ALIBABA CLOUD

Alibaba Cloud

Data Transmission Service

Network Setup

Document Version: 20201009

Alibaba Cloud

Legal disclaimer

Alibaba Cloud reminds you to carefully read and fully understand the terms and conditions of this legal disclaimer before you read or use this document. If you have read or used this document, it shall be deemed as your total acceptance of this legal disclaimer.

1. You shall download and obtain this document from the Alibaba Cloud website or other Alibaba Cloud-authorized channels, and use this document for your own legal business activities only. The content of this document is considered confidential information of Alibaba Cloud. You shall strictly abide by the confidentiality obligations. No part of this document shall be disclosed or provided to any third party for use without the prior written consent of Alibaba Cloud.

2. No part of this document shall be excerpted, translated, reproduced, transmitted, or disseminated by any organization, company or individual in any form or by any means without the prior written consent of Alibaba Cloud.

3. The content of this document may be changed because of product version upgrade, adjustment, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and an updated version of this document will be released through Alibaba Cloud-authorized channels from time to time. You should pay attention to the version changes of this document as they occur and download and obtain the most up-to-date version of this document from Alibaba Cloud-authorized channels.

4. This document serves only as a reference guide for your use of Alibaba Cloud products and services. Alibaba Cloud provides this document based on the "status quo", "being defective", and "existing functions" of its products and services. Alibaba Cloud makes every effort to provide relevant operational guidance based on existing technologies. However, Alibaba Cloud hereby makes a clear statement that it in no way guarantees the accuracy, integrity, applicability, and reliability of the content of this document, either explicitly or implicitly. Alibaba Cloud shall not take legal responsibility for any errors or lost profits incurred by any organization, company, or individual arising from download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, take responsibility for any indirect, consequential, punitive, contingent, special, or punitive damages, including lost profits arising from the use or trust in this document (even if Alibaba Cloud has been notified of the possibility of such a loss).

5. By law, all the contents in Alibaba Cloud documents, including but not limited to pictures, architecture design, page layout, and text description, are intellectual property of Alibaba Cloud and/or its affiliates. This intellectual property includes, but is not limited to, trademark rights, patent rights, copyrights, and trade secrets. No part of this document shall be used, modified, reproduced, publicly transmitted, changed, disseminated, distributed, or published without the prior written consent of Alibaba Cloud and/or its affiliates. The names owned by Alibaba Cloud shall not be used, published, or reproduced for marketing, advertising, promotion, or other purposes without the prior written consent of Alibaba Cloud. The names owned by Alibaba Cloud include, but are not limited to, "Alibaba Cloud", "Aliyun", "HiChina", and other brands of Alibaba Cloud and/or its affiliates, which appear separately or in combination, as well as the auxiliary signs and patterns of the preceding brands, or anything similar to the company names, trade names, trademarks, product or service names, domain names, patterns, logos, marks, signs, or special descriptions that third parties identify as Alibaba Cloud and/or its affiliates.

6. Please directly contact Alibaba Cloud for any errors of this document.

Document conventions

Style	Description	Example
Danger	A danger notice indicates a situation that will cause major system changes, faults, physical injuries, and other adverse results.	Danger: Resetting will result in the loss of user configuration data.
Warning	A warning notice indicates a situation that may cause major system changes, faults, physical injuries, and other adverse results.	Warning: Restarting will cause business interruption. About 10 minutes are required to restart an instance.
Notice	A caution notice indicates warning information, supplementary instructions, and other content that the user must understand.	Notice: If the weight is set to 0, the server no longer receives new requests.
Note	A note indicates supplemental instructions, best practices, tips, and other content.	Note: You can use Ctrl + A to select all files.
>	Closing angle brackets are used to indicate a multi-level menu cascade.	Click **Settings**> **Network**> **Set network type**.
Bold	Bold formatting is used for buttons , menus, page names, and other UI elements.	Click **OK**.
`Courier font`	Courier font is used for commands	Run the `cd /d C:/window` command to enter the Windows system folder.
Italic	Italic formatting is used for parameters and variables.	`bae log list --instanceid` *Instance_ID*
[] or [a|b]	This format is used for an optional value, where only one item can be selected.	`ipconfig [-all|-t]`
{} or {a|b}	This format is used for a required value, where only one item can be selected.	`switch {active|stand}`

Table of Contents

1.Set up a network environment for replication

Before you start data replication workloads, you must set up a network environment that allows Data Transmission Service (DTS) to access your source and target databases, including network connectivity and security settings. For example, you must add the IP ranges of DTS servers to the whitelists of your source and target databases. Your database may reside in your corporate network so you have to connect your network into Alibaba Cloud.

The following table lists the configuration steps that are required for each specific scenario:

Migration path	Replication mode	Required configurations
Source or target: User-Created Database with Public IP Address	• Data migration • Change tracking	• Whitelist DTS IP addresses for your user-created database
Source or target: Database without public IP:Port (Accessed through database gateway)	• Data migration • Data synchronization • Change tracking	• Connect a non-Alibaba Cloud database to Alibaba Cloud Database Gateway • Whitelist DTS IP addresses for your user-created database
Source: Self built database accessed through Cloud Enterprise Network(CEN)	• Data migration • Data synchronization	• Connect a non-Alibaba Cloud database to Alibaba Cloud Database Gateway • Whitelist DTS IP addresses for your user-created database
Source or target: User-Created Database Connected over Express Connect, VPN Gateway, or Smart Access Gateway	• Data migration • Data synchronization • Change tracking	• Connect your on-premises networks to Alibaba Cloud • Configure a route between DTS and Express Connect, VPN Gateway, or Smart Access Gateway • Whitelist DTS IP addresses for your user-created database • Connect your on-premises networks to Alibaba Cloud over an IPsec-VPN tunnel

2.Whitelist DTS IP addresses for your user-created database

Your user-created database hosted off Alibaba Cloud may have been configured to only accept connections from designated IP addresses. In this case, you need to configure your security settings to allow DTS servers to connect.

Applicable data stores

Certain types of user-created databases, either as the source or target database, require that you configure the security settings to allow DTS servers to access your user-created database. For managed database services offered by Alibaba Cloud or user-created database systems running on ECS instances, DTS automatically configures the required whitelist settings in the related database instance or security group.

Use the following table to determine whether you need to whitelist DTS servers:

Data store	Whitelisting required
User-Created Database with Public IP Address	Yes
Database without public IP:Port (Accessed through database gateway)	Yes
Self built database accessed through Cloud Enterprise Network(CEN)	Yes
User-Created Database Connected Over Express Connect, VPN Gateway, or Smart Access Gateway	Yes
User-Created Database in ECS Instance	No
RDS Instance	No
ApsaraDB for MongoDB	No
PolarDB	No

Determine the DTS task region

Use the following list to determine which region of the DTS servers that you need to whitelist:

- Data migration: select the region of the target database
- Change tracking: select the region of the source database

Obtain the IP range

The IP range varies, depending on the network over which DTS accesses your database.

Reachable over the Internet: If DTS accesses your user-created database over the Internet, use the following table to obtain the DTS IP ranges (CIDR blocks) for your selected region:

Region	IP range
China (Hangzhou)	101.37.14.0/24,114.55.89.0/24,115.29.198.0/24,118.178.120.0/24,118.178.121.0/24,120.26.106.0/24,120.26.116.0/24,120.26.117.0/24,120.26.118.0/24,120.55.192.0/24,120.55.193.0/24,120.55.194.0/24,120.55.241.0/24,121.40.125.0/24,121.196.246.0/24,101.37.12.0/24,101.37.13.0/24,101.37.15.0/24,101.37.25.0/24,47.96.39.0/24,118.31.184.0/24,118.31.165.0/24,118.31.246.0/24,120.55.12.0/24,47.97.7.0/24,47.97.27.142/32,47.97.73.210/32,121.43.162.118/32,121.43.185.141/32,121.196.211.16/32,114.55.125.94/32,121.43.179.168/32,121.43.174.187/32,47.99.171.159/32,47.97.118.150/32,47.98.251.185/32,47.99.43.73/32,47.97.195.167/32,120.27.211.237/32,47.97.125.64/32,47.98.52.255/32,47.97.116.109/32,47.97.119.148/32,47.98.51.78/32,47.97.106.64/32,116.62.172.149/32,120.55.40.134/32,47.98.39.64/32,116.62.197.0/24,121.196.199.0/24,116.62.206.0/24,116.62.208.0/24,116.62.57.0/24,116.62.20.0/24,116.62.64.0/24,116.62.201.0/24,121.196.198.0/24,118.31.43.101,101.37.152.136,118.31.38.161,120.55.60.232,120.55.60.183,101.37.149.3
China (Shanghai)	139.196.17.0/24, 139.196.18.0/24, 139.196.25.0/24, 139.196.27.0/24, 139.196.154.0/24, 139.196.116.0/24, 139.196.254.0/24, 139.196.166.0/24, 106.14.46.0/24, 106.14.37.0/24, 106.14.36.0/24, 106.15.250.0/24, 101.132.248.0/24, 47.100.95.0/24, 106.15.73.0/24, 106.15.75.0/24, 47.100.137.0/24, 106.14.177.89/32, 106.14.178.118/32, 139.196.138.36/32, 106.14.4.132/32, 139.196.92.27/32, 139.196.143.11/32, 139.196.44.156/32, 139.196.6.35/32, 139.196.50.106/32, 139.196.25.56/32, 139.196.47.137/32, 139.196.6.124/32, 139.196.49.138/32, 139.196.41.168/32, 139.196.48.218/32, 139.196.51.72/32, 47.101.194.1/32, 47.101.166.207/32, 47.101.181.171/32, 47.101.177.224/32, 47.100.186.20/32
China (Qingdao)	115.28.200.0/24, 115.28.216.0/24, 115.28.226.0/24, 115.28.247.0/24, 118.190.133.0/24, 120.27.53.0/24, 10.31.69.0/24, 10.144.88.0/24, 10.144.153.0/24, 10.161.39.0/24, 10.161.59.0/24, 10.252.29.0/24, 100.104.72.0/24

Region	IP range
China (Beijing)	112.126.80.0/24,112.126.87.0/24,112.126.91.0/24,112.126.92.0/24,123.56.108.0/24,123.56.120.0/24,123.56.137.0/24,123.56.148.0/24,123.56.164.0/24,123.57.48.0/24,182.92.153.0/24,182.92.186.0/24,101.200.174.0/24,101.200.160.0/24,101.200.176.0/24,47.94.36.0/24,47.94.47.0/24,101.201.214.0/24,101.201.82.0/24,123.56.182.0/24,101.201.105.0/24,182.92.132.0/24,60.205.157.0/24,101.201.107.0/24,60.205.164.0/24,60.205.165.0/24,59.110.4.0/24,59.110.17.0/24,123.56.186.0/24,60.205.146.0/24,59.110.37.0/24,59.110.19.0/24,60.205.112.0/24,60.205.243.0/24,101.201.108.0/24,59.110.38.0/24,60.205.197.0/24,60.205.166.0/24,101.200.194.0/24,101.200.182.0/24,123.57.204.0/24,101.200.235.0/24,123.57.206.0/24,123.57.65.0/24,47.94.167.117/32,182.92.157.129/32,101.200.39.123/32,101.200.192.4/32,39.105.58.165/32,101.200.213.59/32,59.110.164.0/24,47.94.150.0/24,39.105.56.0/24,47.93.21.0/24,47.93.30.0/24,47.93.24.0/24,60.205.222.0/24,60.205.186.0/24,47.93.22.174/32,47.93.10.168/32,47.94.246.43/32,47.94.94.233/32,47.95.241.173/32,59.110.155.242/32,60.205.230.219/32,101.200.50.74/32,101.201.65.33/32,112.126.96.49/32,112.126.96.184/32,112.126.98.30/32,112.126.99.22/32,112.126.99.87/32,112.126.99.205/32
China (Zhangjiakou-Beijing Winter Olympics)	47.92.22.0/24, 11.192.243.0/24, 100.104.175.0/24, 11.112.227.0/24
China (Hohhot)	100.104.72.0/24, 39.104.29.0/24, 11.193.183.0/24
China (Shenzhen)	112.74.0.0/16, 120.24.0.0/16, 120.25.0.0/16, 120.78.6.0/24, 120.78.5.0/24, 47.115.165.0/24, 47.115.166.0/24, 47.115.162.0/24, 47.115.161.0/24, 120.24.65.0/24, 120.24.67.0/24, 120.24.160.0/24, 120.25.215.0/24, 120.24.214.0/24, 120.24.223.0/24
China (Hong Kong)	203.88.163.0/24, 47.90.37.0/24, 47.90.38.0/24, 47.89.39.0/24, 10.26.5.0/24, 10.47.47.0/24, 10.175.251.0/24, 10.175.254.0/24, 10.175.255.0/24, 100.104.233.0/24, 47.52.111.0/24, 47.52.25.202/32, 47.91.228.249/32, 47.52.166.98/32, 10.28.201.197/32, 10.28.185.63/32, 10.28.201.14/32
Singapore (Singapore)	47.88.133.0/24, 47.88.139.0/24, 47.74.206.0/24
Australia (Sydney)	47.91.49.0/24, 47.91.50.0/24
Malaysia (Kuala Lumpur)	47.254.212.0/24
Indonesia (Jakarta)	149.129.228.0/24
India (Mumbai)	149.129.164.0/24

Region	IP range
Japan (Tokyo)	47.91.9.0/24, 47.91.13.0/24, 47.91.27.0/24
US (Silicon Valley)	98.11.174.0/24, 198.11.175.0/24, 10.172.115.0/24, 10.172.117.0/24, 10.172.119.0/24, 100.104.175.0/24, 47.89.244.175/32
US (Virginia)	47.89.170.0/24, 47.250.29.0/24
Germany (Frankfurt)	47.91.82.0/24, 47.91.83.0/24, 47.91.84.0/24, 11.192.168.0/24, 11.192.169.0/24, 11.192.170.0/24, 100.104.5.0/24
UK (London)	8.208.17.0/24
UAE (Dubai)	47.91.102.0/24, 47.91.103.0/24

Reachable from an internal network: If DTS accesses your user-created database over a virtual or physical internal network, such as Express Connect, VPN Gateway, and Smart Access Gateway, use the following table to obtain the DTS IP ranges (CIDR blocks) for your selected region:

Region	IP range
China (Hangzhou)	100.104.52.0/24, and 100.104.61.128/26
China (Shanghai)	100.104.205.0/24
China (Qingdao)	100.104.72.0/24
China (Beijing)	100.104.183.0/24, and 100.104.236.128/26
China (Zhangjiakou-Beijing Winter Olympics)	100.104.175.0/24
China (Hohhot)	100.104.72.0/24
China (Shenzhen)	100.104.205.0/24
China (Hong Kong)	100.104.233.0/24
Singapore (Singapore)	100.104.188.0/24
Australia (Sydney)	100.104.233.0/24
Malaysia (Kuala Lumpur)	100.104.5.0/24
Indonesia (Jakarta)	100.104.175.0/24
India (Mumbai)	100.104.8.0/24
Japan (Tokyo)	100.104.112.0/24
US (Silicon Valley)	100.104.175.0/24

Region	IP range
US (Virginia)	100.104.233.0/24
Germany (Frankfurt)	100.104.5.0/24
UK (London)	100.104.133.64/26
UAE (Dubai)	100.104.205.0/24

Whitelist the IP range

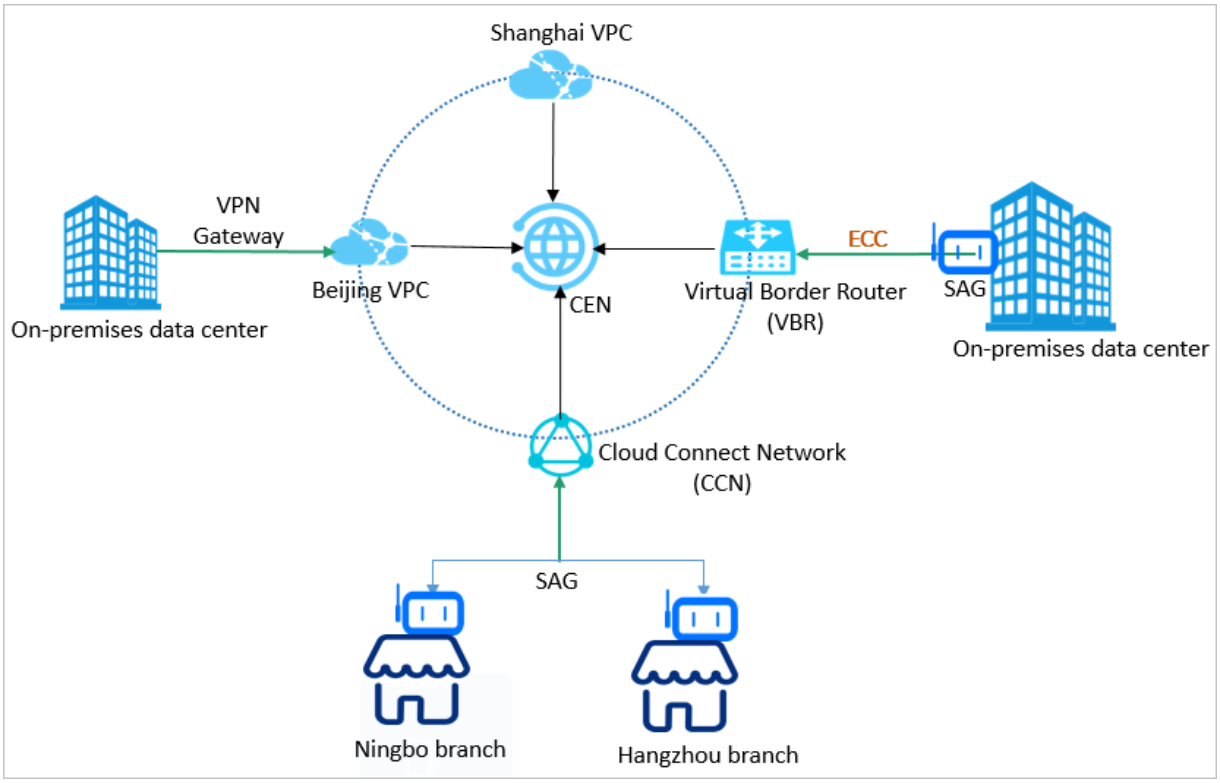
After obtaining the IP range, you need to whitelist the IP range in the security settings of your user-created database system. The actual procedure may vary, depending on your system deployment. For example, if your database is deployed behind a firewall, you need to configure the security rules to allow the DTS IP range to access your database server. If your database is deployed on a virtual machine offered by a third-party vendor, you need to configure the security groups to allow the DTS IP range to access your virtual machine.

3.Connect your on-premises networks to Alibaba Cloud

You can use VPN Gateway, Express Connect, or Smart Access Gateway to connect your on-premises networks to a virtual private cloud (VPC) in Alibaba Cloud.

Overview

Enterprises may leverage cloud services as an extension to their on-premises infrastructure. To allow on-cloud and off-cloud workloads to operate seamlessly together, you must enable your on-premises facilities and Alibaba Cloud infrastructure to communicate over a private network. To help you achieve this goal, Alibaba Cloud offers multiple private networking options, including VPN Gateway, Express Connect, Smart Access Gateway, and Cloud Enterprise Network (CEN).



Solutions

Solution	Description

Solution	Description
VPN Gateway	You can use VPN Gateway to create a VPN over IPsec tunnel between your VPCs and on-premises facilities. VPN Gateway runs on servers with primary/secondary redundancy. If the primary server fails, the tunneling workloads are switched over to a secondary server within seconds. VPN tunnels are based on Internet communications. The transmission performance of a VPN tunnel depends on the Internet speed. Therefore, VPN Gateway is an ideal option for latency-insensitive tasks. For more information, see Establish a connection between a VPC and an on-premises data center.
Express Connect	You can connect your on-premises networks to Alibaba Cloud access points over a leased line provided by a third-party service provider. You can apply for a circuit in the Express Connect console. An Express Connect circuit provides fast and stable connectivity between your on-premises network and Alibaba Cloud networks. Therefore, Express Connect is an ideal option for latency-sensitive tasks. For more information about how to deploy Express Connect circuits, see Overview of access solutions.
Redundant Express Connect circuits	You can use redundant Express Connect circuits to connect your on-premises networks into Alibaba Cloud VPCs. You can provision up to four Express Connect circuits that work in equal-cost multi-path routing (ECMP) mode. For more information, see Create active/standby physical connections and Create redundant connections with load-balancing routing.
Smart Access Gateway	Smart Access Gateway provides an easy-to-deploy but highly secure connection between your on-premises networks and Alibaba Cloud VPCs. You can establish an encrypted connection to the nearest VPC based on Internet communications. Smart Access Gateway is an ideal option for connecting multiple branch sites into Alibaba Cloud with affordable costs and minimal deployment efforts. For more information, see Connect private networks outside mainland China to Alibaba Cloud
Smart Access Gateway as a backup	You can use Smart Access Gateway as a backup if you already have an Express Connect circuit that connects your on-premises network to Alibaba Cloud networks.

4.Connect a non-Alibaba Cloud database to Alibaba Cloud Database Gateway

This topic describes how to connect an on-premises database or a database that is hosted on a third-party cloud to Alibaba Cloud by using Database Gateway. Then, you can specify the connected database as the source or target in your tasks of data migration, data synchronization, or change tracking.

Prerequisites

An AccessKey pair is created. The AccessKey pair consists of an AccessKey ID and AccessKey secret. For more information, see Create an AccessKey pair.

Context

Database Gateway helps you connect your non-Alibaba Cloud databases to Alibaba Cloud. This option is more affordable than other networking solutions, such as Express Connect and Cloud Enterprise Network. This service works with either an on-premises database or a database that is hosted on a third-party cloud. For more information about the design concept of Database Gateway, see How it works.

Precautions

Database Gateway is in public preview and is available only in the following regions:

- China (Hangzhou)
- Singapore
- Indonesia (Jakarta)
- UK (London)
- US (Virginia)

Billing

Database Gateway incurs no fees while it is in public preview.

Procedure

1. Log on to the Database Gateway console.

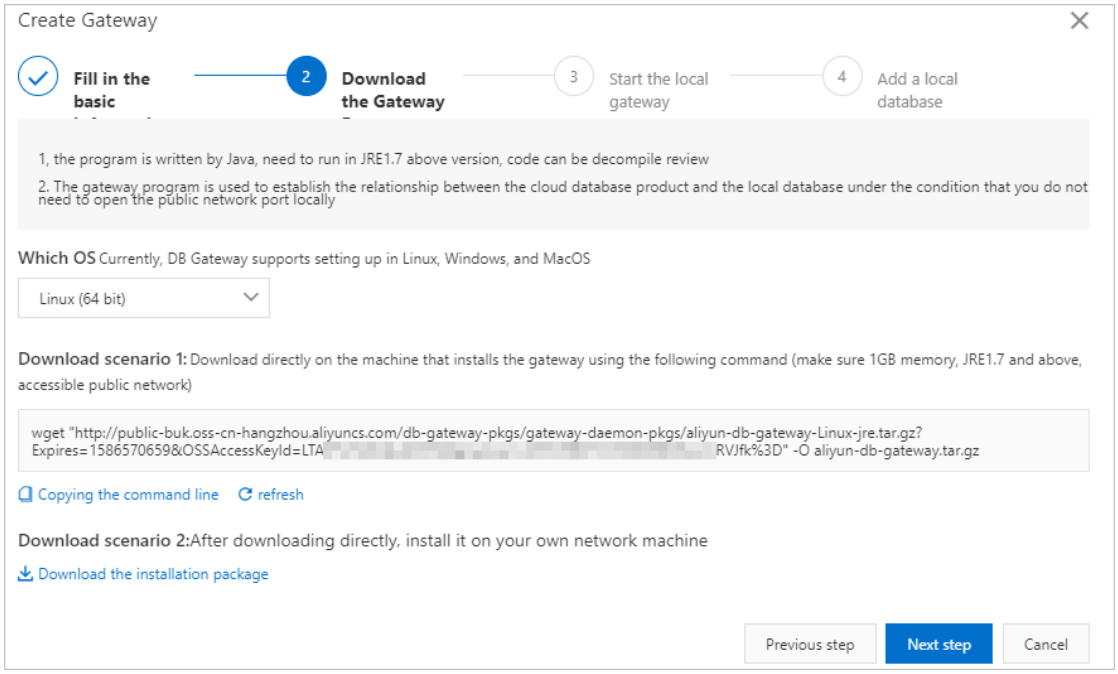
   > **Note** You are prompted to activate the service the first time that you log on to the Database Gateway console. On the **Enable Service** page, select the check box to confirm that you agree to the Terms of Service, and then click **Enable Now**.

2. Click **Create Gateway**.
3. In the Create Gateway dialog box, enter the name and description of the database gateway, and then click **Next step**.
4. Download the gateway program.

Notice The server that runs the gateway program must meet the following requirements:

- Performance: 1 CPU core, 1 GB memory
- Software environment: JRE 1.7 or later. We recommend that you use a 64-bit operating system.
- Network:
  - The server can connect to the target database. You can minimize the network latency by placing the server and the database in the same internal network.
  - The server can access the Internet. The service port of the server does not need to be accessible over the Internet. For an optimal transmission rate, make sure that the outbound bandwidth is 10 Mbit/s or higher.

i. In the **Create Gateway** dialog box, download the gateway program for the target operating system.



ii. Copy the downloaded installation file to the server where you want to deploy the gateway program, and decompress the file.

5. Start the gateway program.

i. Log on to the server where the gateway program is deployed, and go to the directory where the gateway program is decompressed.

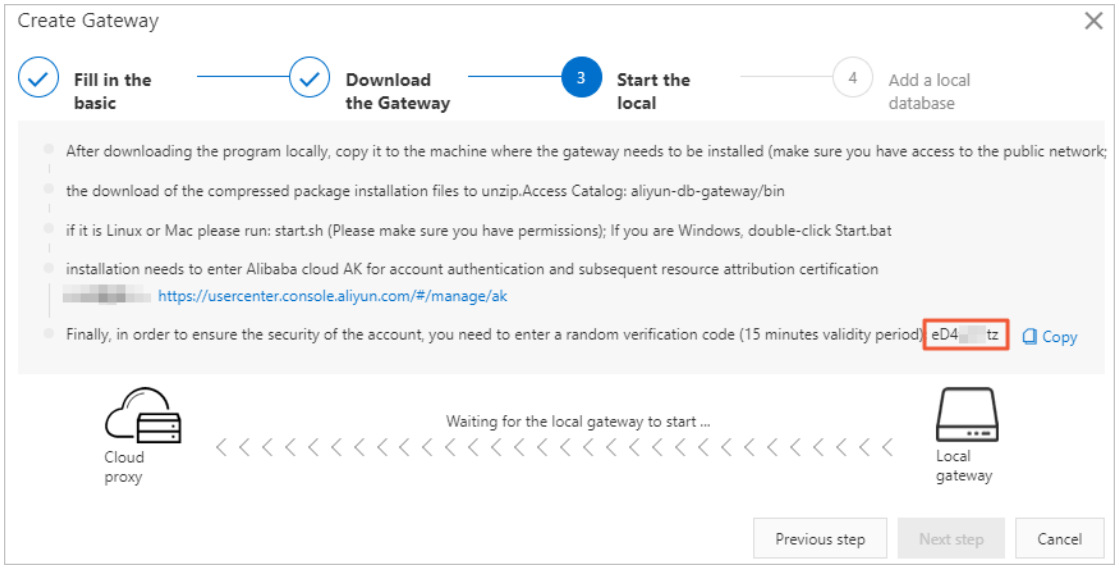
ii. Select one of the following methods to start the gateway program, depending on your operating system:

- For Linux or Mac, run the `bin/start.bat` command.
- For Windows, double-click the *db_agent.bat* file in the *bin* directory.

iii. Enter the AccessKey ID and AccessKey secret.

```
Please choose the install language: [1]、English(Default) [2]、简体中文
>1
Welcome to use Alibaba Cloud Database Gateway(DG).
Aliyun Database Gateway can help you to manage databases in your own network.
The only requirement is that you have access to the https service in public network.

Please make sure you have prepared following information:

   1. your Alibaba Cloud main account AccessKey Id and AccessKey secret. (https://usercen
ter.console.aliyun.com/#/manage/ak)

   2. Register a DG through the Console. (https://dg.console.aliyun.com/)



Please input Alibaba Cloud Account AccessKeys:
AccessKey ID> LTAI4FfCc
AccessKey Secret>
Aliyun account information is being checked, please wait...
Aliyun Account has been successfully certified

Please input VerificationCode(from 'Gateway Config' page):
>
```

iv. After the verification is successful, return to the Database Gateway console and click **Next step** to obtain a random verification code.



v. Enter the verification code in the CLI of the gateway program and press the Enter key. Wait until the connection is established.

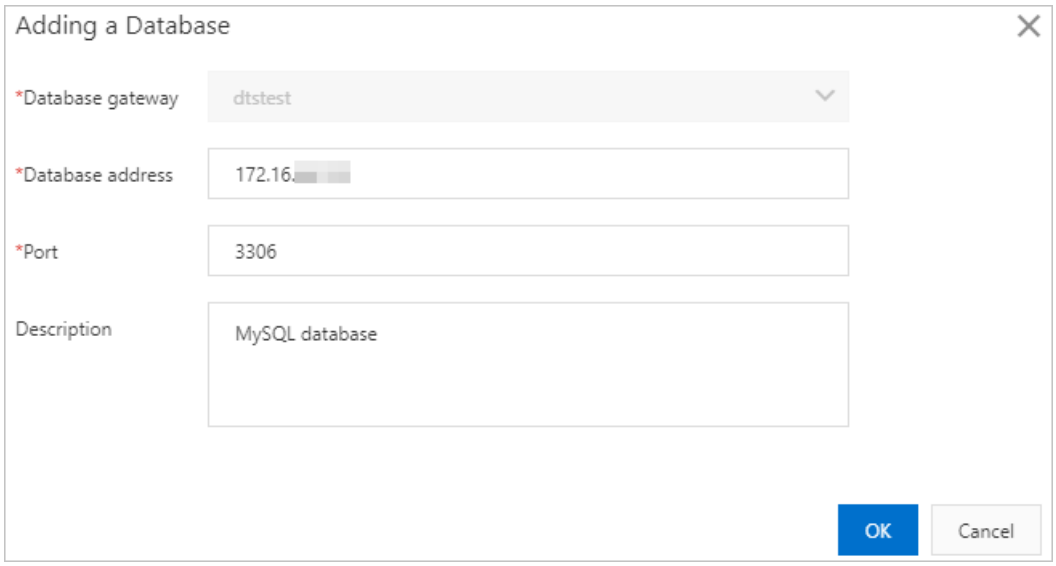
```
Validating the validity of the database gateway validation code...
Congratulations, the validation of local accounts and gateways has all passed. Now start the r
everse channel...
waiting for connection established...

.
connection established successfully..
DBGateway start successfully, PID=18
Note: You can now start adding local databases (IP: PORT accessible to local machines) through
 the Aliyun database gateway platform.
```

6. Add a database.

> **Note** You can repeat this step to add multiple databases.

i. Return to the Database Gateway console and click **Add database**.

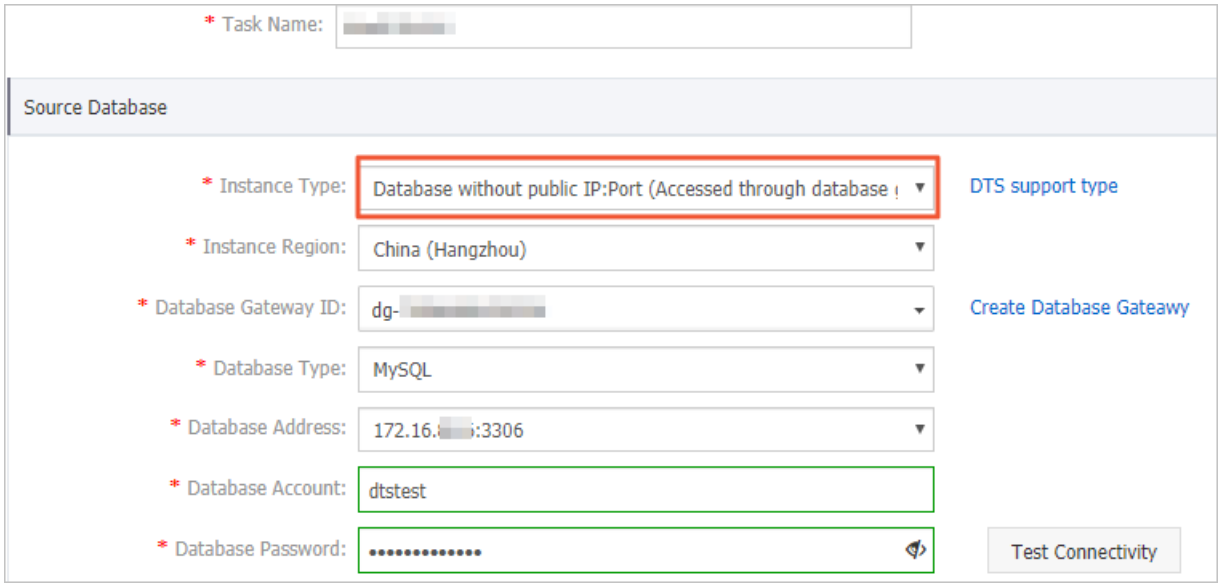
ii. In the dialog box that appears, enter the address and port number of the database server, enter a description for the server connection, and then click **OK**. The address must be reachable from the server that is running the gateway program. If the gateway program is running on the same server as the database server, set the address to 127.0.0.1.



What's next

You can select the database that is connected over Database Gateway as either the source database or target database when you create a task. To do this, select **Database without public IP:Port (Accessed through database gateway)** as the instance type, and then select the database address from the drop-down list.

> **Note** If you select **Database without public IP:Port (Accessed through database gateway)** as the instance type when you configure data migration, the source and target instances must reside in the same region.



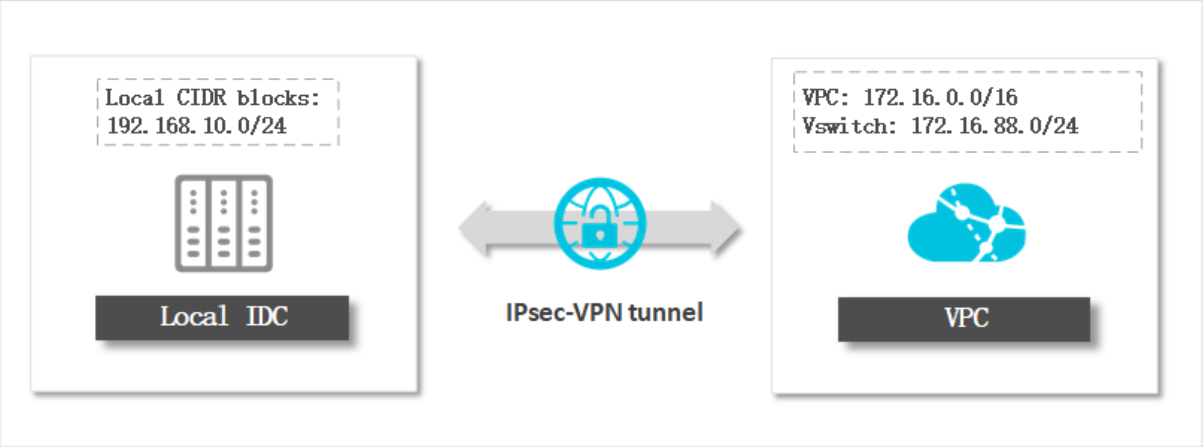
5.Connect your on-premises networks to Alibaba Cloud over an IPsec-VPN tunnel

VPN Gateway allows you to connect on-premises data centers, corporate networks, individual clients to Alibaba Cloud Virtual Private Cloud (VPC) networks through encrypted tunnels. This topic describes how to connect an on-premises data center to a VPC by using an IPsec-VPN tunnel.

Prerequisites

- The gateway device that you use to connect to Alibaba Cloud supports the standard IKEv1 and IKEv2 protocols. In this example, IKEv2 must be supported because multiple subnets are configured. Compatible devices include certain models manufactured by Huawei, H3C, Hillstone, Sangfor, Cisco ASA, Juniper, SonicWall, Nokia, IBM, and Ixia.
- The gateway device has a static public IP address assigned.
- The IP address ranges of the on-premises network do not overlap the IP address ranges of the VPC.

Context



You can select **User-created database connected over Express Connect, VPN Gateway, or Smart Access Gateway** when you create a replication task in data migration, data synchronization, or change tracking mode, and then enter the private IP address of your on-premises database.

Precautions

If you have already connected your on-premises networks to Alibaba Cloud, you can skip the steps of VPN tunnel setup. However, you need to whitelist DTS servers in your VPN settings and create several static routes. To do this, follow these steps:

1. Add the CIDR blocks of DTS servers to the IPsec-VPN connection. For more information, see Modify an IPsec-VPN connection.

> Note Click + Add CIDR Block and enter the CIDR blocks of DTS servers for the corresponding region. For more information, see Add the CIDR blocks of DTS servers to the security settings of on-premises databases.

2. Configure static routes on your customer gateway. For more information, see Step 4: Configure an IPsec-VPN connection and a static route on the on-premises gateway.

Billing

VPN Gateway is a paid service. For more information, see Billing.

Step 1: Create a VPN gateway

1. Log on to the VPC console.
2. In the upper-left corner of the page, select a region.
3. In the left-side navigation pane, click **VPN > VPN Gateways**.
4. On the **VPN Gateways** page, click **Create VPN Gateway**.
5. Complete the VPN gateway settings as follows:

Parameter	Description
Region	Select the region where the VPN gateway resides. > Note The VPN gateway must reside in the same region as the VPC that you want to connect to.
VPC	Select the VPC to be connected.
Assign VSwitch	Optional. You can set this option to **Yes** and select a VSwitch so that the VPN gateway is connected to the specified VSwitch only.
Peak Bandwidth	Select the maximum Internet bandwidth of the VPN gateway.
IPsec-VPN	Select **Enable**. > Note The IPsec-VPN mode supports site-to-site connections. You can create an IPsec tunnel to connect an on-premises network to a VPC, or connect two VPCs.

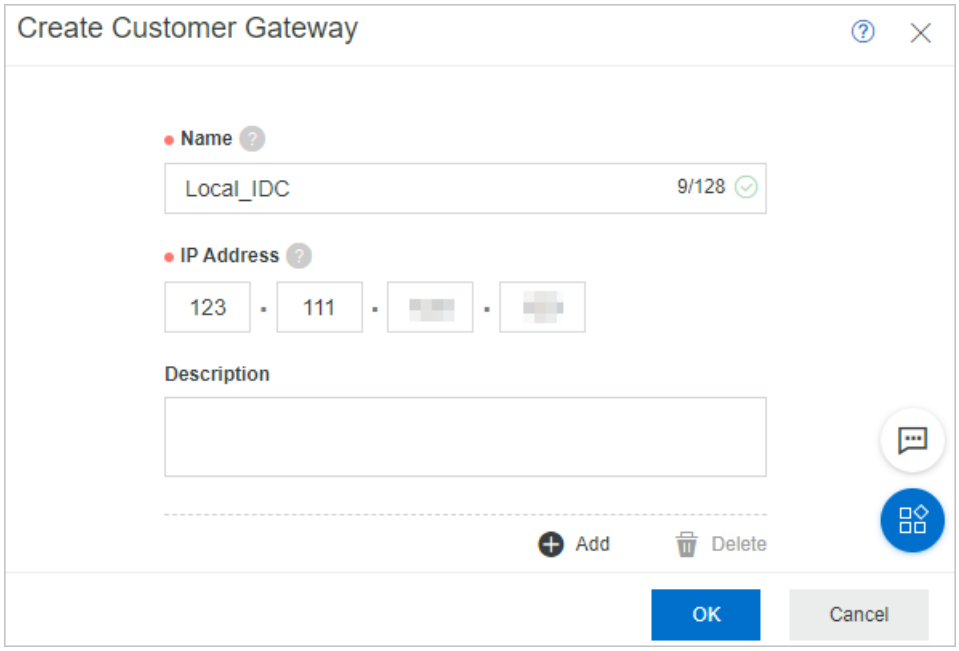
Parameter	Description
SSL-VPN	Select **Disable**. Note The SSL-VPN mode supports point-to-site connections. You can create a VPN connection from a VPN client without configuring a gateway for the client.
Billing Cycle	This setting is fixed to **By Hour**.

6. Click **Buy Now** and follow the instructions to complete the payment.

Step 2: Create a customer gateway

1. Log on to the VPC console.
2. In the upper-left corner of the page, select the region where the VPN gateway resides.
3. In the left-side navigation pane, click **VPN > Customer Gateways**.
4. Click **Create Customer Gateway**.
5. Complete the customer gateway settings as follows:

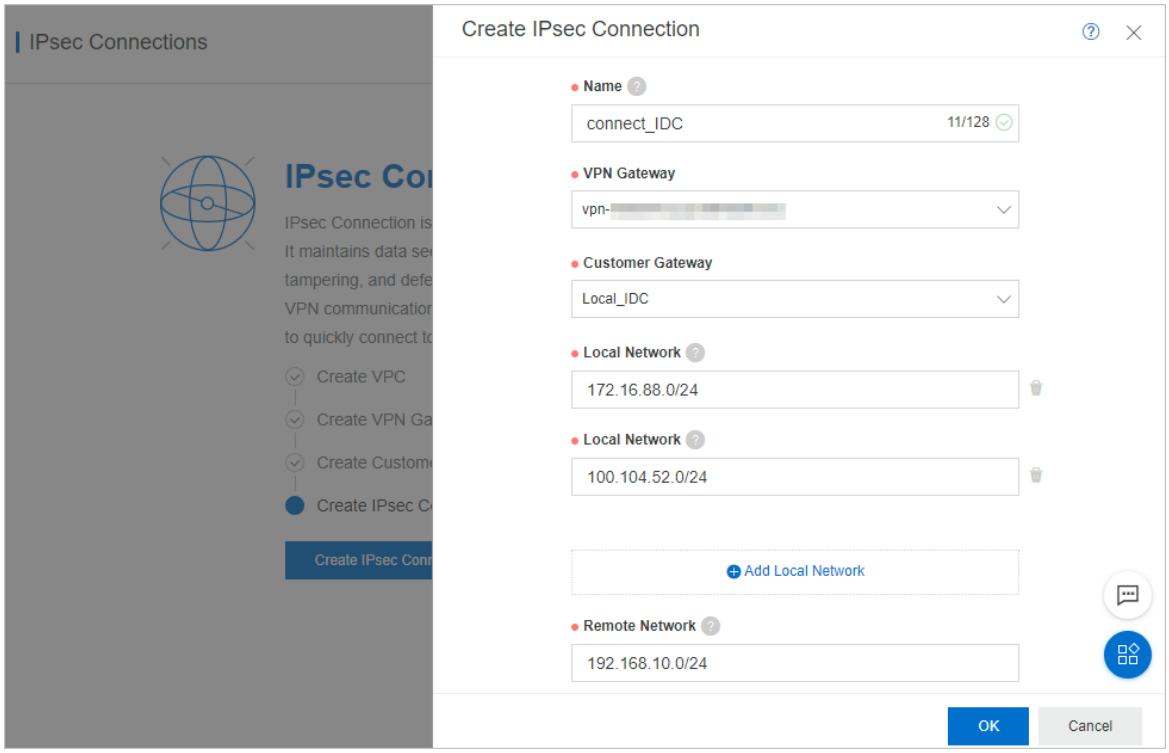
Parameter	Description
Name	Enter a name for the customer gateway.
IP Address	Enter the static public IP address of the gateway device of the on-premises data center.
Description	The description must be 2 to 256 characters in length and cannot start with `http://` or `https://`.



6. Click **OK**.

Step 3: Create an IPsec-VPN connection and configure a route

1. Log on to the VPC console.
2. In the upper-left corner of the page, select the region to which the VPN gateway belongs.
3. In the left-side navigation pane, click **VPN > IPsec Connections**.
4. Click **Create IPsec Connection**.
5. In the **Create IPsec Connection** pane, complete the settings as follows:

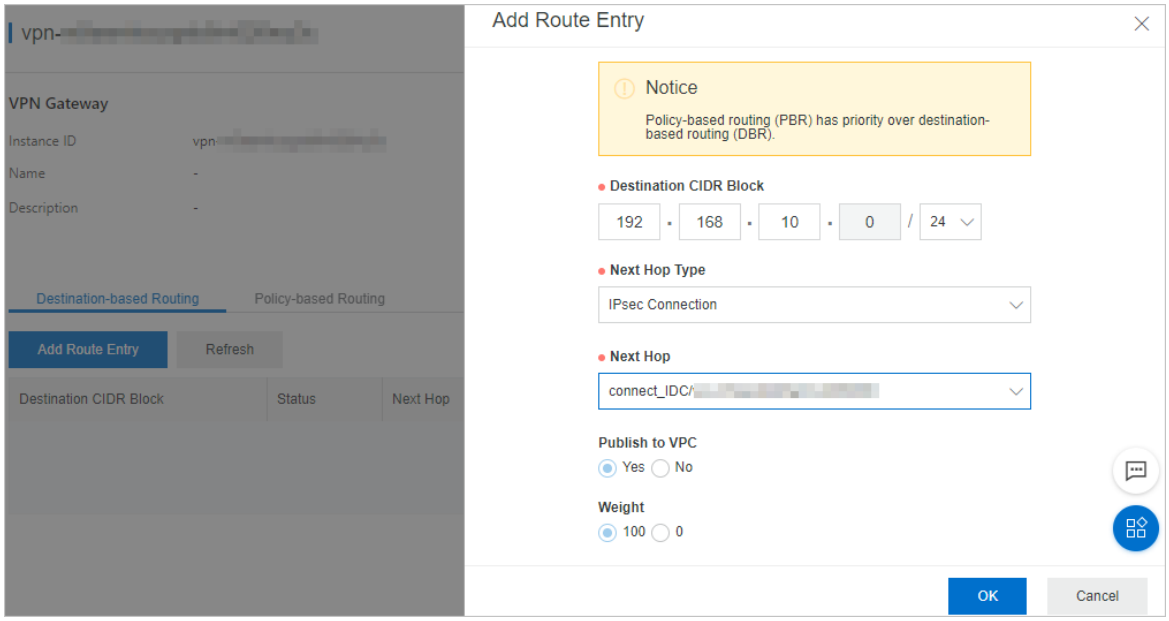


Setting	Description
Name	Enter a name for the IPsec-VPN connection. Note The name must be 2 to 128 characters in length and can contain letters, digits, underscores (_), and hyphens (-). It must start with a letter.
VPN Gateway	Select the VPN gateway to be connected through the IPsec-VPN connection. In this procedure, select the VPN gateway that is created in step 1.
Customer Gateway	Select the customer gateway to be connected through the IPsec-VPN connection. In this procedure, select the customer gateway that is created in step 2.
Local Network	Enter the CIDR block of the VPC. This setting is used for phase two negotiations. Notice ◦ You can enter the CIDR block of the VPC or a VSwitch in the VPC. In this procedure, 172.16.88.0/24 is the CIDR block of a VSwitch in the VPC. ◦ The CIDR block of the VPC cannot overlap the CIDR block of the on-premises data center.
+ Add Local Network	Enter multiple CIDR blocks of the VPC. In this procedure, enter the CIDR blocks of DTS servers. For more information, see Add the CIDR blocks of DTS servers to the security settings of on-premises databases. Note When you add multiple CIDR blocks, set the version to ikev2 in Advanced Configuration.
Remote Network	Enter the CIDR block of the on-premises network. This setting is used for phase two negotiations. Note The CIDR block of the on-premises network must not overlap the CIDR block of the VPC.
+ Add Remote Network	Enter multiple CIDR blocks of the on-premises network. Notice When you add multiple CIDR blocks, set the version to ikev2 in Advanced Configuration.

Setting	Description
Effective Immediately	Specify whether the settings take effect immediately. ○ **Yes**: initiates the negotiation phase immediately after the configuration is applied. ○ **No**: initiates the negotiation phase the first time that traffic is detected in the IPsec-VPN tunnel.
Advanced Configuration	For more information about the IPsec-VPN configurations, see Create an IPsec-VPN connection.
Health Check	

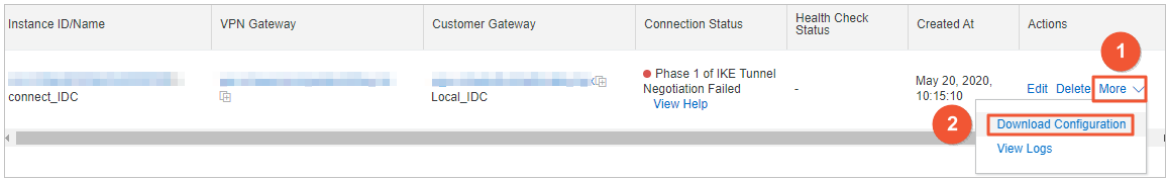
6. Click **OK**.
7. In the success message, click **OK** to configure routing for the VPN gateway.
8. The **VPN Gateway** page appears. On the **Destination-based Routing** tab, click **Add Route Entry**.
9. In the **Add Route Entry** pane, complete the settings as follows.

Setting	Description
Destination CIDR block	Enter the private CIDR block of the on-premises network. In this example, enter 192.168.10.0/24.
Next Hop Type	Select **IPsec Connection**.
Next Hop	Select the IPsec-VPN connection that you create.
Publish to VPC	Specify whether to publish the new route entry to the VPC routing table. ○ **Yes**(recommended): publish the new route entry to the VPC routing table. ○ **No**: do not publish the new route entry to the VPC routing table. **Note** If you select No, you must publish the route entry to the destination-based routing table after you add the destination-based route entry.
Weight	Select a weight: ○ **100**: The highest weight ○ **0**: The lowest weight **Note** If two static routes are based on the same destination CIDR block, you cannot set the weight of both route entries to 100.



Step 4: Configure an IPsec-VPN connection and a static route on the on-premises gateway

1. Log on to the VPC console.
2. In the upper-left corner of the page, select the region where the VPN gateway resides.
3. In the left-side navigation pane, click **VPN > IPsec Connections**.
4. Find the target IPsec-VPN connection and choose **More > Download Configuration** in the **Actions** column.



5. In the **IPsec Connection Configuration** pane, the JSON notation of the peer configuration is displayed. Add the peer configuration to the on-premises gateway device. The configurations vary depending on the device manufacturer and model. For more information, see Configure anon-premises gateway

6. Add a static route entry to the on-premises gateway device. The destination addresses are the CIDR blocks of DTS servers for the corresponding region. For more information, see Add the CIDR blocks of DTS servers to the security settings of on-premises databases. The next hop is the new IPsec-VPN tunnel interface.