Direct Connect

User Guide

Date **2020-02-26**

Contents

1 Service Overview

1.1 Overview

What Is Direct Connect?

Direct Connect establishes a dedicated connection between your data center and the cloud. You can use one connection to access cloud computing resources in different regions, helping build a secure and reliable hybrid environment.

Application Scenarios

You need a dedicated network connection between your data center and a Virtual Private Cloud (VPC) to ensure high bandwidth, low latency, and robust security.

Components

There are three key components for you to use Direct Connect: connection, virtual gateway, and virtual interface.

- **Connection**

  A connection is a dedicated network connection between your on-premises data center and a Direct Connect location over a leased line provided by a carrier. You can request standard connections or hosted connections. If you are a partner, you can also request operations connections.

  A standard connection provides a port that is exclusive to you and allows you to have multiple virtual interfaces associated.

  A hosted connection allows multiple users to share one port. Partners provision hosted connections and specify VLANs for those connections. Each user can associate only one virtual interface with a hosted connection. If a partner has created an operations connection, you can request a hosted connection from the partner, who will allocate the VLAN and bandwidth to your hosted connection.

- **Virtual gateway**

  A virtual gateway is a logical gateway for accessing a VPC. A virtual gateway can be associated with only one VPC. If you have multiple connections, you

can associate one virtual gateway to these connections to access the same VPC.

- **Virtual interface**

  A virtual interface is an entrance for you to access VPCs through a leased line. A virtual interface associates your connection with a virtual gateway, which connects to a VPC so that your network can access the cloud.

Advantages

- High security

  You can use Direct Connect to connect to VPCs. Direct Connect provides a dedicated channel for communication, and this channel is isolated from other networks, ensuring the security.

- Low latency

  A dedicated network is used for data transmission, which brings high network performance, low latency, and excellent user experience.

- High bandwidth

  A connection supports a maximum of 10 Gbit/s bandwidth, meeting various requirements.

- Seamless resource expansion

  You can use Direct Connect to connect your data center to the resources in the cloud, which enables you to deploy a hybrid cloud in a flexible and scalable manner.

1.2 Product Advantages

Direct Connect has the following advantages:

- **High security**

  Direct Connect establishes private connectivity between your premises and one or more VPCs while maintaining network isolation between different workloads.

- **Low latency**

  A dedicated network is used for data transmission, which brings high network performance, low latency, and excellent user experience.

- **High bandwidth**

  A single connection supports up to 10 Gbit/s bandwidth, meeting your connectivity needs today and tomorrow.

- **Great scalability**

  By connecting your on-premises network to the cloud, you gain access to virtually unlimited cloud resources for flexible, scalable hybrid deployment.

1.3 Network Requirements

- Your network must use a single-mode fiber with a 1GE or 10GE optical module to connect to the access device in the cloud.

- Auto-negotiation for the port must be disabled.
- Port speed and full-duplex mode must be manually configured.
- 802.1Q VLAN encapsulation must be supported on the entire connection, including intermediate devices.
- Your device must support Border Gateway Protocol (BGP) and authentication using MD5 Message-Digest Algorithm (MD5).
- (Optional) You can configure Bidirectional Forwarding Detection (BFD) on the network.
- The maximum transmission unit (MTU) supported at the physical layer is 1522 bytes (14-byte Ethernet header + 4-byte VLAN tag + 1500-byte IP datagram + 4-byte frame check sequence).
- Private IP addresses are recommended on the cloud, and network segments for interworking cannot conflict with each other.

1.4 Quotas

Resource	Quota	Remarks
Number of connections that can be created for an account in each region	10	The quota cannot be increased.
Number of virtual interfaces that can be created for an account in each region	50	The quota cannot be increased.
Number of routes for BGP sessions on a virtual interface	100	To increase the quota, submit a service ticket.
Number of static routes on a virtual interface	50	To increase the quota, submit a service ticket.

1.5 Permissions Management

If you need to assign different permissions to employees in your enterprise to access your Direct Connect resources, Identity and Access Management (IAM) is a good choice for fine-grained permissions management. IAM provides identity authentication, permissions management, and access control, helping you secure access to your resources.

With IAM, you can use your account to create IAM users, and assign permissions to the users to control their access to specific resources. For example, some software developers in your enterprise need to use Direct Connect but should not be allowed to delete other Direct Connect resources or perform any other high-risk operations. In this scenario, you can create IAM users for the software developers and grant them only the required permissions.

Skip this part if your account does not require individual IAM users for permissions management.

IAM is free. You pay only for the resources in your account.

For more information, see **IAM Service Overview**.

Direct Connect Permissions

By default, new IAM users do not have permissions assigned. You need to add a user to one or more groups, and attach permissions policies or roles to these groups. Users inherit permissions from the groups to which they are added and can perform specified operations on cloud services based on the permissions.

Direct Connect is a project-level service deployed and accessed in specific physical regions. To assign permissions to a user group, specify the scope as region-specific projects and select projects for the permissions to take effect. If **All projects** is selected, the permissions will take effect for the user group in all region-specific projects. When accessing Direct Connect, the users need to switch to a region where they have been authorized to use this service.

Table 1-1 lists all system-defined roles supported by Direct Connect.

Table 1-1 Direct Connect roles

Role Name	Description	Type	Dependency
Direct Connect Administrator	Has all permissions for Direct Connect resources. For permissions of this role to take effect, users must also have the **Tenant Guest** and **VPC Administrator** permissions.	System-defined role	**Tenant Guest** and **VPC Administrator** • **VPC Administrator**: project-level policy, which must be assigned in the same project as the **Direct Connect Administrator** policy • **Tenant Guest**: project-level policy, which must be assigned in the same project as the **Direct Connect Administrator**

Table 1-2 lists common operations supported by each system-defined role or policy of Direct Connect.

Table 1-2 Common operations and required system-defined permissions

Operation	Direct Connect Administrator
Creating a connection	√

Operation	Direct Connect Administrator
Viewing a connection	√
Modifying a connection	√
Deleting a connection	√
Creating a virtual gateway	√
Viewing a virtual gateway	√
Modifying a virtual gateway	√
Deleting a virtual gateway	√
Creating a virtual interface	√
Viewing a virtual interface	√
Modifying a virtual interface	√
Deleting a virtual interface	√
Creating an operations connection	√
Viewing an operations connection	√
Modifying an operations connection	√
Deleting an operations connection	√
Creating a hosted connection	√
Viewing a hosted connection	√
Modifying a hosted connection	√
Deleting a hosted connection	√

Helpful Links

- **IAM Service Overview**
- **3.6.1 Creating a User and Granting Permissions**

1.6 Basic Concepts

1.6.1 Connection

A connection is a dedicated network connection between your on-premises data center and a Direct Connect location over a leased line provided by a carrier. You can request standard connections or hosted connections. If you are a partner, you can also request operations connections.

A standard connection provides a port that is exclusive to you and allows you to have multiple virtual interfaces associated.

A hosted connection allows multiple users to share one port. Partners provision hosted connections and specify VLANs for those connections. Each user can associate only one virtual interface with a hosted connection. If a partner has created an operations connection, you can request a hosted connection from the partner, who will allocate the VLAN and bandwidth to your hosted connection.

1.6.2 Virtual Gateway

A virtual gateway is a logical gateway for accessing a VPC. A virtual gateway can be associated with only one VPC. If you have multiple connections, you can associate one virtual gateway to these connections to access the same VPC.

1.6.3 Virtual Interface

A virtual interface is an entrance for you to access VPCs through a leased line. A virtual interface associates your connection with a virtual gateway, which connects to a VPC so that your network can access the cloud.

1.6.4 Region and AZ

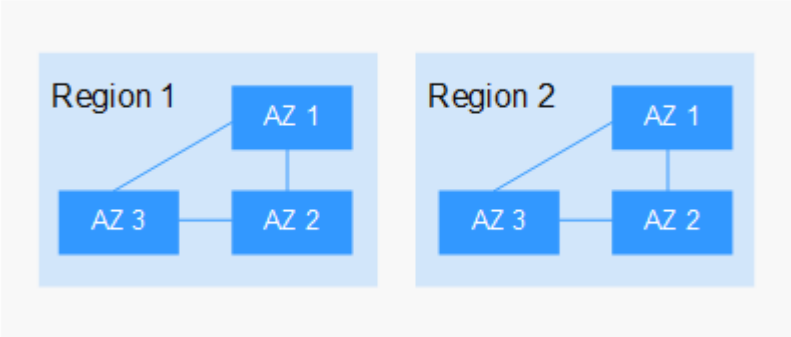
Concept

A region and availability zone (AZ) identify the location of a data center. You can create resources in a specific region and AZ.

- A region is a physical data center, which is completely isolated to improve fault tolerance and stability. The region that is selected during resource creation cannot be changed after the resource is created.
- An AZ is a physical location where resources use independent power supplies and networks. A region contains one or more AZs that are physically isolated but interconnected through internal networks. Because AZs are isolated from each other, any fault that occurs in one AZ will not affect others.

Figure 1-1 shows the relationship between regions and AZs.

Figure 1-1 Regions and AZs



Selecting a Region

Select a region closest to your target users for lower network latency and quick access.

Selecting an AZ

When deploying resources, consider your applications' requirements on disaster recovery (DR) and network latency.

- For high DR capability, deploy resources in different AZs within the same region.
- For lower network latency, deploy resources in the same AZ.

Regions and Endpoints

Before you use an API to call resources, specify its region and endpoint. For more details, see **Regions and Endpoints**.

2 Getting Started

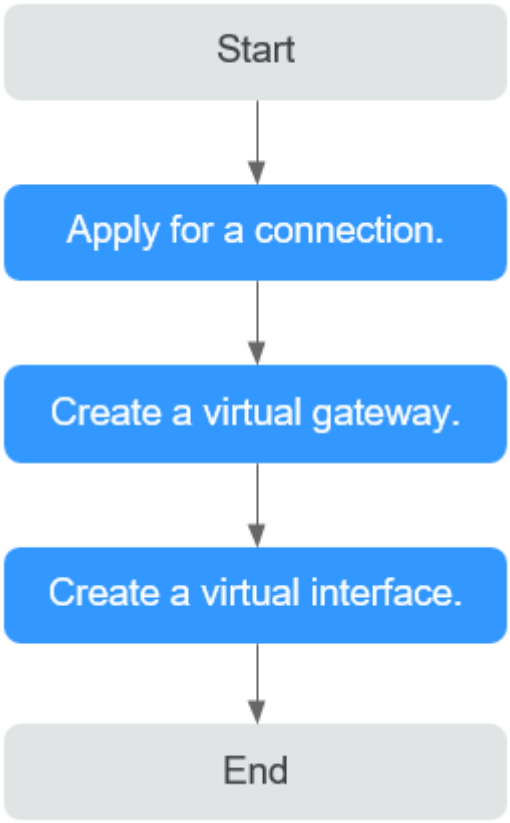
2.1 Process Description

Establish network connectivity to enable ECSs in your VPC to communicate with your data center or private network.

To do so, you first need to apply for a connection to book the port used to connect your data center to the location you select. After that, create a virtual gateway and associate it with a VPC, and finally create a virtual interface to connect to the VPC.

Figure 2-1 shows the whole process for connecting your on-premises data center to the cloud.

Figure 2-1 Enabling Direct Connect



2.2 Establishing Network Connectivity

Scenarios

Establish network connectivity using Direct Connect if cloud servers in your VPC need to communicate with your on-premises data center.

Procedure

1. Apply for a connection from your account manager. If you do not have an account manager, contact customer service.
2. Log in to the management console.
3. Under **Network**, click **Direct Connect**.
4. In the navigation pane on the left, choose **Direct Connect** > **Virtual Gateways**.
5. Click **Create Virtual Gateway**.
6. Configure parameters as prompted.

Table 2-1 Parameter description

Parameter	Description
Name	Specifies the virtual gateway name. The name can contain 1 to 64 characters, including letters, digits, underscores (_), hyphens (-), and periods (.).
VPC	Specifies the VPC to be associated with the virtual gateway.
Subnet CIDR Block	Specifies the CIDR blocks of subnets in the VPC to connect to the on-premises network.
Description	Provides supplementary information about the virtual gateway. You can enter 0 to 128 characters.

7. Click **OK**.
8. In the navigation pane on the left, choose **Direct Connect** > **Virtual Interfaces**.
9. Click **Create Virtual Interface**.
10. Set the parameters as prompted and then click **Create Now**.

Table 2-2 Parameter description

Parameter	Description
Region	Select the region of the VPC that needs to communicate with the on-premises data center.
Name	Specifies the virtual interface name. The name can contain 1 to 64 characters, including letters, digits, underscores (_), hyphens (-), and periods (.).
Connection	Specifies the connection with which the virtual interface is to be associated. A virtual interface can be associated with only one connection.
Virtual Gateway	Select the virtual gateway with which the virtual interface is to be associated. A virtual interface can be associated with only one virtual gateway.
VLAN	Specifies the virtual interface VLAN ID. You need to configure the VLAN if you create a standard connection. The VLAN of the virtual interface of the hosting private line uses the VLAN allocated by the carrier or partner for the hosting private line. You do not need to configure the VLAN.

Parameter	Description
Bandwidth	Specifies the virtual interface bandwidth in the unit of Mbit/s. If the selected connection is a hosted connection, the virtual interface exclusively uses the connection bandwidth.
Local Gateway	Specifies the IP address for connecting to the cloud network.
Remote Gateway	Specifies the IP address for connecting to your on-premises network.
Remote Subnet	Specifies the subnets used by the on-premises network. Specifies the remote subnet using CIDR notation. You can enter a maximum of 50 subnets. Ensure that each subnet is unique and separate every two subnets with commas (,).
Routing Mode	Specifies the routing mode. Two options are available, **Static** and **BGP**. If there are two or more connections, select BGP routing.
BGP ASN	Specifies the autonomous system number (ASN) of the BGP peer. 64512 cannot be used because it has been used by the cloud.
BGP MD5 Authentication Key	Specifies the message digest algorithm 5 (MD5) password of the BGP peer.
Description	Provides supplementary information about the virtual interface. You can enter 0 to 128 characters.

3 Management

3.1 Managing Connections

3.1.1 Viewing a Connection

Scenarios

View the details of a connection.

Procedure

1. Log in to the management console.
2. Under **Network**, click **Direct Connect**.
3. In the navigation pane on the left, choose **Direct Connect** > **Connections**.
4. Locate the connection and view its details.

3.1.2 Modifying a Connection

Scenarios

Modify the name and description of a connection.

Procedure

1. Log in to the management console.
2. Under **Network**, click **Direct Connect**.
3. In the navigation pane on the left, choose **Direct Connect** > **Connections**.
4. Locate the connection you want to modify and click **Modify** in the **Operation** column.
5. Modify the parameters and click **OK**.

3.2 Managing Virtual Gateways

3.2.1 Viewing a Virtual Gateway

Scenarios

View details of a virtual gateway.

Procedure

1. Log in to the management console.
2. Under **Network**, click **Direct Connect**.
3. In the navigation pane on the left, choose **Direct Connect** > **Virtual Gateways**.
4. Locate the virtual gateway you want to view and click before its name to view the details.

3.2.2 Modifying a Virtual Gateway

Scenarios

Modify the name, subnet CIDR block, and description of a virtual gateway.

Procedure

1. Log in to the management console.
2. Under **Network**, click **Direct Connect**.
3. In the navigation pane on the left, choose **Direct Connect** > **Virtual Gateways**.
4. Locate the virtual gateway you want to modify and click **Modify** in the **Operation** column.
5. Modify the parameters and click **OK**.

3.2.3 Deleting a Virtual Gateway

Scenarios

Delete a virtual gateway if you no longer need it. Before deleting the virtual gateway, you need to delete all associated virtual interfaces.

Procedure

1. Log in to the management console.
2. Under **Network**, click **Direct Connect**.
3. In the navigation pane on the left, choose **Direct Connect** > **Virtual Gateways**.

4. Locate the virtual gateway you want to delete and click **Delete** in the **Operation** column.
5. Click **Yes**.

3.3 Managing Virtual Interfaces

3.3.1 Viewing a Virtual Interface

Scenarios

View details of a virtual interface.

Procedure

1. Log in to the management console.
2. Under **Network**, click **Direct Connect**.
3. In the navigation pane on the left, choose **Direct Connect** > **Virtual Interfaces**.
4. Locate the virtual interface you want to view and click before its name to view the details.

3.3.2 Modifying a Virtual Interface

Scenarios

Modify the name, remote subnet, and description of a virtual interface.

Procedure

1. Log in to the management console.
2. Under **Network**, click **Direct Connect**.
3. In the navigation pane on the left, choose **Direct Connect** > **Virtual Interfaces**.
4. Locate the virtual interface you want to modify and click **Modify** in the **Operation** column.
5. Modify the parameters and click **OK**.

3.3.3 Deleting a Virtual Interface

Scenarios

Delete a virtual interface if you no longer need it.

Procedure

1. Log in to the management console.

2. Under **Network**, click **Direct Connect**.
3. In the navigation pane on the left, choose **Direct Connect** > **Virtual Interfaces**.
4. Locate the virtual interface you want to delete and click **Delete** in the **Operation** column.
5. Click **Yes**.

3.4 Managing Historical Connections

3.4.1 Viewing a Historical Connection

Scenarios

View the details of a connection that you requested through email or phone call.

Procedure

1. Log in to the management console.
2. Under **Network**, click **Direct Connect**.
3. In the navigation pane on the left, choose **Direct Connect** > **Historical Connections**.
4. Locate the connection you want to view and click ˅ before its name to view the details.

3.4.2 Modifying a Historical Connection

Scenarios

Modify the name and remote subnets of a historical connection.

Procedure

1. Log in to the management console.
2. Under **Network**, click **Direct Connect**.
3. In the navigation pane on the left, choose **Direct Connect** > **Historical Connections**.
4. Locate the connection you want to modify and click **Modify** in the **Operation** column.
5. Modify the parameters and click **OK**.

3.5 Managing Operations or Hosted Connections

3.5.1 Operations Connection

Viewing an Operations Connection

Scenarios

View details of an operations connection you created as a partner.

Procedure

1. Log in to the management console.
2. Under **Network**, click **Direct Connect**.
3. In the navigation pane on the left, choose **Direct Connect** > **Connections**.
4. Locate the operations connection you want to view and click its name.
5. View detailed information about the operations connection.

Modifying an Operations Connection

Scenarios

Modify an operations connection you created as a partner.

Procedure

1. Log in to the management console.
2. Under **Network**, click **Direct Connect**.
3. In the navigation pane on the left, choose **Direct Connect** > **Connections**.
4. Locate the operations connection you want to modify, click **Modify** in the **Operation** column.
5. Modify the parameters and then click **OK**.

3.5.2 Hosted Connection

Viewing a Hosted Connection

Scenarios

View the details of a hosted connection you created as a partner.

Procedure

1. Log in to the management console.
2. Under **Network**, click **Direct Connect**.
3. In the navigation pane on the left, choose **Direct Connect** > **Connections**.
4. Locate the operations connection on which the hosted connection is created and click **Manage Hosted Connection** in the **Operation** column.
5. Locate the hosted connection you want to view and click ⌄ before its name to view the details.

Modifying a Hosted Connection

Scenarios

Modify the name, bandwidth, and description of a hosted connection you created as a partner.

Procedure

1. Log in to the management console.
2. Under **Network**, click **Direct Connect**.
3. In the navigation pane on the left, choose **Direct Connect** > **Connections**.
4. Locate the operations connection on which the hosted connection is created and click **Manage Hosted Connection** in the **Operation** column.
5. Locate the hosted connection you want to modify and click **Modify** in the **Operation** column.
6. Modify the parameters and click **OK**.

3.6 Permissions

3.6.1 Creating a User and Granting Permissions

Use **IAM** to implement fine-grained permissions control over your Direct Connect resources. With IAM, you can:

- Create IAM users for employees based on the organizational structure of your enterprise. Each IAM user has their own security credentials, providing access to cloud resources.
- Grant only the permissions required for users to perform a specific task.
- Entrust another account or cloud service to perform professional and efficient O&M on your cloud resources.

Skip this part if your account does not require individual IAM users.

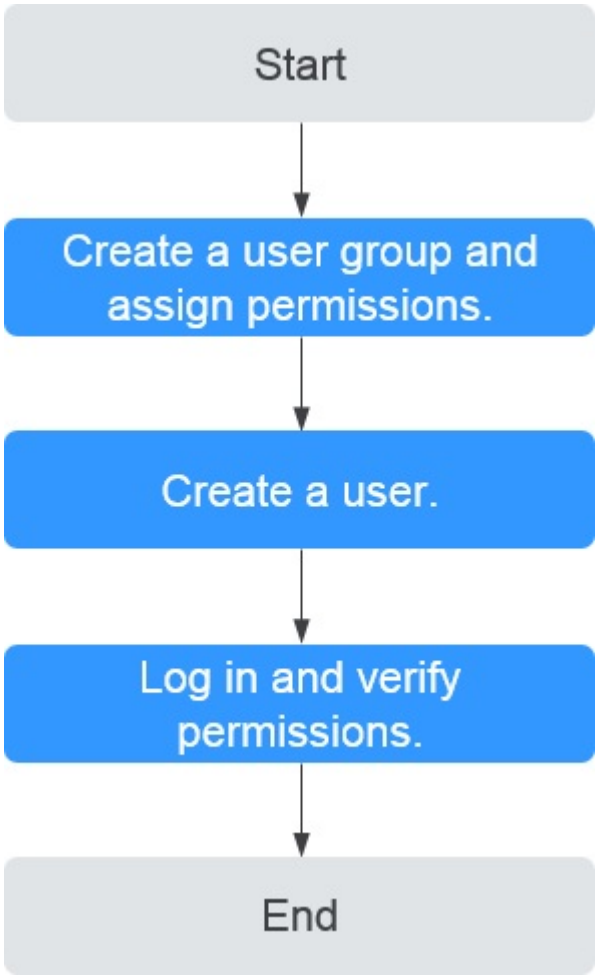
The following is the procedure for granting permissions.

Prerequisites

Before assigning permissions to user groups, you should learn about Direct Connect system policies and select the policies based on service requirements. For details about system permissions of Direct Connect, see **1.5 Permissions Management**. For system permissions of other cloud services, see **Permission Description**.

Process Flow

Figure 3-1 Process for granting Direct Connect permissions



1. **Create a user group and grant permissions**.

   Create a user group on the IAM console and attach the **Direct Connect Administrator** policy to the group, which grants users read-only permissions to Direct Connect resources.

2. **Create a user and add the user to the user group** created in the preceding step.

3. **Log in to the management console as the created user**.

   Switch to the authorized region and verify the permissions.

   - Choose **Service List** > **Network** > **Direct Connect**. On the displayed page, click **Create Connection**. If the connection fails to be created, the **Direct Connect Administrator** policy has taken effect.
   - Choose any other service in **Service List**. If a message appears indicating that you have insufficient permissions to access the service, the **Direct Connect Administrator** policy has already taken effect.

3.7 Quotas

What Is Quota?

Quotas are enforced for service resources on the platform to prevent unforeseen spikes in resource usage. Quotas can limit the number or amount of resources available to users, such as the maximum number of ECSs or EVS disks that can be created.

If the existing resource quota cannot meet your service requirements, you can apply for a higher quota.

How Do I View My Quotas?

1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. In the upper right corner of the page, click  .

   The **Service Quota** page is displayed.
4. View the used and total quota of each type of resources on the displayed page.

   If a quota cannot meet service requirements, apply for a higher quota.

How Do I Apply for a Higher Quota?

The system does not support online quota adjustment. If you need to adjust a quota, call the hotline or send an email to the customer service mailbox. Customer service personnel will timely process your request for quota adjustment and inform you of the real-time progress by making a call or sending an email.

Before dialing the hotline number or sending an email, make sure that the following information has been obtained:

- Account name, project name, and project ID, which can be obtained by performing the following operations:

  Log in to the management console using the cloud account, click the username in the upper right corner, select **My Credentials** from the drop-down list, and obtain the account name, project name, and project ID on the **My Credentials** page.
- Quota information, which includes:
  - Service name
  - Quota type
  - Required quota

Learn how to obtain the service hotline and email address.

4 Best Practices

4.1 Accessing a VPC over a Connection That Uses Static Routing

Solution Overview

Connect your on-premises network to the cloud through a connection that uses static routing so that your on-premises network can access the VPCs.

Prerequisites

- Your on-premises network uses a single-mode fiber with a 1GE or 10GE optical module to connect to the network device used by the cloud.
- Auto-negotiation for the port has been disabled, and port speed and full-duplex mode have been manually configured.
- 802.1Q VLAN encapsulation is supported on your on-premises network.

Network Topology

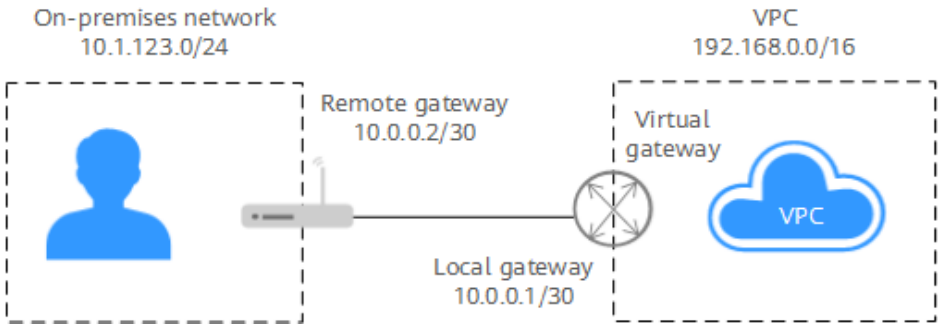
Your on-premises network is connected to a VPC in the **ru-moscow** region over a a single connection. For details about how to create a VPC, see the **Virtual Private Cloud User Guide**.

Table 4-1 lists the CIDR blocks involved in this solution.

Table 4-1 CIDR blocks

Item	CIDR Block
Your on-premises network	10.1.123.0/24
Remote and local gateways	10.0.0.0/30
VPC	192.168.0.0/16

Figure 4-1 Accessing a VPC over a connection that uses static routing



Procedure

Step 1 Apply for a connection.

1. Apply for a connection from your account manager. If you do not have an account manager, contact customer service.
2. Log in to the management console.
3. On the console homepage, click  in the upper left corner and select the desired region and project.
4. Hover on  to display **Service List** and choose **Network** > **Direct Connect**.
5. In the navigation pane on the left, choose **Direct Connect** > **Connections**.
6. On the **Connections** page, view the connection you have applied for.

Step 2 Create a virtual gateway.

1. In the navigation pane on the left, choose **Direct Connect** > **Virtual Gateways**.
2. Click **Create Virtual Gateway**.
3. Configure the parameters based on **Table 4-2**.

Figure 4-2 Creating a virtual gateway

Table 4-2 Parameter description

Parameter	Description	Example Value
Name	Specifies the virtual gateway name. The name can contain 1 to 64 characters.	vgw-test
VPC	Specifies the VPC you want to access using the connection.	VPC-001
Subnet CIDR Block	Specifies CIDR blocks of the VPC subnets. You can enter one or more CIDR blocks and separate every entry with a comma (,).	192.168.0.0/16
Description	Provides supplementary information about the virtual gateway.	N/A

4. Click **OK**.

Step 3 Create a virtual interface.

1. In the navigation pane on the left, choose **Direct Connect** > **Virtual Interfaces**.
2. Click **Create Virtual Interface**.
3. Configure the parameters based on **Table 4-3**.

Figure 4-3 Creating a virtual interface

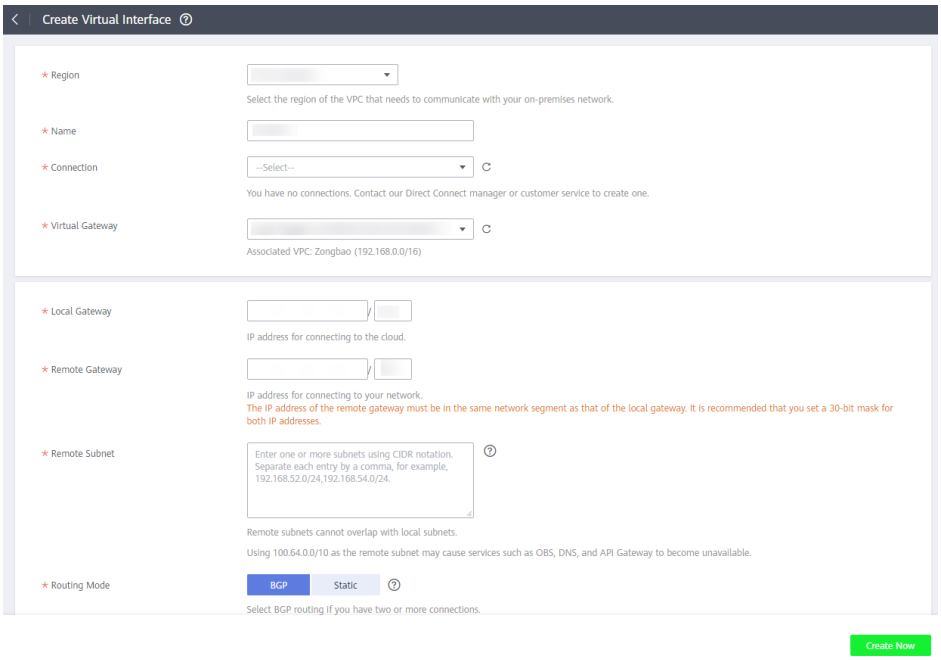


Table 4-3 Parameter description

Parameter	Description	Example Value
Region	Specifies the region where the connection resides. You can change the region in the upper left corner of the console.	ru-moscow
Name	Specifies the virtual interface name. The name can contain 1 to 64 characters.	vif-test
Connection	Specifies the connection you use to connect your on-premises network to the cloud.	dc-test12
Virtual Gateway	Specifies the virtual gateway to which the virtual interface will connect.	vgw-test
VLAN	Specifies the virtual interface VLAN ID. You need to configure the VLAN if you create a standard connection. The VLAN of the virtual interface of the hosting private line uses the VLAN allocated by the carrier or partner for the hosting private line. You do not need to configure the VLAN.	30
Bandwidth	Specifies the bandwidth that can be used by the virtual interface, in Mbit/s. The bandwidth cannot exceed that of the connection.	1,000 Mbit/s
Local Gateway	Specifies the IP address used for connecting to the cloud.	10.0.0.1/30

Parameter	Description	Example Value
Remote Gateway	Specifies the IP address for connecting to your on-premises network. The remote gateway must be in the same IP address range as the local gateway. Generally, a subnet with a 30-bit mask is recommended.	10.0.0.2/30
Remote Subnet	Specifies the subnets of your on-premises network. Separate every entry with a comma (.).	10.1.123.0/24
Routing Mode	Specifies the routing mode. Two options are available, static routing and BGP routing.	Static
Description	Provides supplementary information about the virtual interface.	N/A

Step 4 Wait for route advertisement on the cloud.

The network device used on the cloud automatically advertises the routes after you complete all configurations on the management console.

Step 5 Advertise the routes on your on-premises network.

Example routes (on a third-party device)

ip route-static 192.168.0.0 255.255.0.0 10.0.0.1

----End

4.2 Accessing a VPC over a Connection That Uses Dynamic Routing

Solution Overview

Connect your on-premises network that uses dynamic routing so that your on-premises network can access the VPCs.

Prerequisites

- Your on-premises network uses a single-mode fiber with a 1GE or 10GE optical module to connect to the network device used by the cloud.
- Auto-negotiation for the port has been disabled, and port speed and full-duplex mode have been manually configured.
- 802.1Q VLAN encapsulation is supported on your on-premises network.
- Your device supports BGP and does not use ASN 64512, which is used by the cloud.

Network Topology

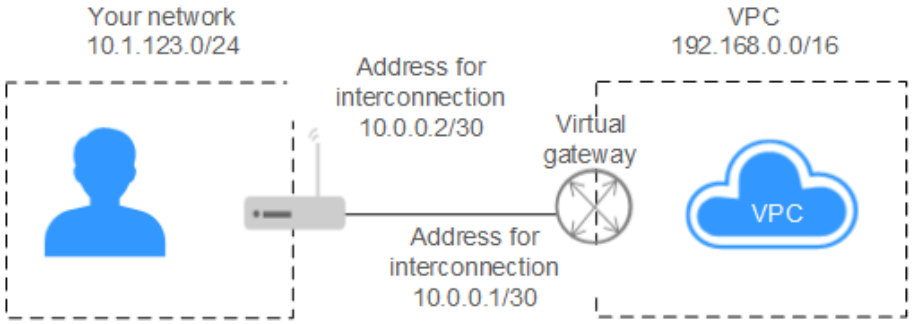
Your on-premises network is connected to a VPC in the **ru-moscow** region over a a single connection. For details about how to create a VPC, see the **Virtual Private Cloud User Guide**.

Table 4-4 lists the CIDR blocks involved in this solution.

Table 4-4 CIDR blocks

Item	CIDR Block
Your on-premises network	10.1.123.0/24
Remote and local gateways	10.0.0.0/30
VPC	192.168.0.0/16

Figure 4-4 Accessing a VPC over a connection that uses BGP routing



Procedure

Step 1 Apply for a connection.

1. Apply for a connection from your account manager. If you do not have an account manager, contact customer service.
2. Log in to the management console.
3. On the console homepage, click in the upper left corner and select the desired region and project.
4. Hover on to display **Service List** and choose **Network** > **Direct Connect**.
5. In the navigation pane on the left, choose **Direct Connect** > **Connections**.
6. On the **Connections** page, view the connection you have applied for.

Step 2 Create a virtual gateway.

1. In the navigation pane on the left, choose **Direct Connect** > **Virtual Gateways**.
2. Click **Create Virtual Gateway**.
3. Configure the parameters based on **Table 4-5**.

Figure 4-5 Creating a virtual gateway

Table 4-5 Parameter description

Parameter	Description	Example Value
Name	Specifies the virtual gateway name. The name can contain 1 to 64 characters.	vgw-test
VPC	Specifies the VPC you want to access using the connection.	VPC-001
Subnet CIDR Block	Specifies CIDR blocks of the VPC subnets. You can enter one or more CIDR blocks and separate every entry with a comma (,).	192.168.0.0/16
Description	Provides supplementary information about the virtual gateway.	N/A

4. Click **OK**.

Step 3 Create a virtual interface.

1. In the navigation pane on the left, choose **Direct Connect** > **Virtual Interfaces**.
2. Click **Create Virtual Interface**.
3. Configure the parameters based on **Table 4-6**.

Figure 4-6 Creating a virtual interface

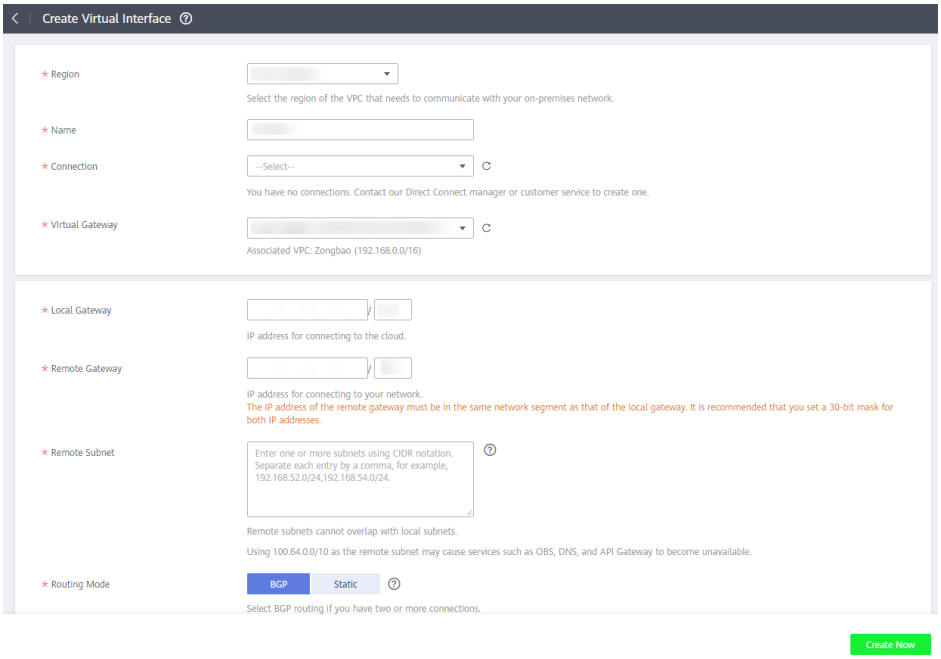


Table 4-6 Parameter description

Parameter	Description	Example Value
Region	Specifies the region where the connection resides. You can change the region in the upper left corner of the console.	ru-moscow
Name	Specifies the virtual interface name. The name can contain 1 to 64 characters.	vif-test
Connection	Specifies the connection you use to connect your on-premises network to the cloud.	dc-test12
Virtual Gateway	Specifies the virtual gateway to which the virtual interface will connect.	vgw-test
VLAN	Specifies the virtual interface VLAN ID. You need to configure the VLAN if you create a standard connection. The VLAN of the virtual interface of the hosting private line uses the VLAN allocated by the carrier or partner for the hosting private line. You do not need to configure the VLAN.	30
Bandwidth	Specifies the bandwidth that can be used by the virtual interface, in Mbit/s. The bandwidth cannot exceed that of the connection.	1,000 Mbit/s

Parameter	Description	Example Value
Local Gateway	Specifies the IP address used for connecting to the cloud.	10.0.0.1/30
Remote Gateway	Specifies the IP address for connecting to your on-premises network. The remote gateway must be in the same IP address range as the local gateway. Generally, a subnet with a 30-bit mask is recommended.	10.0.0.2/30
Remote Subnet	Specifies the subnets of your on-premises network. Separate every entry with a comma (.).	10.1.123.0/24
Routing Mode	Specifies the routing mode. Two options are available, static routing and BGP routing.	BGP
BGP ASN	Specifies the ASN of the BGP peer. This parameter is required when you select **BGP** for **Routing Mode**. 64512 cannot be used because it has been used by the cloud.	64510
BGP MD5 Authentication Key	Specifies the password used to authenticate the BGP peer using MD5. This parameter is required when you select **BGP** for **Routing Mode**.	1234567
Description	Provides supplementary information about the virtual interface.	N/A

Step 4 Wait for route advertisement on the cloud.

The network device used on the cloud automatically advertises the routes after you complete all configurations on the management console.

Step 5 Advertise the routes on your on-premises network.

Example routes (on a third-party device)

bgp 64510

peer 10.0.0.1 as-number 64512

peer 10.0.0.1 password simple 1234567

network 10.1.123.0 255.255.255.0

----End

5 FAQs

5.1 Is BGP Routing Supported in Direct Connect?

Yes. Direct Connect allows you to use BGP for routing.

5.2 What Are the Network Requirements for Connections?

- Your network must use a single-mode fiber with a 1GE or 10GE optical module to connect to the access device in the cloud.
- Auto-negotiation for the port must be disabled. Port speed and full-duplex mode must be manually configured.
- 802.1Q VLAN encapsulation must be supported on the entire connection, including intermediate devices.
- Your device must support Border Gateway Protocol (BGP) and BGP MD5 authentication.
- (Optional) You can configure Bidirectional Forwarding Detection (BFD) on the network.
- The maximum transmission unit (MTU) supported at the physical layer is 1522 bytes (14-byte Ethernet header + 4-byte VLAN tag + 1500-byte IP datagram + 4-byte frame check sequence).
- Private IP addresses are recommended on the cloud, and network segments for interworking cannot conflict with each other.

6 Change History

Release On	Description
2020-02-26	This issue is the first official release.