ALIBABA CLOUD

Alibaba Cloud

Data Transmission Service

Network Setup

Document Version: 20220711

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 ranges 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 ranges 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 ranges 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 ranges for your user-created database • Connect your on-premises networks to Alibaba Cloud over an IPsec-VPN tunnel

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

Your user-created database hosted off Alibaba Cloud may have been configured to only accept connections from designated IP ranges. 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. This is required if the database type is any of the following types: user-created database with public IP address, database without public IP:port (accessed through database gateway), self built database accessed through Cloud Enterprise Network (CEN), or user-created database connected over Express Connect, VPN Gateway, or Smart Access Gateway.

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 and whitelist the corresponding IP ranges in the source and target database settings.
- Change tracking: select the region of the source database and whitelist the corresponding IP ranges in the source database settings.
- Data synchronization:
  - To allow DTS to access the source database, select the regions of the source and target databases and whitelist the corresponding IP ranges in the source database settings.
  - To allow DTS to access the target database, select the region of the target database and whitelist the corresponding IP ranges in the target database settings.

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:

> **Note** Data synchronization does not support user-created databases that are reachable over the Internet.

Warning

- If the source ordestination database is an Alibaba Cloud database instance (such as an ApsaraDB RDS for MySQL instance and an ApsaraDB for MongoDB instance), DTS automatically adds the CIDR blocks of DTS servers in the corresponding region to the whitelist of the database instance. If the source or destination database is a self-managed database hosted on Elastic Compute Service (ECS), DTS automatically adds the CIDR blocks of DTS servers in the corresponding region to the security rules of the ECS instance. You do not need to manually add the CIDR blocks of DTS servers. The following table lists the CIDR blocks of DTS servers in each region.
- If the source or destination database is a self-managed database and the public IP addresses of DTS servers are added to allow access from DTS servers, security risks may arise. Proceed with caution. We recommend that you keep your account and password strictly confidential, control access to port numbers, or establish connections over internal networks (Express Connect, VPN Gateway, or Smart Access Gateway).
- After the DTS task is completed or released, we recommend that you remove the CIDR blocks of DTS servers from the whitelist.

Region	IP range
China (Hangzhou)	101.37.14.0/24,114.55.89.0/24,115.29.198.0/24,118.178.120.0/24,118.178.121.0/24,120.26.106.0/24,120.26.116.0/24,120.26.117.0/24,120.26.118.0/24,120.55.192.0/24,120.55.193.0/24,120.55.194.0/24,120.55.241.0/24,121.40.125.0/24,121.196.246.0/24,101.37.12.0/24,101.37.13.0/24,101.37.15.0/24,101.37.25.0/24,47.96.39.0/24,118.31.165.0/24,118.31.246.0/24,120.55.12.0/24,47.97.7.0/24,47.97.27.142,47.97.73.210,121.43.162.118,121.43.185.141,121.196.211.16,114.55.125.94,121.43.179.168,121.43.174.187,47.99.171.0/24,118.31.118.0/24,47.97.118.0/24,47.98.251.0/24,47.99.43.0/24,47.97.195.0/24,120.27.211.0/24,47.97.125.0/24,47.98.52.0/24,47.97.116.0/24,47.97.119.0/24,47.98.51.0/24,47.97.106.0/24,116.62.172.0/24,120.55.40.0/24,47.98.39.0/24,121.43.162.0/24,47.97.73.0/24,121.43.174.0/24,114.55.125.0/24,47.97.27.0/24,121.43.179.0/24,121.43.185.0/24,118.31.238.0/24,118.31.43.0/24,118.31.38.0/24,101.37.152.0/24,120.55.60.0/24,101.37.149.0/24,47.98.103.0/24,47.98.101.0/24,47.98.96.0/24,118.31.45.0/24,47.97.103.0/24,47.96.31.0/24,47.98.115.0/24,47.96.15.0/24,121.40.66.0/24,120.55.67.0/24,112.124.6.0/24,121.41.48.20,121.199.28.0/24,121.41.49.0/24,121.40.249.0/24,121.41.50.0/24,121.196.211.0/24,112.124.237.96/27,112.124.239.0/26,118.31.37.0/24,121.40.111.0/24,121.41.113.0/24,121.40.155.0/24,121.41.104.0/24,121.41.106.0/24,47.97.98.0/24,120.26.42.0/24,114.55.92.0/24,120.55.94.0/24,114.55.36.0/24,116.62.171.0/24,121.40.60.0/24,121.43.233.0/24,121.41.73.0/24,112.124.140.0/24,120.55.129.0/24,47.102.181.0/24,47.102.234.0/24,47.101.109.0/24

Region	IP range
China (Shanghai)	139.196.17.0/24,139.196.18.0/24,139.196.25.0/24,139.196.27.0/24,139.196.154.0/24,139.196.116.0/24,139.196.254.0/24,139.196.166.0/24,106.14.46.0/24,106.14.37.0/24,106.14.36.0/24,106.15.250.0/24,101.132.248.0/24,47.100.95.0/24,106.15.73.0/24,106.15.75.0/24,47.100.137.0/24,106.14.177.89,106.14.178.118,139.196.138.36,106.14.4.132,139.196.92.27,139.196.143.11,139.196.44.156,139.196.6.35,139.196.50.106,139.196.25.56,139.196.47.137,139.196.6.124,139.196.49.138,139.196.41.168,139.196.48.218,139.196.51.72,47.101.194.0/24,47.101.166.0/24,47.101.181.0/24,47.101.177.0/24,47.100.186.0/24,139.196.6.0/24,139.196.138.0/24,139.196.51.0/24,139.196.49.0/24,106.14.177.0/24,139.196.48.0/24,106.14.178.0/24,106.14.4.0/24,139.196.41.0/24,139.196.44.0/24,139.196.92.0/24,139.196.143.0/24,139.196.47.0/24,47.101.175.0/24,101.132.174.0/24,139.196.52.0/24,47.101.31.0/24,47.100.3.0/24,47.100.160.244,47.101.61.0/24,47.101.205.0/24,106.14.95.0/24,101.132.133.0/24,139.224.19.0/24,139.196.155.0/24,47.102.40.0/24,106.15.248.0/24,139.196.209.0/24,101.132.17.0/24,106.14.105.0/24,101.132.223.0/24,101.133.205.0/24,112.124.140.0/24,120.55.129.0/24,47.102.181.0/24,47.102.234.0/24,47.101.109.0/24
China (Qingdao)	115.28.200.0/24,115.28.216.0/24,115.28.226.0/24,115.28.247.0/24,118.190.133.0/24,120.27.53.0/24,10.31.69.0/24,10.144.88.0/24,10.144.153.0/24,10.161.39.0/24,10.161.59.0/24,10.252.29.0/24,100.104.72.0/24,47.104.10.200,118.190.157.247,47.104.19.209,47.104.105.196,47.104.97.251,120.55.129.0/24,47.102.181.0/24,47.102.234.0/24,47.101.109.0/24,118.190.207.25,118.190.207.194,118.190.159.0/24,118.190.158.0/24,112.124.140.0/24,120.55.129.0/24,47.102.181.0/24,47.102.234.0/24,47.101.109.0/24

Region	IP range
China (Beijing)	112.126.80.0/24,112.126.87.0/24,112.126.91.0/24,112.126.92.0/24,123.56.108.0/24,123.56.137.0/24,123.56.148.0/24,123.56.164.0/24,123.57.48.0/24,182.92.153.0/24,101.200.174.0/24,101.200.160.0/24,101.200.176.0/24,47.94.36.0/24,47.94.47.0/24,101.201.214.0/24,101.201.82.0/24,123.56.182.0/24,101.201.105.0/24,182.92.132.0/24,60.205.157.0/24,101.201.107.0/24,60.205.164.0/24,60.205.165.0/24,59.110.4.0/24,59.110.17.0/24,123.56.186.0/24,60.205.146.0/24,59.110.37.0/24,59.110.19.0/24,60.205.112.0/24,60.205.243.0/24,59.110.38.0/24,60.205.197.0/24,60.205.166.0/24,101.200.194.0/24,101.200.182.0/24,123.57.204.0/24,101.200.235.0/24,123.57.206.0/24,123.57.65.0/24,47.94.167.117/32,182.92.157.129/32,101.200.39.123/32,101.200.192.4/32,39.105.58.165/32,101.200.213.59/32,59.110.164.0/24,47.94.150.0/24,39.105.56.0/24,47.93.21.0/24,47.93.30.0/24,47.93.24.0/24,60.205.222.0/24,60.205.186.0/24,47.93.22.174/32,47.93.10.168/32,47.94.246.43/32,47.94.94.233/32,47.95.241.173/32,59.110.155.242/32,60.205.230.219/32,101.200.50.74/32,101.201.65.33/32,112.126.96.49/32,112.126.96.184/32,112.126.98.30/32,112.126.99.22/32,112.126.99.87/32,112.126.99.205/32,39.105.247.0/24,8.131.132.0/26,39.105.161.255/32,123.56.70.208/32,101.200.120.94/32,123.57.238.231/32,182.92.217.14/32,47.94.240.86/32,47.94.2.56/32,59.110.226.187/32,47.94.210.30/32,47.93.236.163/32,47.94.212.10/32,47.95.241.0/24,101.201.152.0/24,47.93.10.0/24,182.92.217.0/24,112.126.96.0/24,101.200.192.0/24,120.55.129.0/24,47.102.181.0/24,47.102.234.0/24,47.101.109.0/24,123.56.244.0/24,101.200.215.0/24,123.56.43.0/24,101.200.72.0/24,123.56.100.0/24,123.57.166.0/24,182.92.196.0/24,101.200.141.0/24,123.57.136.0/24,123.57.5.0/24,182.92.0.0/24,39.106.90.0/24,123.56.128.0/24,123.57.205.0/24,101.200.189.0/24,101.200.209.0/24,112.124.140.0/24,120.55.129.0/24,47.102.181.0/24,47.102.234.0/24,47.101.109.0/24,100.104.143.0/26,100.104.201.0/26,100.104.247.64/26,100.104.232.128/26
China (Zhangjiakou)	47.92.22.0/24,47.92.185.0/26,47.92.185.64/26,47.92.185.128/26,47.92.185.192/26,39.98.96.0/26,39.98.96.128/26,39.98.96.192/26,39.98.96.64/26,39.101.252.128/26,47.92.22.110,47.92.22.16,47.92.22.131,47.92.22.169,47.92.22.212,47.92.22.211,47.92.22.210,47.92.22.209,47.92.22.208,47.92.22.68,120.55.129.0/24,47.102.181.0/24,47.102.234.0/24,47.101.109.0/24,112.124.140.0/24,120.55.129.0/24,47.102.181.0/24,47.102.234.0/24,47.101.109.0/24,100.104.144.128/26,100.104.84.128/26,100.104.52.0/26,100.104.32.64/26

Region	IP range
China (Hohhot)	39.104.29.0/24,120.55.129.0/24,47.102.181.0/24,47.102.234.0/24,47.101.109.0/24,112.124.140.0/24,120.55.129.0/24,47.102.181.0/24,47.102.234.0/24,47.101.109.0/24
China (Shenzhen)	120.78.6.0/24,120.78.5.0/24,47.115.165.0/24,47.115.166.0/24,47.115.162.0/24,47.115.161.0/24,120.24.65.0/24,120.24.67.0/24,120.24.160.0/24,120.25.215.0/24,120.24.214.0/24,120.24.223.0/24,120.25.124.0/24,120.25.107.0/24,120.25.79.0/24,112.74.211.0/24,120.24.174.0/24,120.24.173.0/24,120.25.150.0/24,112.74.98.0/24,120.25.123.0/24,112.74.97.0/24,47.106.221.0/24,120.78.184.0/24,47.107.118.0/24,47.106.38.0/24,39.108.66.0/24,39.108.110.0/24,47.113.76.192/26,120.25.248.86,120.24.64.155,120.25.105.105,47.106.37.166,47.112.160.156,120.79.71.173,120.79.74.179,112.74.44.248,120.79.72.217,120.79.68.184,120.79.71.129,120.55.129.0/24,47.102.181.0/24,47.102.234.0/24,47.101.109.0/24,120.77.195.128/26,120.77.195.192/26,47.106.63.192/26,112.124.140.0/24,120.55.129.0/24,47.102.181.0/24,47.102.234.0/24,47.101.109.0/24
China (Guangzhou)	8.134.79.124,8.134.79.169,8.134.79.140/30,112.124.140.0/24,120.55.129.0/24,47.102.181.0/24,47.102.234.0/24,47.101.109.0/24
China (Chengdu)	47.109.5.0/26,120.55.129.0/24,47.102.181.0/24,47.102.234.0/24,47.101.109.0/24,112.124.140.0/24,120.55.129.0/24,47.102.181.0/24,47.102.234.0/24,47.101.109.0/24,100.104.166.64/26,100.104.100.128/26,100.104.136.192/26,100.104.16.64/26
China (Hong Kong)	203.88.163.0/24,47.90.37.0/24,47.90.38.0/24,47.89.39.0/24,47.52.111.0/24,47.52.25.202/32,47.91.228.249/32,47.52.166.98/32,47.244.33.65/32,47.244.35.187/32,47.243.9.0/24,47.91.155.181,47.52.23.184,47.89.12.225,120.55.129.0/24,47.102.181.0/24,47.102.234.0/24,47.101.109.0/24,47.244.92.0/24,47.56.45.0/24,112.124.140.0/24,120.55.129.0/24,47.102.181.0/24,47.102.234.0/24,47.101.109.0/24,47.243.0.32/28
Singapore	47.88.235.0/24,47.88.139.0/24,161.117.146.128/26,161.117.146.192/26,161.117.164.0/26,161.117.164.64/26,47.88.235.0/24,47.88.139.0/24,161.117.146.128/26,161.117.146.192/26,161.117.164.0/26,161.117.164.64/26,47.88.235.0/24,47.88.139.0/24,161.117.146.128/26,161.117.146.192/26,161.117.164.0/26,161.117.164.64/26,161.117.234.42,47.241.209.7,47.241.217.237,10.88.51.0/24,112.124.140.0/24,120.55.129.0/24,47.102.181.0/24,47.102.234.0/24,47.101.109.0/24

Region	IP range
Australia (Sydney)	47.91.49.0/24,47.91.50.0/24,112.124.140.0/24,120.55.129.0/24,47.102.181.0/24,47.102.234.0/24,47.101.109.0/24
Malaysia (Kuala Lumpur)	47.254.212.0/24,120.55.129.0/24,112.124.140.0/24,112.124.140.0/24,120.55.129.0/24,47.102.181.0/24,47.102.234.0/24,47.101.109.0/24
Indonesia (Jakarta)	149.129.228.0/24,149.129.229.0/24,147.139.156.0/24,112.124.140.0/24,120.55.129.0/24,47.102.181.0/24,47.102.234.0/24,47.101.109.0/24
Thailand (Bangkok)	8.213.0.128/26,8.213.0.192/26,8.213.5.0/26,8.213.5.64/26
India (Mumbai)	149.129.164.0/24,147.139.21.0/24,147.139.23.0/24,149.129.165.192/26,147.139.23.0/26,147.139.23.128/26,147.139.23.64/26,149.129.165.192/26,112.124.140.0/24,120.55.129.0/24,47.102.181.0/24,47.102.234.0/24,47.101.109.0/24
Japan (Tokyo)	47.91.9.0/24,47.91.13.0/24,47.91.27.0/24,47.245.18.0/24,47.245.51.0/24,47.91.0.192/26,47.91.0.128/26,112.124.140.0/24,120.55.129.0/24,47.102.181.0/24,47.102.234.0/24,47.101.109.0/24,47.88.1.17,47.88.6.196,47.88.10.217,47.88.15.174,47.245.51.128/26,47.245.51.192/26,8.209.192.160/28
US (Silicon Valley)	198.11.174.0/24,198.11.175.0/24,47.89.244.175/32,112.124.140.0/24,120.55.129.0/24,47.102.181.0/24,47.102.234.0/24,47.101.109.0/24,100.104.166.64/26,100.104.100.128/26,100.104.136.192/26,100.104.16.64/26,47.88.98.0/26,47.88.98.64/26,47.88.98.128/26,47.88.98.192/26
US (Virginia)	47.89.170.0/24,47.88.98.0/24,47.250.29.0/24,112.124.140.0/24,120.55.129.0/24,47.102.181.0/24,47.102.234.0/24,47.101.109.0/24,47.253.64.0/28
Germany (Frankfurt)	47.89.170.0/24,47.88.98.0/24,47.250.29.0/24,112.124.140.0/24,120.55.129.0/24,47.102.181.0/24,47.102.234.0/24,47.101.109.0/24
UK (London)	8.208.17.0/24,8.208.72.0/24,47.91.82.0/24,47.91.83.0/24,112.124.140.0/24,120.55.129.0/24,47.102.181.0/24,47.102.234.0/24,47.101.109.0/24
UAE (Dubai)	47.91.102.0/24,47.91.103.0/246,112.124.140.0/24,120.55.129.0/24,47.102.181.0/24,47.102.234.0/24,47.101.109.0/24,100.104.161.0/26,100.104.53.0/26,100.104.111.128/26,100.104.248.128/26

Region	IP range
South Korea (Seoul)	149.129.13.0/26,149.129.13.64/26,149.129.14.128/26,149.129.14.192/26
SAU (Riyadh)	8.213.0.128/26,8.213.0.192/26,8.213.5.0/26,8.213.5.64/26

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:

> **Note** When DTS adds new servers, your user-created database may become inaccessible if you do not update the whitelist settings in a timely manner. To avoid this issue, we recommend that you whitelist the 100.104.0.0/16 IP range for all user-created databases that are reachable from an internal network.

Region	IP range
China (Hangzhou)	100.104.52.0/24,100.104.61.128/26,100.104.244.64/26,100.104.216.192/26,100.104.85.0/26,100.104.221.128/26,100.104.2.0/26,100.104.251.192/26,100.104.159.64/26,100.104.216.128/26
China (Shanghai)	100.104.205.0/24,100.104.226.128/26,100.104.149.64/26,100.104.241.128/26,100.104.177.128/26,100.104.203.192/26
China (Qingdao)	100.104.72.0/24,100.104.35.192/26,100.104.12.0/26,100.104.111.0/26
China (Beijing)	100.104.183.0/24,100.104.236.128/26,100.104.227.192/26,100.104.128.192/26,100.104.11.64/26,100.104.84.128/26,100.104.200.64/26
China (Zhangjiakou)	100.104.175.0/24,100.104.249.0/26,100.104.180.192/26
China (Hohhot)	100.104.72.0/24
China (Shenzhen)	100.104.75.64/26,100.104.235.192/26,100.104.205.0/24,100.104.41.64/26,100.104.171.128/26
China (Guangzhou)	100.104.132.64/26,100.104.240.128/26,100.104.122.128/26,100.104.233.0/26
China (Chengdu)	100.104.76.192/26,100.104.145.64/26,100.104.235.192/26,100.104.127.0/26
China (Hong Kong)	100.104.233.0/24,100.104.177.192/26,100.104.158.192/26,100.104.180.192/26

Region	IP range
Singapore	100.104.188.0/24,100.104.207.128/26,100.104.12.0/26,100.104.179.64/26,100.104.12.0/26,10.88.51.0/24
Australia (Sydney)	100.104.233.0/24,100.104.3.128/26
Malaysia (Kuala Lumpur)	100.104.5.0/24,100.104.36.0/26,100.104.234.192/26,100.104.76.192/26
Indonesia (Jakarta)	100.104.175.0/24,100.104.35.192/26
Philippines (Manila)	100.104.153.64/26,100.104.76.192/26,100.104.246.192/26
Thailand	100.104.150.192/26
India (Mumbai)	100.104.8.0/24,100.104.127.0/26
Japan (Tokyo)	100.104.112.0/24,100.104.117.192/26,100.104.12.0/26,100.104.166.64/26
US (Silicon Valley)	100.104.175.0/24,100.104.48.128/26,100.104.166.64/26,100.104.108.128/26
US (Virginia)	100.104.233.0/24,100.104.240.128/26,100.104.132.64/26,100.104.177.192/26,100.104.12.0/26,100.104.111.0/26
Germany (Frankfurt)	100.104.5.0/24,100.104.193.128/26
UK (London)	100.104.133.64/26,100.104.207.128/26
UAE (Dubai)	100.104.205.0/24
South Korea (Seoul)	100.104.119.128/26,100.104.153.64/26,100.104.76.192/26,100.104.246.192/26,100.104.106.192/26,100.104.210.128/26
SAU (Riyadh)	100.104.76.192/26,100.104.210.128/26,100.104.48.128/26,100.104.69.0/26,100.104.87.192/26,100.104.145.64/26

Whitelist the IP range

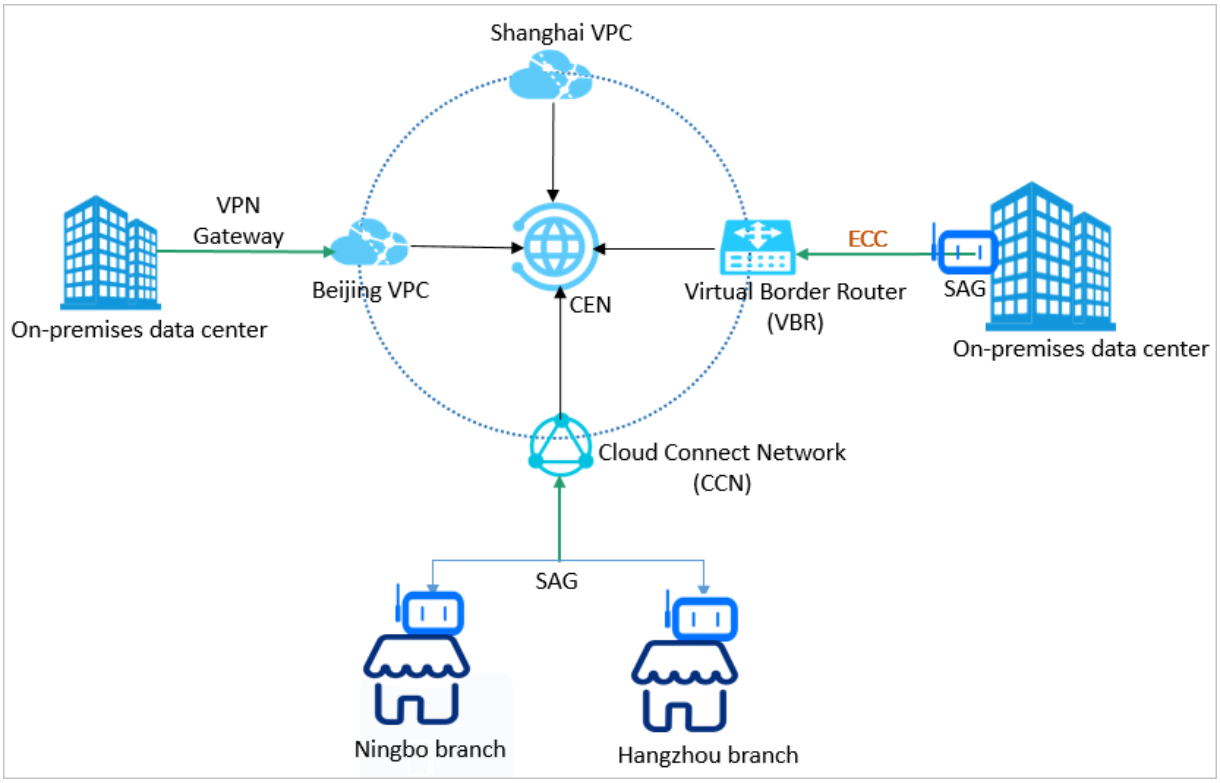
After obtaining the IP range, you need to whitelist the IP range in the security settings of your user-created database system. The actual procedure may vary, depending on your system deployment. For example, if your database is deployed behind a firewall, you need to configure the security rules to 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 建立VPC到本地数据中心的连接.
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 Establish active/standby connections between a data center and Alibaba Cloud and Establish active/active connections between a data center and Alibaba Cloud.
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 the Chinese mainland 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

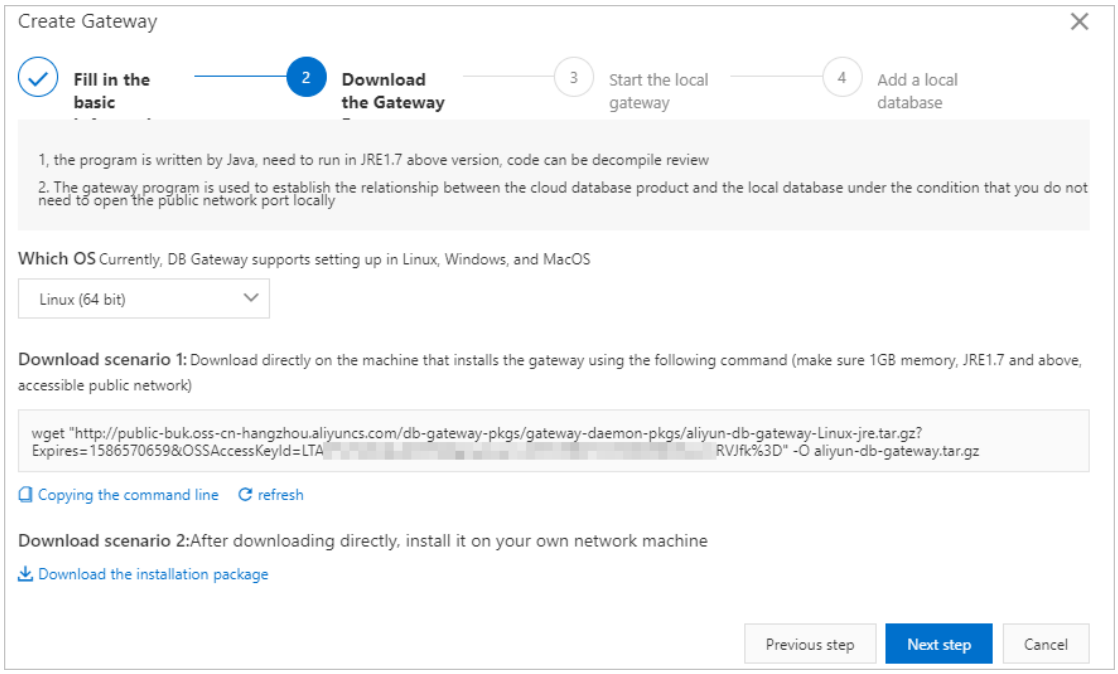
1. Log on to the Database Gateway console.

   > **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.

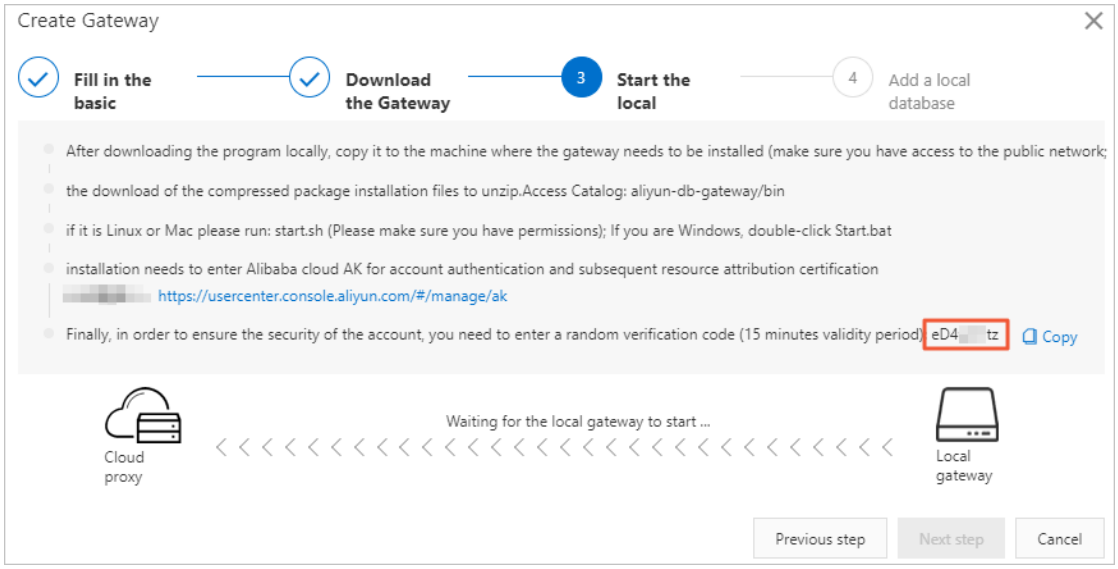
ii. Select one of the following methods to start the gateway program, depending on your operating system:

- 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.

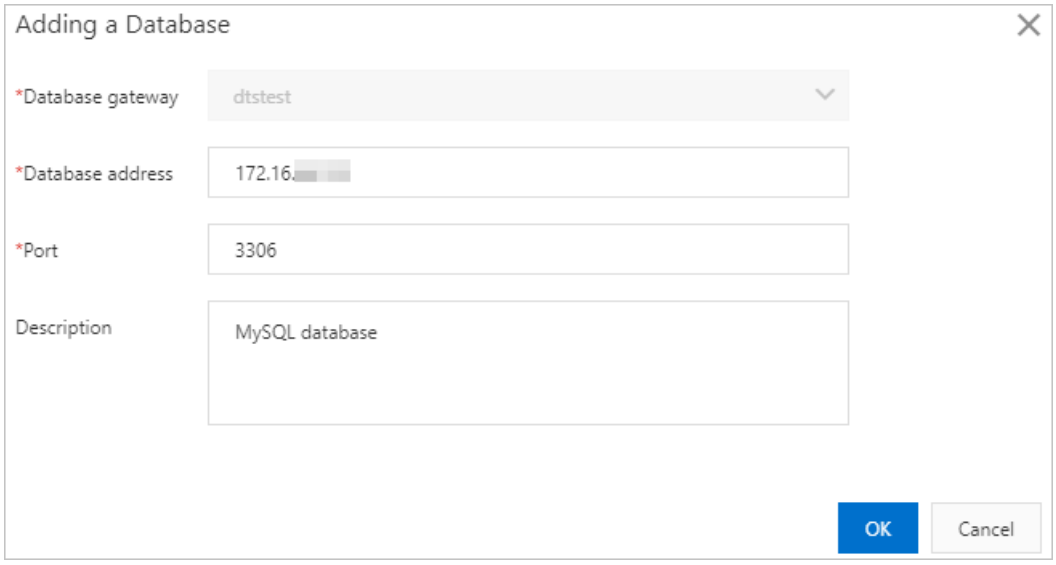
```
Validating the validity of the database gateway validation code...
Congratulations, the validation of local accounts and gateways has all passed. Now start the r
everse channel...
waiting for connection established...

.
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**.

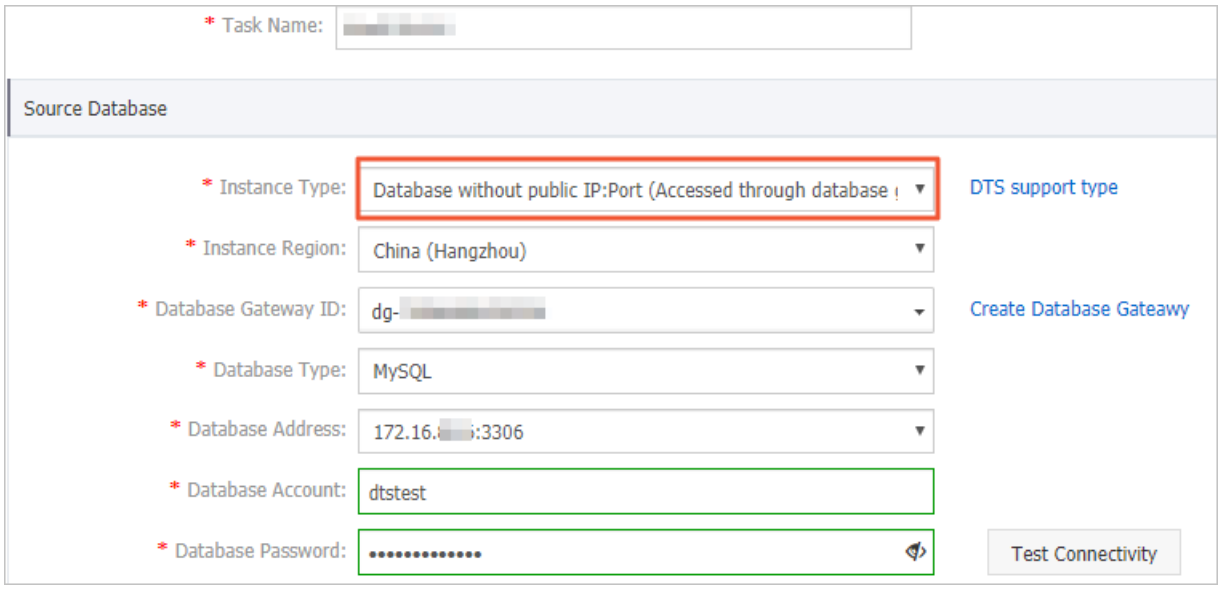
ii. In the dialog box that appears, enter the address and port number of the database server, enter a description for the server connection, and then click **OK**. The address must be reachable from the server that is running the gateway program. If the gateway program is running on the same server as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



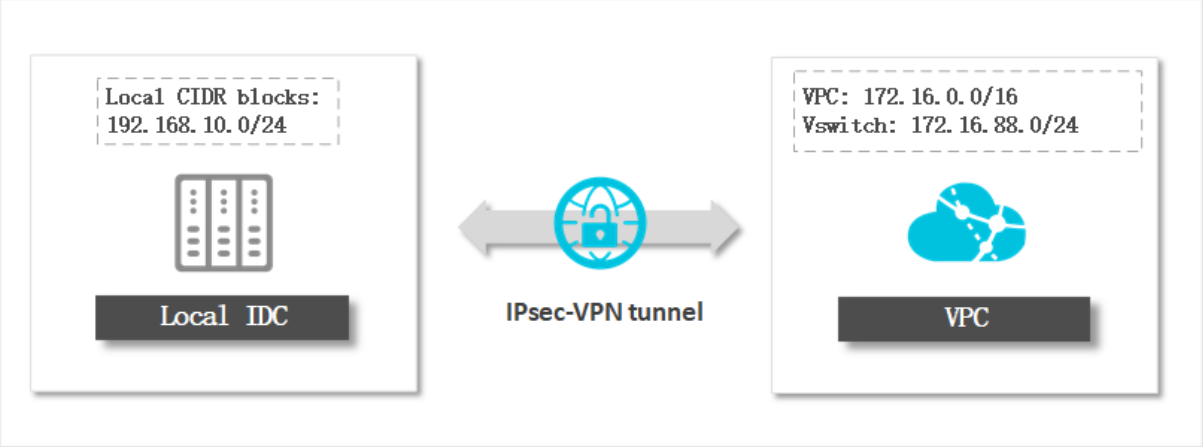
5.Connect your on-premises networks to Alibaba Cloud over an IPsec-VPN tunnel

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 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 Pay-as-you-go.

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 **Interconnections > VPN > VPN Gateways**.
4. On the **VPN Gateways** page, click **Create VPN Gateway**.
5. Complete the VPN gateway settings as follows:
   - **Name**: Enter a name for the VPN gateway.
   - **Region**:Select the region where you want to deploy the VPN gateway.

     > **Note** Make sure that the VPC and the VPN gateway are deployed in the same region.

   - **VPC**:Select the VPC to be associated with the VPN gateway.
   - **Specify vSwitch**: Specify whether to create the VPN gateway in a vSwitch of the VPC. In this example, **No** is selected.

     If you select **Yes**, you must also specify a **vSwitch**.
   - **Peak Bandwidth**: Select a maximum bandwidth value for the VPN gateway. Unit: Mbit/s.
   - **Traffic**: By default, the VPN gateway uses the pay-by-data-transfer billing method.
   - **IPsec-VPN**: Specify whether to enable IPsec-VPN for the VPN gateway. In this example, **Enable** is selected.
   - **SSL-VPN**: Specify whether to enable SSL-VPN. In this example, **Disable** is selected.
   - **Duration**: By default, the VPN gateway is billed on an hourly basis.
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 **Interconnections > 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.

Parameter	Description
ASN	Enter the autonomous system number (ASN) of the gateway device in the 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 **Interconnections > VPN > IPsec Connections**.
4. Click **Create IPsec Connection**.
5. In the **Create IPsec Connection** pane, complete the settings as follows:

Parameter	Description
Name	Enter a name for the IPsec-VPN connection. The name must be 2 to 128 characters in length and can contain digits, hyphens (-), and underscores (_). It must start with a letter.
VPN Gateway	Select the standard VPN gateway to be connected through the IPsec-VPN connection.
Customer Gateway	Select the customer gateway to be connected through the IPsec-VPN connection.

Parameter	Description
Routing Mode	Select a routing mode. Default value: **Destination Routing Mode**. ○ **Destination Routing Mode**: forwards traffic to specified destination IP addresses. After you create an IPsec-VPN connection, you must add destination-based routes to the route table of the VPN gateway. ○ **Protected Data Flows**: forwards traffic based on source and destination IP addresses. If you select **Protected Data Flows** when you create an IPsec-VPN connection, you must configure **Local Network** and **Remote Network**. After you complete the configurations, the system automatically adds policy-based routes to the route table of the VPN gateway. After the system adds policy-based routes to the route table of the VPN gateway, the routes are not advertised by default. You must manually advertise the routes to the VPC. **Note** ○ If you use an earlier version of VPN Gateway, you do not need to select a routing mode. After you create an IPsec-VPN connection, you must manually add destination-based routes or policy-based routes to the VPN gateway. ○ Do not create a route that meets the following conditions: The destination CIDR block is 100.64.0.0/10 or one of its subnets. The next hop is an IPsec-VPN connection. If you create such a route, one of the following errors occurs: The status of the IPsec-VPN connection cannot be displayed in the console. The negotiations of the IPsec-VPN connection fail.
Local Network	Enter the CIDR block on the VPC side. The CIDR block is used in Phase 2 negotiations. Click + next to the field to add multiple CIDR blocks on the VPC side. **Note** You can add multiple CIDR blocks only if IKEv2 is used.

Parameter	Description
Remote Network	Enter the CIDR block on the data center side. This CIDR block is used in Phase 2 negotiations. Click + next to the field to add multiple CIDR blocks on the data center side. **Note** You can add multiple CIDR blocks only if IKEv2 is used.
Effective Immediately	Specify whether to immediately start negotiations. ○ **Yes**: starts connection negotiations after the configuration is completed. ○ **No**: starts negotiations when inbound traffic is detected.
Pre-Shared Key	Enter the pre-shared key that is used for identity authentication between the VPN gateway and the data center. The key must be 1 to 100 characters in length. If you do not specify a pre-shared key, the system randomly generates a 16-bit string as the pre-shared key. After you create an IPsec-VPN connection, you can click **Edit** to view the pre-shared key that is generated by the system. **Notice** The pre-shared key of the IPsec-VPN connection must be the same as the authentication key of the data center. Otherwise, you cannot establish a connection between the data center and the VPN gateway.
Advanced Configuration: IKE Configurations	
Version	Select an IKE version. ○ **ikev1** ○ **ikev2** IKEv1 and IKEv2 are supported. Compared with IKEv1, IKEv2 simplifies the SA negotiation process and provides better support for scenarios in which multiple CIDR blocks are used. We recommend that you select IKEv2.
Negotiation Mode	Select a negotiation mode. ○ **main**: This mode offers higher security during negotiations. ○ **aggressive**: This mode is faster and has a higher success rate. Connections negotiated in both modes ensure the same level of security for data transmission.
Encryption Algorithm	Select the encryption algorithm that is used in Phase 1 negotiations. Supported algorithms are **aes**, **aes192**, **aes256**, **des**, and **3des**.
Authentication Algorithm	Select the authentication algorithm that is used in Phase 1 negotiations. Supported algorithms are **sha1**, **md5**, **sha256**, **sha384**, and **sha512**.

Parameter	Description
DH Group	Select the DH key exchange algorithm that is used in Phase 1 negotiations. The following DH groups are supported: ○ **group1**: DH group 1 ○ **group2**: DH group 2 ○ **group5**: DH group 5 ○ **group14**: DH group 14
SA Life Cycle (seconds)	Specify the lifecycle of the SA after Phase 1 negotiations succeed. Unit: seconds. Default value: **86400**. Valid values: **0 to 86400**.
LocalId	Specify the identifier of the VPN gateway that is used in Phase 1 negotiations. The default value is the public IP address of the VPN gateway. If you set LocalId to a fully qualified domain name (FQDN), we recommend that you set Negotiation Mode to **aggressive**.
RemoteId	Specify the identifier of the customer gateway that is used in Phase 1 negotiations. The default value is the public IP address of the customer gateway. If you set RemoteId to an FQDN, we recommend that you set Negotiation Mode to **aggressive**.
Advanced Configuration: IPSec Configurations	
Encryption Algorithm	Select the encryption algorithm that is used in Phase 2 negotiations. Supported algorithms are **aes**, **aes192**, **aes256**, **des**, and **3des**.
Authentication Algorithm	Select the authentication algorithm that is used in Phase 2 negotiations. Supported algorithms are **sha1**, **md5**, **sha256**, **sha384**, and **sha512**.
DH Group	Select the DH key exchange algorithm that is used in Phase 2 negotiations. Standard VPN gateways support the following values: ○ **disabled**: does not use a DH key exchange algorithm. ■ For clients that do not support perfect forward secrecy (PFS), select **disabled**. ■ If you select a value other than **disabled**, the PFS feature is enabled by default, which requires a key update for every renegotiation. Therefore, you must also enable PFS for the client. ○ **group1**: DH group 1 ○ **group2**: DH group 2 ○ **group5**: DH group 5 ○ **group14**: DH group 14
SA Life Cycle (seconds)	Specify the lifecycle of the SA after Phase 2 negotiations succeed. Unit: seconds. Default value: **86400**. Valid values: **0 to 86400**.
DPD	Specify whether to enable the DPD feature. This feature is enabled by default.

Parameter	Description
NAT Traversal	Specify whether to enable the NAT traversal feature. This feature is enabled by default.
BGP Configuration	
Tunnel CIDR Block	Enter the CIDR block of the IPsec tunnel. The CIDR block must fall within 169.254.0.0/16. The subnet mask of the CIDR block must be 30 bits in length.
Local BGP IP address	Enter the BGP IP address on the VPC side. This IP address must fall within the CIDR block of the IPsec tunnel. **Note** Make sure that the BGP IP addresses on the VPC side and on the data center side do not conflict with each other.
Local ASN	Enter the autonomous system number (ASN) on the VPC side. Valid values: **1 to 4294967295**. Default value: **45104**. **Note** We recommend that you use a private ASN to establish a connection with Alibaba Cloud over BGP. Refer to the relevant documentation for the valid range of a private ASN.
Health Check	
Destination IP	Enter the IP address on the data center side that the VPC can communicate with through the IPsec-VPN connection.
Source IP	Enter the IP address on the VPC side that the data center can communicate with through the IPsec-VPN connection.
Retry Interval	Specify the interval between two consecutive health checks. Unit: seconds.
Number of Retries	Specify the maximum number of health check retries.

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**.

Setting	Description
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 **Interconnections > VPN > IPsec Connections**.
4. Find the target IPsec-VPN connection and choose ⋮ **> 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.

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.