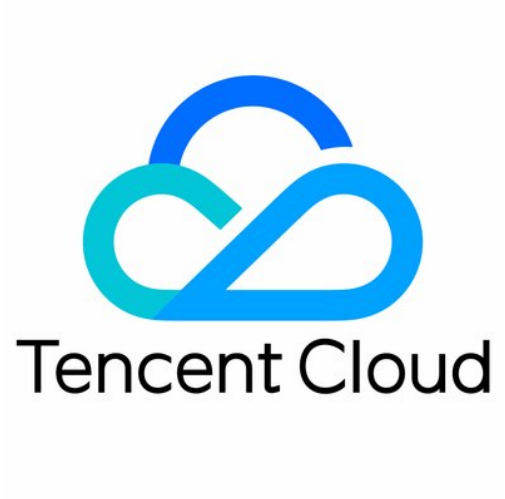
Data Transmission Service

Preparations

Product Documentation



Contents

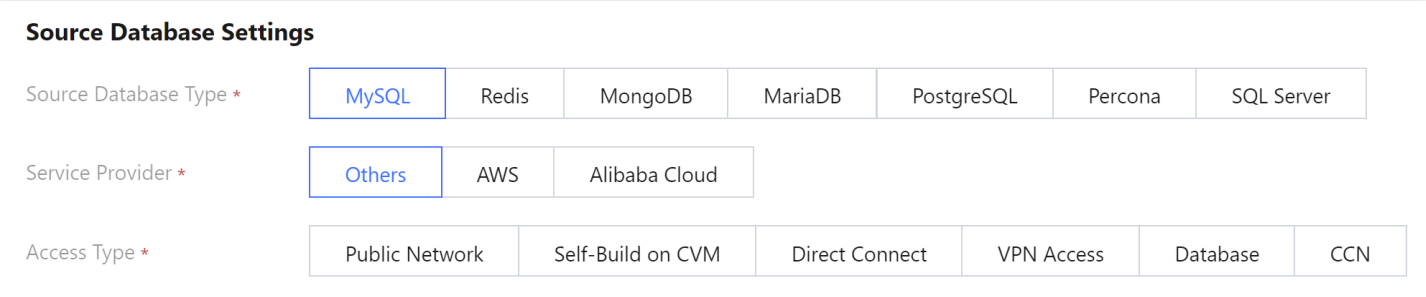
Preparations

Overview

Last updated：2022-09-21 17:24:21

Overview

When creating a migration, sync, or subscription task, you need to select different access types based on the deployment conditions of your source database. This document describes how to select an access type and prepare accordingly.



Prerequisites

Note：
Determine the access type in advance. For the same source and target databases, if an access type such as **Public Network** is selected and the connectivity verification is passed, you cannot switch to another access type such as **Direct Connect**; otherwise, an error will be reported during connectivity verification.

- If the source database is an IDC-based self-built database or a third-party cloud database, you can select **Public Network** generally. If you require a higher transfer performance, you can select **VPN Access**, **Direct Connect**, or **CCN** based on your actual network conditions.
- If the source database is a TencentDB instance, select **Database**.
- If the source database is a CVM-based self-built database, select **Self-Build on CVM**.

Access Type	Use Case	Operation Guide

Access Type	Use Case	Operation Guide
Public Network	• The source database can be accessed through a public IP. • The public network option cannot guarantee the transfer bandwidth and is applicable to scenarios with low requirements for the transfer performance.	Manually add the SNAT IP of the DTS server to the allowlist (generally the firewall) of the self-built database as instructed in Adding DTS IP Address to Database Allowlist to connect the source database and DTS instance.
Direct Connect/VPN Access	• The source database can be interconnected with VPCs through VPN Connections or Direct Connect. • The network bandwidth of Direct Connect is guaranteed.	• Configure VPN-IDC interconnection as instructed in Direct Connect or VPN Access: Configuring VPN-IDC Interconnection. • Manually add the SNAT IP of the DTS server to the allowlist (generally the firewall) of the self-built database as instructed in Adding DTS IP Address to Database Allowlist to connect the source database and DTS instance.
CCN	The source database can be interconnected with VPCs through CCN.	• Configure VPC-IDC interconnection through CCN as instructed in CCN Access: Configuring VPC-IDC Interconnection Through CCN. • Manually add the SNAT IP of the DTS server to the allowlist (generally the firewall) of the self-built database as instructed in Adding DTS IP Address to Database Allowlist.
Self-Build on CVM	The source database is deployed in a CVM instance.	Manually add the SNAT IP of the DTS server to the security group of the CVM instance as instructed in Adding DTS IP Address to Database Allowlist to connect the source database and DTS instance.
VPC	The source and target databases are both deployed in Tencent Cloud VPCs.	Manually add the SNAT IP address of the DTS server to the security group of the source database as instructed in Adding DTS IP Address to Database Allowlist. To use the VPC access type, submit a ticket for application.

Access Type	Use Case	Operation Guide
Database	The source database is a TencentDB instance.	• If the source database is a TencentDB for MySQL, TencentDB for PostgreSQL, TDSQL-C for PostgreSQL, TDSQL for TDStore, TDSQL for PostgreSQL, or TDSQL-A for PostgreSQL instance, DTS will automatically add the SNAT IP address of the DTS server to the security group rule of the source database. • For other database types, you need to do so manually as instructed in Adding DTS IP Address to Database Allowlist.

Note：

- Manually or automatically adding the SNAT IP address of the DTS server to the security group or allowlist of the source database may cause certain security risks to the source database. Therefore, you should enhance security protection measures when performing such operations; for example, you can standardize account password management, require authentication for API communication, and restrict unnecessary IP ranges. By using DTS, you acknowledge the existence of risks. If you have high security requirements, we recommend you use Direct Connect, VPN, or VPC for access.
- After using DTS, we recommend you delete the DTS IP address from the security group or firewall promptly.

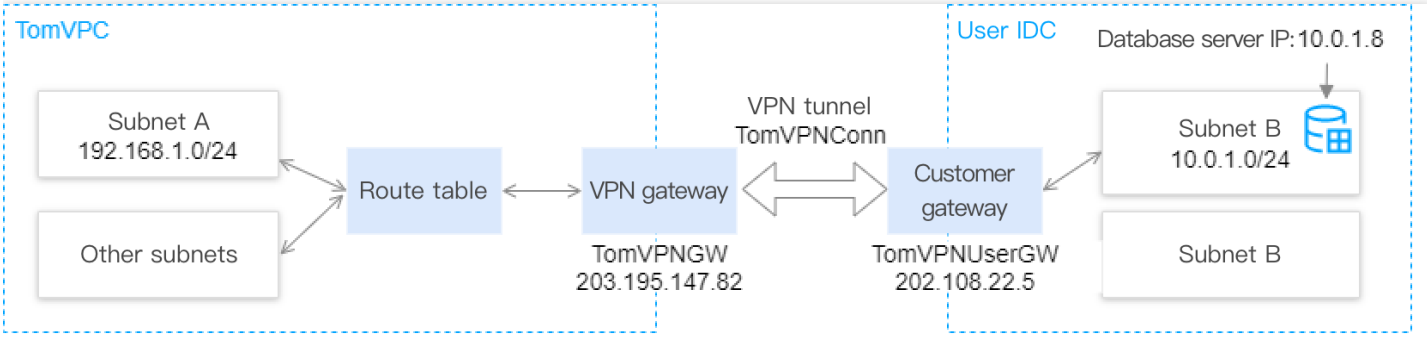
Direct Connect or VPN Access: Configuring VPN-IDC Interconnection

Last updated：2021-12-27 11:20:37

Overview

If the access type is VPN gateway, you need to create a VPC and VPN and establish a tunnel between the VPN and IDC for interconnection.

In this scenario, your VPC is "TomVPC", your subnet is "subnet A", and the IP range of “subnet A” is `192.168.1.0/24`. The created VPN gateway is "TomVPNGW", the public IP of the VPN gateway is `203.195.147.82`, the subnet IP range of your IDC is `10.0.1.0/24`, the public IP of the VPN gateway in your IDC is `202.108.22.5`, and the IP address of the source database server is `10.0.1.8`.



Directions

Configure as instructed in Overview.

Subsequent Steps

1. After the VPN is connected to your IDC, on the DTS task page, select **VPN Access**.

Parameter	Description	Sample Value

Parameter	Description	Sample Value
VPN Gateway	Name of the VPN gateway created in the VPC.	TomVPNGW
VPC	Name of your VPC.	TomVPC
Subnet	Name of the subnet of your VPC.	Subnet A
Host Address	IP address of the source database server.	10.0.1.8
Port	Port used by the source database. Below are the default ports for common databases (if they are modified, enter the actual ports): ◦ MySQL: 3306 ◦ SQL Server: 1433 ◦ PostgreSQL: 5432 ◦ MongoDB: 27017 ◦ Redis: 6379	3306

2. Click **Test Connectivity**. If the test fails, troubleshoot as follows:
   - The Telnet test fails.

     In the created VPC ("TomVPC" in this example), purchase a CVM instance and ping the source database server address from it:
     - If the address is unpingable:
       - The source database has a security group or firewall configured.
       - The SNAT IP address is blocked in the source database.
       - The port settings of the source database are incorrect.
     - If the address is pingable:

       Submit a ticket for assistance.
   - The Telnet test is passed, but the database connection fails.
     - The migration account is not properly authorized. Authorize it again as instructed in the corresponding scenario in data migration and data sync.
     - The account or password is incorrect.

CCN Access: Configuring VPC-IDC Interconnection Through CCN

Last updated：2022-09-07 14:24:00

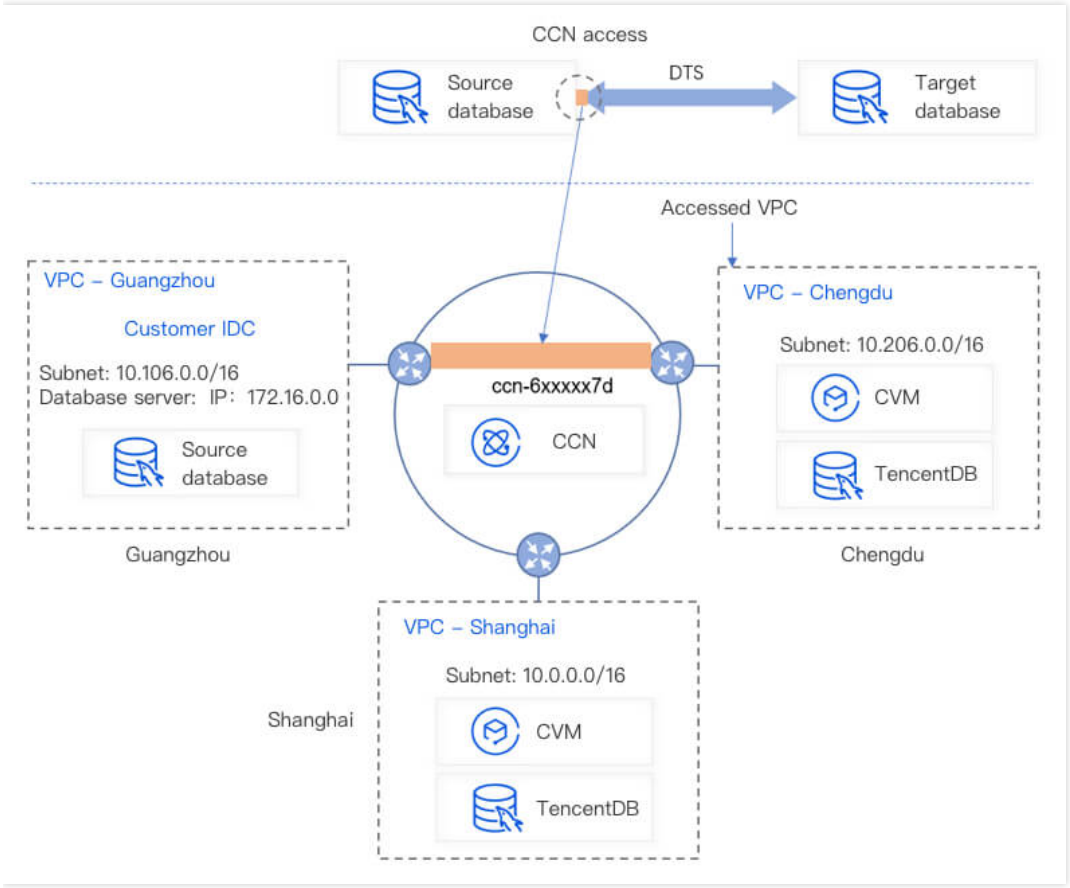
Overview

CCN can interconnect a VPC with another VPC or a local IDC. To use CCN access, you must establish cross-VPC and VPC-IDC interconnections through CCN in advance.

In this scenario, you have used CCN to interconnect the three networks of VPC-Guangzhou, VPC-Chengdu, and VPC-Shanghai, have a self-built database in Guangzhou, and plan to migrate the data in the source database in Guangzhou to the target database in Nanjing. VPC-Chengdu is selected as the **Accessed VPC**.

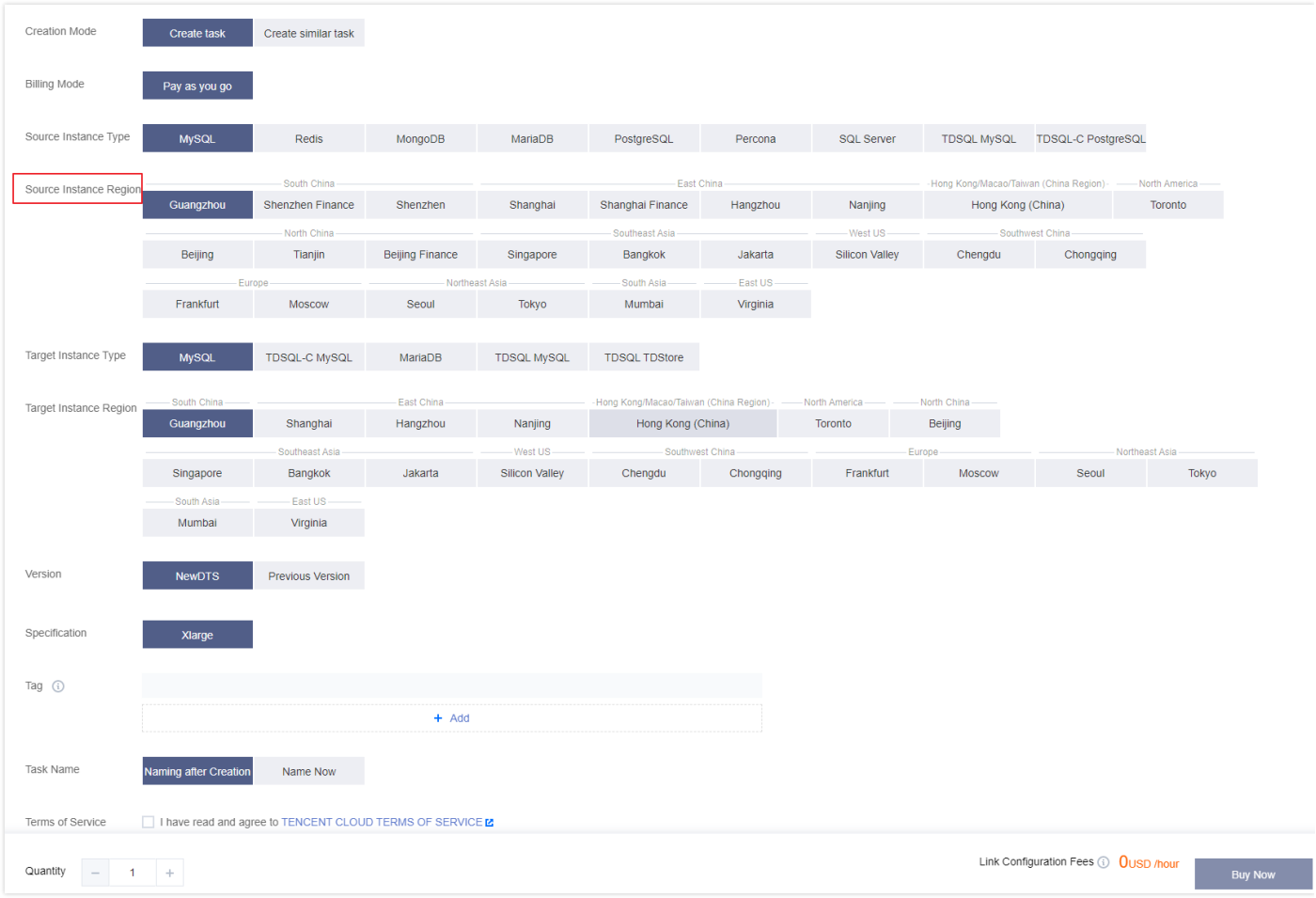
Configuration principles

When selecting CCN access, you need to connect the source database to the source of the DTS migration/sync linkage over CCN as follows: source database > accessed VPC > source of the migration/sync linkage, as shown in orange below.



The accessed VPC and the source of the migration/sync linkage are interconnected as follows in the entire DTS task:

- The source of the migration/sync linkage is the network in the region of the source database selected during the task purchase, as shown below:
  The region of the source database selected during task purchase must be the same as the region of the accessed VPC; otherwise, the networks cannot be interconnected, and DTS will change the former to the latter.



- Accessed VPC: The accessed VPC refers to the VPC in CCN over which the migration/sync linkage is connected. It can be configured when you set the source and target databases as shown below:
  The accessed VPC and the VPC of the source database are interconnected over CCN.

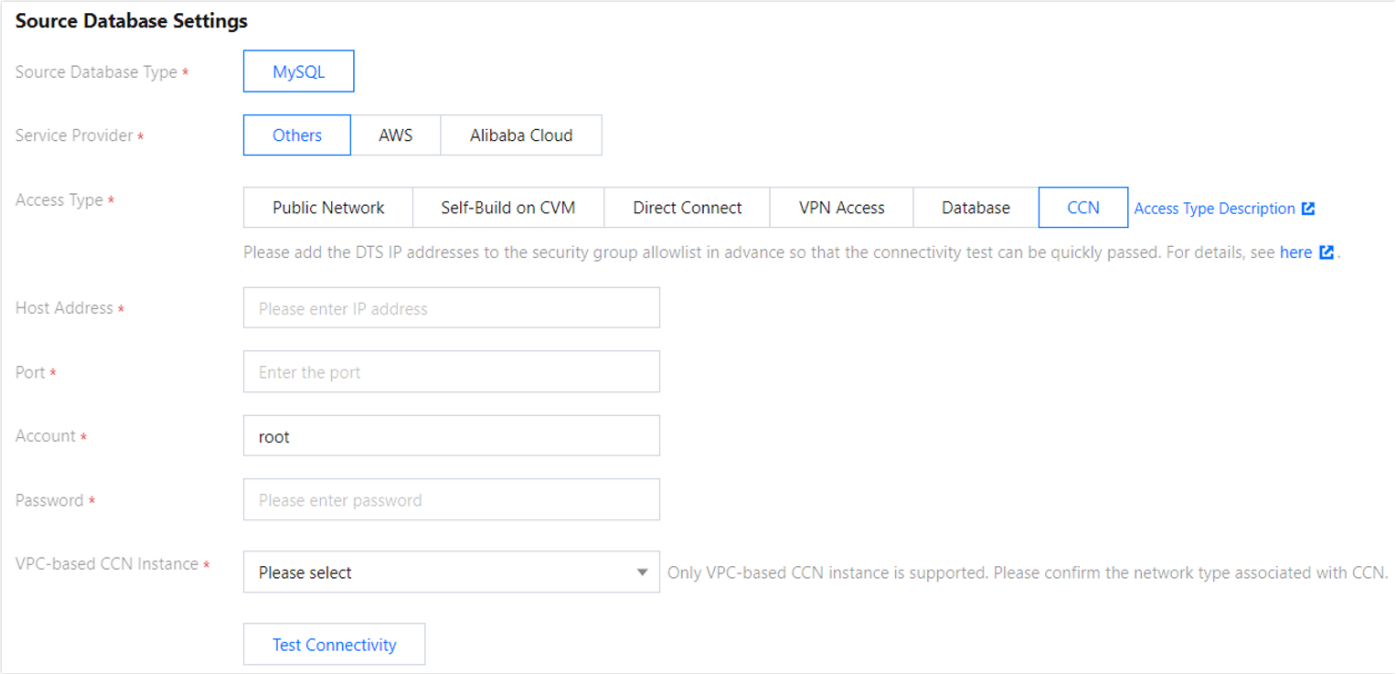
Directions

Establish interconnections as instructed in Connecting Network Instances Under the Same Account.

> Note：
> CCN only provides bandwidth below 10 Kbps between all regions free of charge. However, DTS requires a higher bandwidth. Therefore, bandwidth configuration in the link is required.

Subsequent operations

1. To perform a data migration task or data sync task, you need to configure relevant parameters. Here, data migration from MySQL is used as an example. In the **Set source and target databases** step of the data migration task, select **CCN** and configure key parameters as follows:



Parameter	Description	Sample Value
Host Address	IP address of the source database server.	172.16.0.0
Port	Port used by the source database. Below are the default ports for common databases (if they are modified, enter the actual ports): ◦ MySQL: 3306 ◦ SQL Server: 1433 ◦ PostgreSQL: 5432 ◦ MongoDB: 27017 ◦ Redis: 6379	3306
VPC-based CCN Instance	CCN instance name.	ccn6-xxxx7d

Parameter	Description	Sample Value
Accessed VPC	The accessed VPC refers to the VPC in CCN over which the migration/sync linkage is connected. You need to select a CCN-associated VPC other than the VPC where the source database resides. For example, if the database in Guangzhou region is selected as the source database, you should select **VPC-Chengdu** or **VPC-Shanghai** as the **accessed VPC**. Here, **Chengdu-VPC** is selected.	VPC-Chengdu
Subnet	Name of the subnet of the selected VPC. If you cannot pull the subnet, there may be a problem with your account. The account of the accessed VPC must be the same as the migration account. For example, to migrate a database under account A to account B, you should use account B to create a task. Therefore, the accessed VPC must be under account B.	VPC-Chengdu-Subnet
Region of Accessed VPC	The region of the source database selected during task purchase must be the same as the region of the accessed VPC; otherwise, DTS will change the former to the latter.	Chengdu

2. Click **Test Connectivity**. If the test fails, troubleshoot as follows:

- The Telnet test fails.
  In the CCN-associated VPC (VPC-Chengdu in this example), purchase a CVM instance and ping the source database server address from it:
  - If the address is unpingable:
  - The server where the source database resides has a security group or firewall configured as described in Database Connection Check.
  - The SNAT IP address is blocked in the source database as described in Database Connection Check.
  - The port settings of the source database are incorrect.
  - Some route tables in the CCN instance are not enabled due to IP range conflicts.
  - If the address is pingable, the routing between the source database and CCN is normal.
  - The selected CCN-associated VPC is incorrect.
    The CCN-associated VPC and host address cannot be in the same region (if the network environment of the source database is a VPC in Guangzhou, you cannot select another VPC in Guangzhou as the CCN-associated VPC). The CCN-associated VPC and host address cannot be in the same VPC (if the network environment of the source database is VPC-A, you cannot select VPC-A as the CCN-associated VPC).
  - Submit a ticket for assistance.
- The Telnet test is passed, but the database connection fails.

- The migration account is not properly authorized. Authorize it again as instructed in the corresponding scenario in Migration from MySQL to TencentDB for MySQL and data sync.
- The account or password is incorrect.

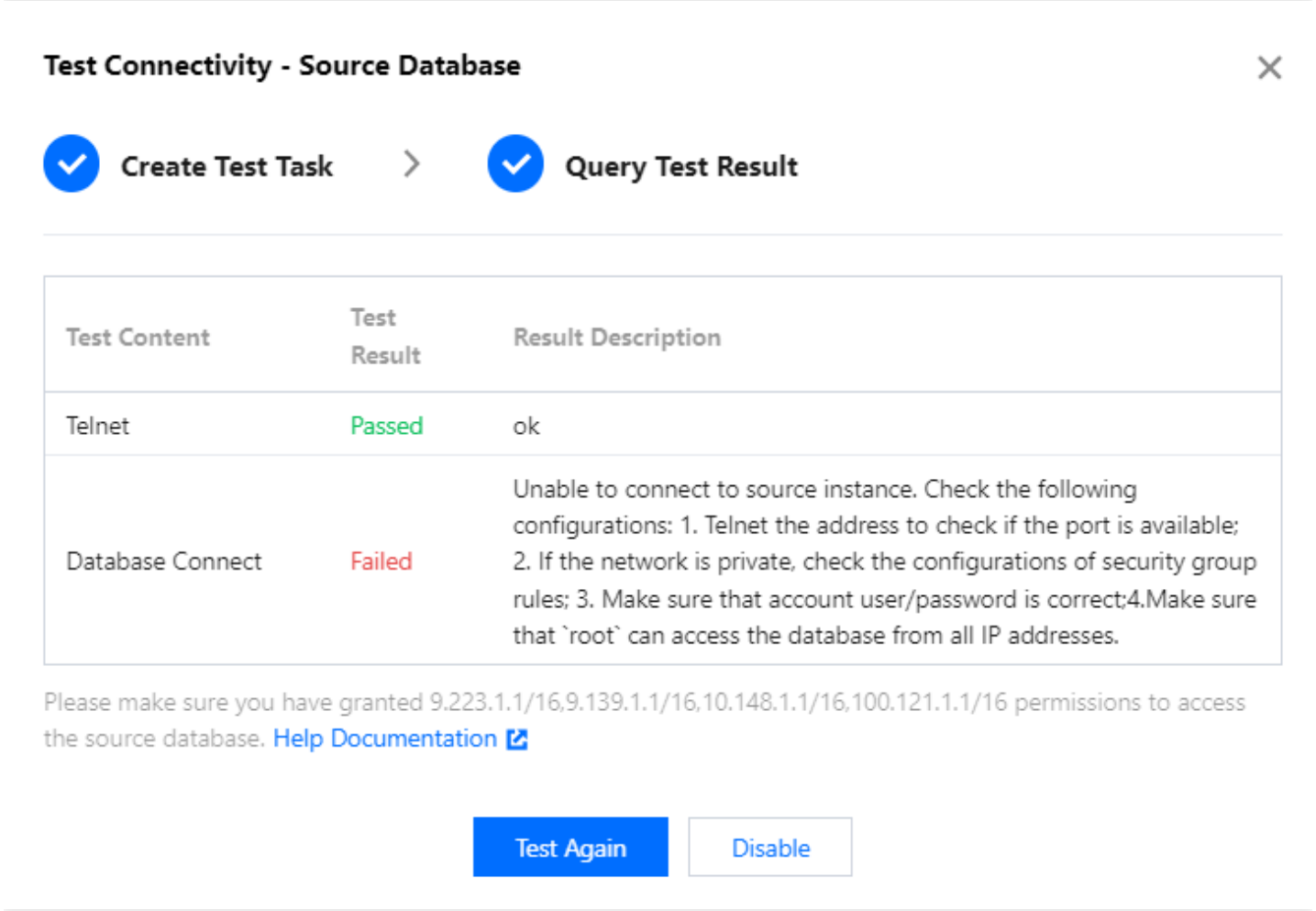
Adding DTS IP Address to Database Allowlist

Last updated：2022-08-26 17:52:47

Overview

When creating a data migration, sync, or subscription task, you need to add the DTS IP address to the allowlists of the source and target databases so that they can communicate with each other.

If you don't add the DTS IP address to the database allowlists, the connectivity test may fail, and you will be prompted to do so if the test fails.



Principle

Add the IP addresses for each region to the source or target database allowlist. For IP address information, see DTS IP Addresses.

> Note：
> If the source or target database is TencentDB for MySQL or TencentDB for PostgreSQL, the DTS IP address will be automatically added to the database's security group rule; otherwise, it must be added to the allowlist manually.

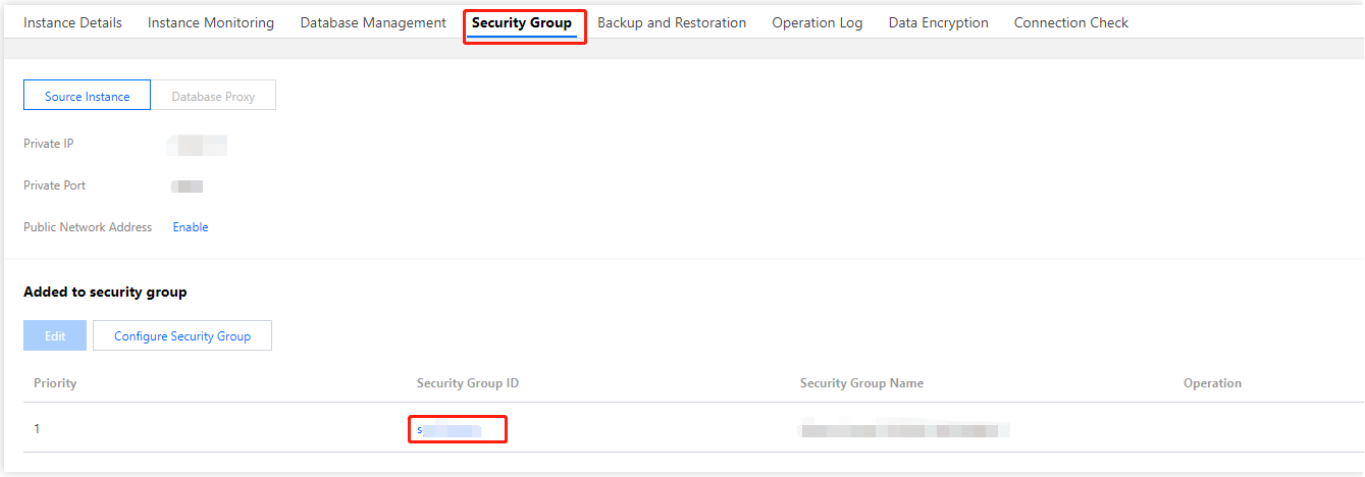
Example 1: If the source database is self-built MySQL in Beijing region and the target database is TencentDB for MySQL in Guangzhou region, you need to get the IP address for Beijing region from DTS IP Addresses and add it to the source database allowlist. As the target database is TencentDB for MySQL, the DTS IP address is automatically added to the target database allowlist.

Example 2: If the source database is self-built MongoDB in Beijing region and the target database is TencentDB for MongoDB in Guangzhou region, you need to get the IP addresses for both regions from DTS IP Addresses and add them to the database allowlists, respectively.

Directions

Get the IP address for the database region from DTS IP Addresses, and add it to the source or target database allowlist.

- For a self-built database, allow the DTS IP address to access the database when you set the firewall.
  - Windows: Open “Control Panel”, find “Windows Defender Firewall”, and view the firewall policies.
  - Linux: Run the `iptables -L` command to view the server’s firewall policies.
- For a TencentDB database or a self-built database on CVM, follow the directions below to add the DTS IP address to the security group.
  i. Log in to the source database and click an instance ID in the instance list to enter the instance management page.
  ii. On the instance management page, select the **Security Group** or **Data Security** tab and add the DTS IP address to the security group.



- For a third-party cloud database, add the DTS IP address to the security group of that database.

DTS IP Addresses

Public network

Region	DTS IP Address
Guangzhou	111.230.198.143,118.89.34.161,123.207.84.254,139.199.74.159
Shanghai	111.231.139.59,111.231.142.94,115.159.71.186,182.254.153.245
Beijing	123.207.145.84,211.159.157.165,211.159.160.104,58.87.92.66
Chengdu	111.231.225.99,118.24.42.158
Chongqing	139.186.122.1/24,129.28.12.1/24,129.28.14.1/24,139.186.77.242,139.186.109.1/24, 139.186.131.1/23,94.191.102.144,94.191.98.210
Hangzhou-ec	111.231.139.59,111.231.142.94,115.159.71.186,182.254.153.245
Nanjing	129.211.166.117,129.211.167.130
Tianjin	154.8.246.150,154.8.246.48
Shenzhen	118.126.124.6,118.126.124.83
Hong Kong (China)	119.29.180.130,119.29.208.220,124.156.168.151,150.109.72.54
Beijing Finance	62.234.240.36,62.234.241.241

Region	DTS IP Address
Shenzhen Finance	118.89.251.206,139.199.90.75
Shanghai Finance	115.159.237.246,211.159.242.74
Singapore	119.28.103.40,119.28.104.184,119.28.116.123,150.109.11.113
Jakarta	43.129.33.41,43.129.35.144
Bangkok	150.109.164.203,150.109.164.82
Mumbai	119.28.246.130,119.28.246.18
Seoul	119.28.150.71,119.28.157.173
Tokyo	150.109.195.201,150.109.196.137
Silicon Valley	49.51.38.216,49.51.39.189
Virginia	170.106.2.63,49.51.85.120
Toronto	45.113.70.156,45.113.70.6,49.51.10.104,49.51.9.221
Frankfurt	49.51.132.38,49.51.133.85
Moscow	162.62.16.46,162.62.21.243

VPN access /Direct Connect/CCN/Self-built on CVM/VPC/Database

If the source or target database is TencentDB for MySQL or TencentDB for PostgreSQL, no action is required. Otherwise, you need to manually add the following DTS IP address to the allowlist.

Region	DTS IP Address
All regions	10.0.1.1/16,10.1.1.1/16,172.19.1.1/16,169.254.1.1/16,10.200.1.1/16,172.20.1.1/16, 10.159.1.1/16,10.45.1.1/16,192.168.1.1/16,172.16.1.1/16,172.30.1.1/16,172.31.1.1/16, 10.26.1.1/16,10.162.1.1/16,10.203.1.1/16,10.206.1.1/16,9.145.1.1/16,9.146.1.1/16, 10.209.1.1/16,10.6.1.1/16

Configuring Binlog in Self-Built MySQL

Last updated：2022-10-19 18:25:37

Overview

If the source database in a data migration, sync, or subscription task is a self-built MySQL, TDSQL for MySQL, or TDSQL-C for MySQL database, you need to set the binlog in the self-built database to meet the requirements for the source database during verification.

Operation impact

This operation requires database restart, which affects the business. We recommend you perform it during off-peak hours.

Directions

1. Log in to the source database.

2. Modify the `my.cnf` configuration file as follows:

Note：

- The default path of the `my.cnf` configuration file is `/etc/my.cnf`, subject to the actual conditions.
- We recommend you retain the binlog of the source database for at least three days; otherwise, the task cannot be resumed from the checkpoint and will fail.
  - Modifications in the `my.cnf` configuration file take effect permanently. If you want modifications to take effect only temporarily, run the `set global expire_logs_days=3` command to make modifications.
  - You can also use `binlog_expire_logs_seconds` to modify the binlog retention period (in seconds) in MySQL 8.0 or later.

```
log_bin = MYSQL_BIN
binlog_format = ROW
```

```
server_id = 2 // We recommend you set it to an integer above 1. The value here
is only an example
binlog_row_image = FULL
expire_logs_days=3 // Modify the binlog retention period (at least 3 days prefe
rably).
```

3. Restart the MySQL process.

```
[\$Mysql_Dir]/bin/mysqladmin -u root -p shutdown
[\$Mysql_Dir]/bin/safe_mysqld &
```

Note：

`[\$Mysql_Dir]` is the installation path of the source database. Replace it with the actual path.