insufficient at the DC access point.

Error codes	Description
InvalidParameter.DirectConnectIdIsNotUin	The physical DC does not belong to this account.
InvalidParameter	Wrong parameter.
ResourceUnavailable.InsufficientBalance	Sorry, your account is overdue. Products cannot be activated in an overdue status. Please recharge first.
InvalidParameterValue.VlanConfLict	VLAN Conflict
LimitExceeded.DirectConnectTunnelLimitExceeded	Number of dedicated channels for the physical DC has reached a limit.
InvalidParameter.AddressError	Interconnect IP Error
InvalidParameterValue	Incorrect parameter value
ResourceInUse.DcVpcIsExist	The VPC for the physical DC already exists.
UnauthorizedOperation	Unauthorized operation
InvalidParameter.DcBandwidthOutOfRange	Physical DC bandwidth is out of range. Physical DC bandwidth is required to be greater than 1, not less than the maximum bandwidth of the private channel, not greater than the port bandwidth, and not less than a sum of private channel bandwidths in a non-overselling mode.
LimitExceeded.DirectConnectLimitExceeded	Number of physical DCs has reached a limit.
InternalError	Internal error
ResourceNotFound	The resource does not exist.
InvalidParameter.DcResourceNotFound	The direct connection resource does not exist.
ResourceUnavailable	Resource unavailable
FailedOperation	Operation Failed
UnsupportedOperation.CrossBorderDirectConnectTunnel	Creating cross-border dedicated channels is not allowed. Please contact us.

Error codes	Description
InvalidParameter.DcxBandwidthOutOfRange	Physical DC bandwidth is out of range. Private channel bandwidth is required to be greater than 1, and not greater than the physical DC bandwidth, and a sum of private channel bandwidths is not greater than the physical DC bandwidth in a non-overselling mode.
LimitExceeded	Exceeded quota limit
InvalidParameter.PortBandwidthMismatch	Port bandwidths of the cloud side and the IDC side mismatch.
ResourceNotFound.DirectConnectTunnelIdIsNotExist	Dedicated channel does not exist.
UnsupportedOperation.StateConfLict	Status Conflict
InvalidParameter.InvalidIpMulticastConfig	An error in IP multicast configuration occurs.
MissingParameter	Parameter missing
InvalidParameter.UinIsNotExist	This account ID does not exist.
UnsupportedOperation	Operation unsupported.