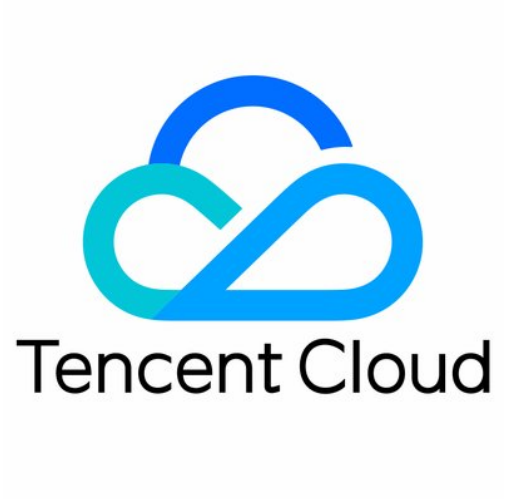
Data Transfer Service

Preparations

Product Documentation



Contents

Preparations
Business Evaluation

Last updated：2024-04-30 17:07:12

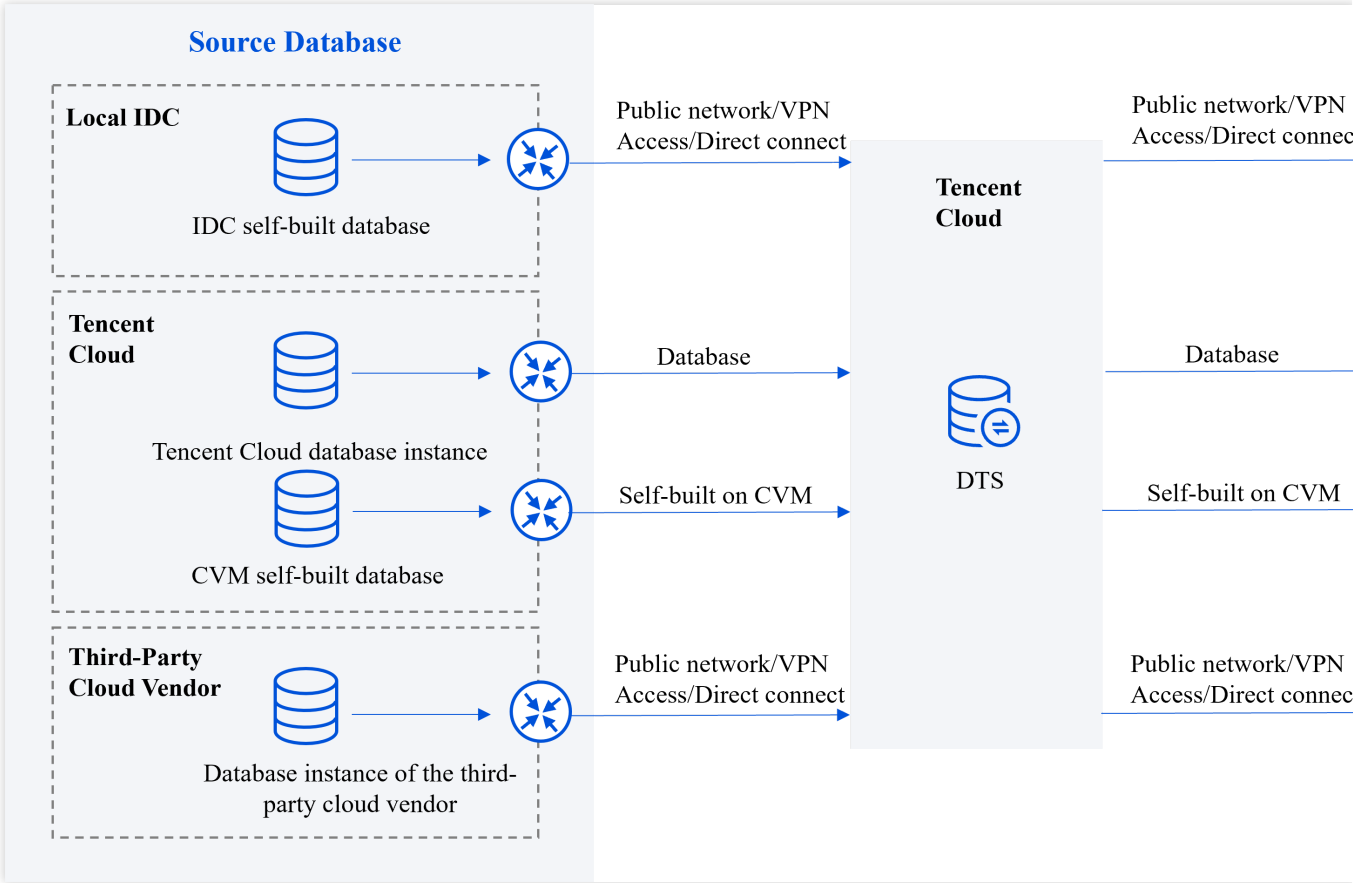
Note:
This section introduces the MySQL to MySQL Link as an example.
1. When DTS executes a full data migration/synchronization, it will read all the data from the source database once, thus increasing the load on the source database. If your database specification is low, we recommend performing the migration/synchronization during off-peak business hours, or reducing the DTS rate before starting the task.
2. Different source database specifications and DTS task configurations result in different impacts on the source database's performance. For example, with source database specifications of 8 cores and 16 GB, the default DTS task uses 8 thread concurrency (which can be adjusted), and in the absence of network bottlenecks, the impacts of the DTS task on the source database's performance are as follows.
During full export phase of the source database, it occupies about 18%-45% of the source database's CPU, increases query pressure of the source database by about 40-60 MB/s, and occupies about 8 active session connections.
During incremental export phase of the source database, there is virtually no pressure on the source database, with only one connection continuously listening to the source database's binlog logs.
3. By default, lock-free migration/synchronization is employed, which means no global lock (FTWRL) is applied to the source database during the task. Only tables without a primary key are added with table locks, others are not locked.
4. When performing data consistency checks, DTS uses the executing account of the task to write into the system database `__tencentdb__` in the source database, in order to record data comparison information during the task. Do not delete this system database.
To ensure that data comparison issues can be traced later, the DTS does not delete the `__tencentdb__` in the source database after completing the task.
The system database `__tencentdb__` occupies a very small space, roughly one thousandth to one ten-thousandth of the source database storage space (for example, if the source database is 50 GB, then the system database `__tencentdb__` would be approximately 5 MB-50 MB). It also uses a single-threaded and waiting connection mechanism, so it almost has no impact on the performance of the source database, nor does it pre-empt resources.

Network Preparation
Overview of Preparations Related to Network

Last updated：2024-08-13 14:54:23

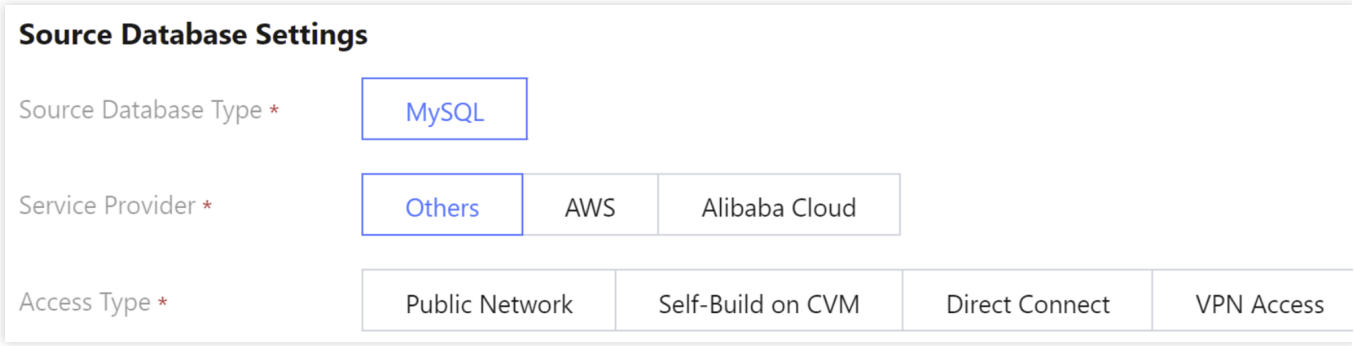
Overview

Using DTS, you can synchronize databases between different deployment forms such as local IDC, Tencent Cloud, and other third-party cloud vendors. This facilitates database migration, database backup, and building a hybrid cloud architecture with active-active deployment for enterprise users.
The DTS is part of the Tencent Cloud Network. If you use DTS for database synchronization, it's necessary to connect the networks where the source/target databases reside with the Tencent Cloud Network to which DTS belongs, ensuring DTS can connect to the source/target databases.



Choosing DTS Assess Type

The method chosen to connect the source/target database with the Tencent Cloud for DTS determines the access type selected when the DTS task is configured.



Note:

Adding DTS IP address to the security group or the allowlist of the interfacing database may pose certain security risks. Users are advised to enhance security measures during use, such as standardizing account password management, using authentication methods for internal API communications, inspecting and restricting unnecessary network segments, etc. Using DTS indicates you acknowledge the potential risks. If high security is a concern, it's recommended to choose Direct Connect, VPN Access, or VPC connections.

After using DTS, we recommend that you delete the DTS IP address from the security group or firewall promptly.

Deployment Type of Source/Target Database	Access Type	Applicable Scenarios	Network Configuration Guide
IDC self-built database Other Cloud Vendors' Databases Lighthouse Database on Tencent Cloud Lighthouse	Public Network	The database can be accessed through the public network IP. The public network cannot guarantee transmission bandwidth and poses security risks, making it suitable for scenarios with low transmission requirements.	Add DTS IP address to the database allowlist.(For self-built databases, it is usually configured in the firewall; for other cloud vendor databases, it is configured in security groups.)
	VPN Access	The database is interconnected with Tencent Cloud VPC through VPN connections. VPN connection uses encrypted transmission with a certain bandwidth guarantee, meeting most	1. Configure interconnection between VPC and IDC through VPN gateway. 2. Add DTS IP address to the database allowlist.

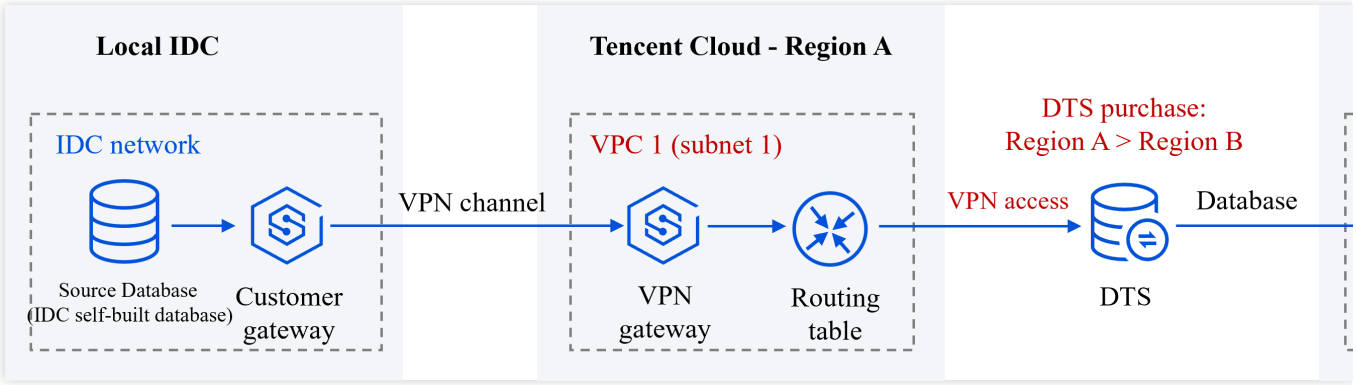
		network transmission security requirements.	
	Direct Connect	The database is interconnected with Tencent Cloud VPC through Direct Connect. When Direct Connect is used, network links are dedicated to users, with no risk of data leakage, high security, and meet the high-level network connection requirements for users such as financial institutions and governments.	1. Configure interconnection between VPC and IDC through Direct Connect Gateway. 2. Add DTS IP address to the database allowlist.
	CCN	The database is interconnected with Tencent Cloud VPC through CCN.	1. Configure Interconnection between VPC and IDC through CCN. 2. Add DTS IP Address to the database Allowlist.
CVM Self-built Database on Tencent Cloud	Self-Build on CVM	The database is deployed on Tencent Cloud's Cloud Virtual Machine (CVM).	Add DTS IP addresses to the allowlist of the corresponding databases.
Tencent Cloud Database Instance	Database	The database belongs to Tencent Cloud's database instance.	Add DTS IP addresses to the allowlist of the corresponding databases.
CVM Self-Built Database/Lighthouse Database/Tencent Cloud Database Instance	VPC	Both the source and target databases are deployed on Tencent Cloud and are connected via a VPC.	1. If you need to use of the VPC access type, please submit a ticket to apply for it. 2. Add DTS IP addresses to the allowlist of the corresponding databases.

Interworking Between local IDC and Tencent Cloud
VPN Access

Last updated：2024-04-30 17:14:44

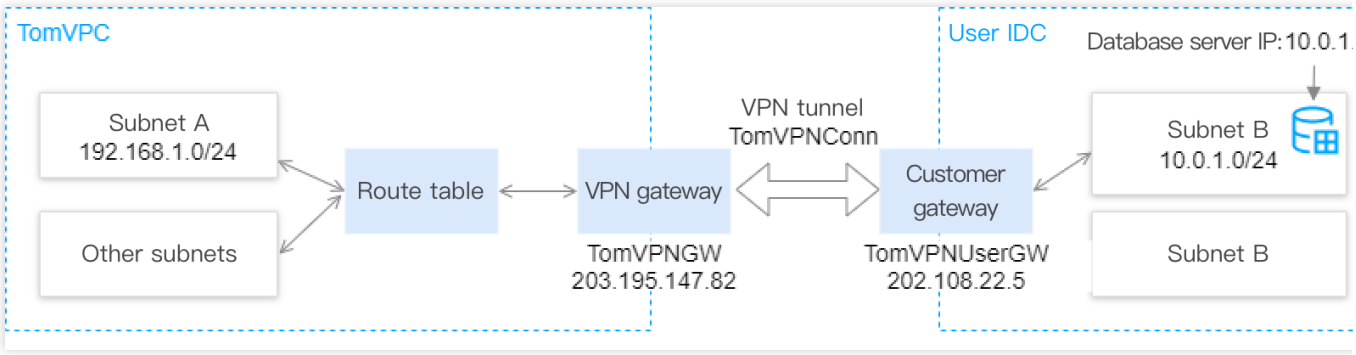
Overview

To use VPN access, users need to purchase a Tencent Cloud VPC and VPN gateway, establish a tunnel between the VPN and IDC, and connect the local IDC database to the Tencent Cloud VPC through nearby access, then use DTS for transfer tasks.



Directions

For instructions on establishing a VPN tunnel, see Establishing Connection Between VPC and IDC.
In this scenario, the user's VPC network is TomVPC, subnet is Subnet A, with the subnet range of `192.168.1.0/24` . The newly created VPN gateway is TomVPNGW, and the public IP address of the VPN gateway is `203.195.147.82` . The host IP address of the user's IDC database is `10.0.1.8` .



Subsequent Steps

1. After establishing connection between the VPN and IDC, select **VPN Access** on the DTS configuration task page.

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.

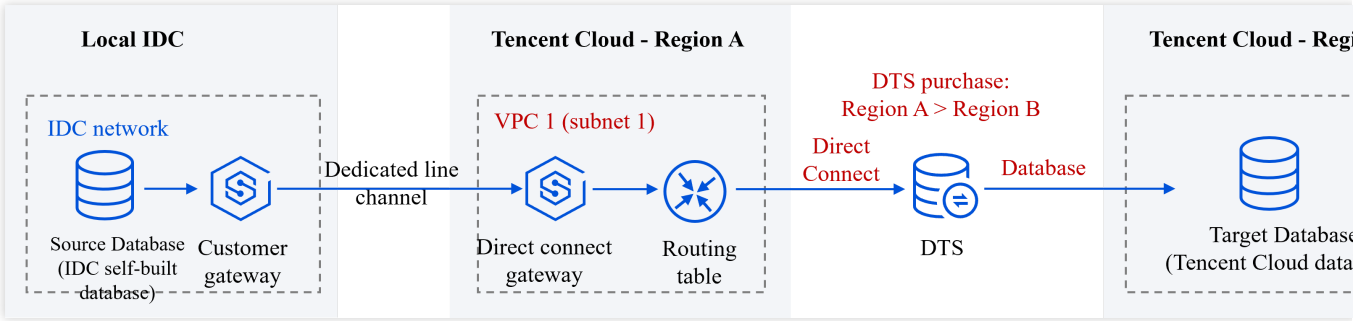
The account or password is incorrect.

Direct Connect

Last updated：2024-04-30 17:09:09

Overview

To use Direct Connect, users need to purchase a Tencent Cloud VPC and Direct Connect gateway, apply for Direct Connect, and connect the local IDC database to the Tencent Cloud VPC through nearby access, then transfer data via DTS.
DTS supports using the local IDC database as the source/destination for data transmission. The following example scenario is Local IDC Database (Direct Connect) -> Tencent Cloud Database (Database).



Establishing Network Interconnection Through Direct Connect

See Establishing Connection Between VPC and IDC Through Direct Connect.

DTS Task Configuration

1. Purchasing a DTS Task

When purchasing a DTS task, select the Tencent Cloud VPC1's region as **Source Instance Region**, that is, region A. Select the region where the target database is located as **Target Instance Region**, that is, region B.

2. Configuring DTS Task

In source database settings, select Direct Connect as **Access Type**, select VPC1 as **VPC**, and select one of its subnets Subnet1. In target database settings, select Database as **Access Type**.

3. Connectivity Test

If the database and its associated network have configured security access rules, such as security groups, firewall, IP access restrictions, etc., it is necessary to allow DTS IP address, otherwise, connectivity test may fail.

Allowing DTS IP Address

1. When the connectivity test fails, follow the instructions in the popup to access DTS IP address.
2. Sequentially check if the database has set the following network rules, and if so, allow DTS IP address in the corresponding rules.

Check if the database-associated network layer has set network ACLs or security groups.

Check if the server layer where the database resides has set up a firewall (e.g., iptables rules for Linux systems).

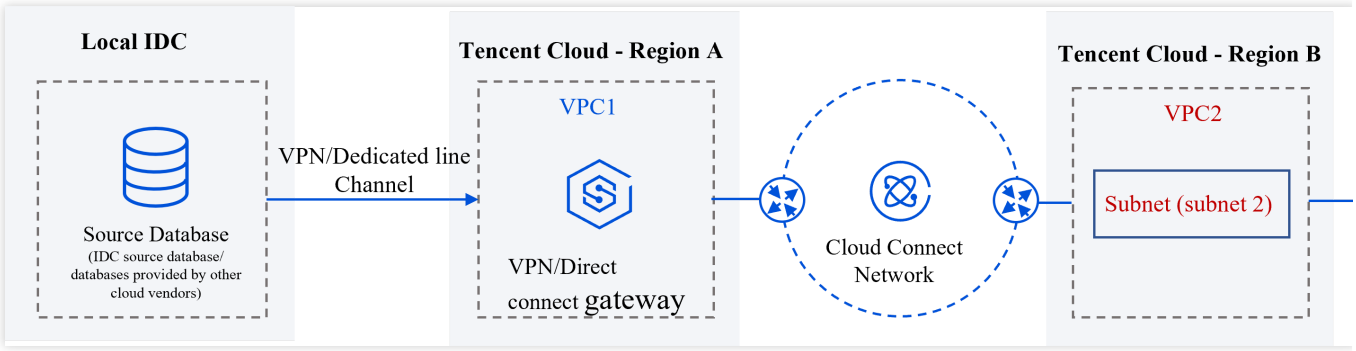
Check if the source database layer has set IP access restrictions.

Cloud Connect Network Access

Last updated：2024-04-30 17:19:27

Overview

To use CCN access, users must first use VPN/Direct Connect to connect their local IDC database to Tencent Cloud VPC (e.g., VPC1) through nearby access, and then use CCN to interconnect VPC1 and access VPC2.
In this scenario, you may select CCN under the DTS task account (i.e., the root account of the target database), or under a different account. Using another account's CCN feature is suitable for resource sharing between multiple companies. For example, if the CCN resources belong to the parent company's root account A, and the user's DTS and target database resources belong to subsidiary's root account B, and account B does not have CCN resources, you may use the CCN resources under account A to connect to the self-built database and then carry out the DTS task.
This section takes CCN under the same account as an example. For details on cross-account CCN configuration, see Migrating Data from Self-Built MySQL to TencentDB for MySQL Through CCN.



Network Interconnection Through CCN Access

1. To establish interconnection between a self-built IDC and VPC, see Establishing a connection between VPC and IDC.
2. To establish Interconnection between VPCs, see Connecting network instances under the same account through CCN.

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.

DTS Task Configuration

1. Purchasing a DTS Task

When purchasing a DTS task, select the region where the VPC (VPC2) is located as the **Source Instance Region**, that is, region B. Select the region where the target database is located as the **Target Instance Region**, that is, region C.

2. Configuring a DTS Task

Source Database Settings
Select CCN as **Access Type**. Select My Account as **CCN Instance Account**. Select "VPC2" as **CCN Associated VPC** and choose a subnet as Subnet2. In Target database settings, select Database as **Access Type**.
CCN-associated VPC refers to the VPC that is connected to DTS through CCN. You need to select a VPC other than the one used for source database access from all VPCs connected through CCN.
When selecting a subnet, if it can't be retrieved, it might be an account issue. The account for CCN-associated VPC and the DTS task account need to be consistent. For instance, to migrate a database instance from account A to account B, you need to create the task with account B. Therefore, CCN Associated VPC must be under account B.
VPC Region: No need to configure, but it's required that the source instance region selected by the user when purchasing a task remains consistent with the VPC region selected in the CCN Associated VPC above. If inconsistent, DTS will modify the region to be consistent.
Target Database Settings
Access type: Select Database.

3. Connectivity Test

If the database and its associated network have configured security access rules, such as security groups, firewall, IP access restrictions, etc., it is necessary to allow DTS IP address, otherwise, connectivity test may fail.

Allow DTS Service IP

1. When the connectivity test fails, follow the instructions in the popup to access "DTS Service IP".
2. Sequentially check if the database has set the following network rules, and if so, allow DTS IP address in the corresponding rules.
Check if the database-associated network layer has set network ACLs or security groups.
Check if the server layer where the database resides has set up a firewall (e.g., iptables rules for Linux systems).
Check if the source database layer has set IP access restrictions.

Public Network Access

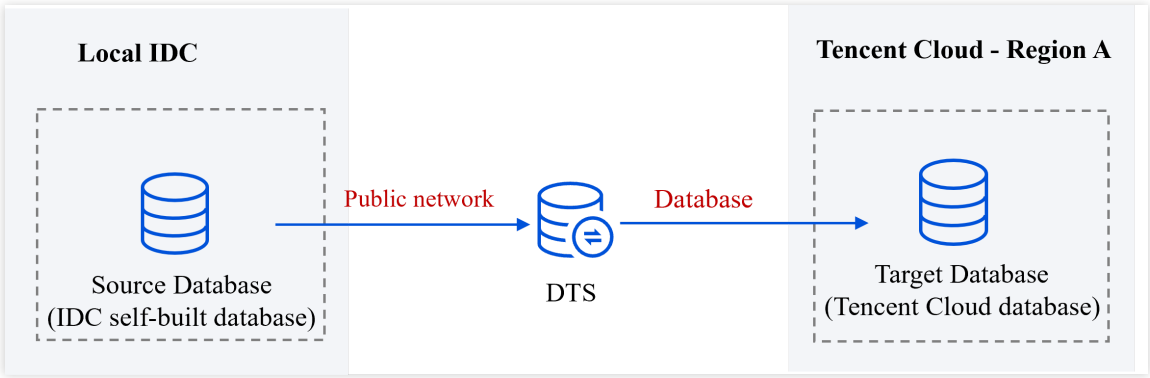
Last updated：2024-04-30 17:10:27

Overview

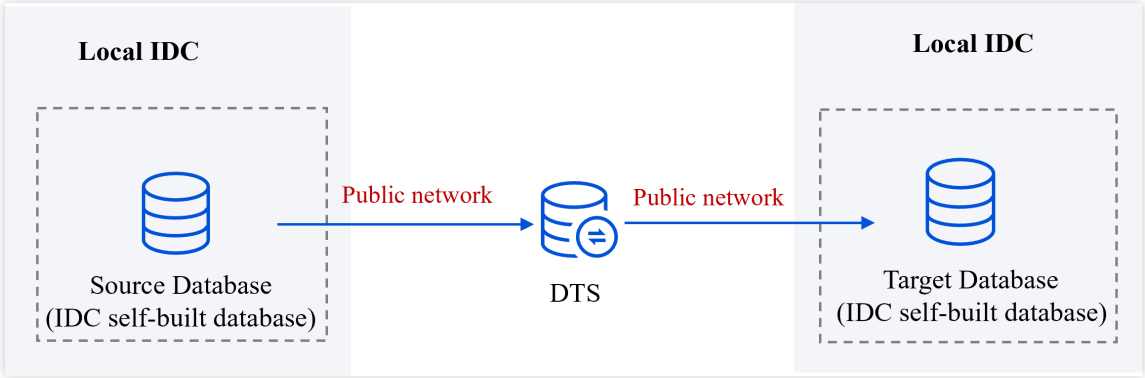
To use the Public Network Access method, users must choose the region closest to their physical database's region when purchasing a DTS task, and then use DTS for the transmission task. For example, If the region of the physical database is not included in the service regions of DTS, then choose a DTS service region that is closest to the region of the physical database. This ensures the optimal transmission path for DTS, reducing the duration of data transmission.

DTS supports using the local IDC database as a source/destination for data transmission, as shown in the examples below.

Scenario One: Local IDC Database (Public Network) -> Tencent Cloud Database (Database)



Scenario Two: Local IDC Database (Public Network) -> Local IDC Database (Public Network)



DTS Task Configuration

The following explains configuration instructions using Scenario One as an example.

1. When a DTS task is purchased, select the DTS region closest to the source database as the **Source Instance Region**. Select the region where the target database is located as the **Target Instance Region**, i.e., A.

2. When a DTS task is configured, in the source database and target database settings, select public network as **Access Type**.

3. Connectivity Test

If the database and its associated network have configured security access rules, such as security groups, firewall, IP access restrictions, etc., it is necessary to allow DTS IP address, otherwise, connectivity test may fail.

Allow DTS Service IP

1. When the connectivity test fails, follow the instructions in the popup to access "DTS Service IP".

2. Sequentially check if the database has set the following network rules, and if yes, allow DTS Service IP in the corresponding rules.

Check if network ACLs or security groups are set for the database-associated network layer.

Check if the firewall is set for the server layer where the database resides (e.g., iptables rules for Linux systems).

Check if IP access restrictions are set for the source database layer.

Interworking Between Other Cloud Vendors and Tencent Cloud

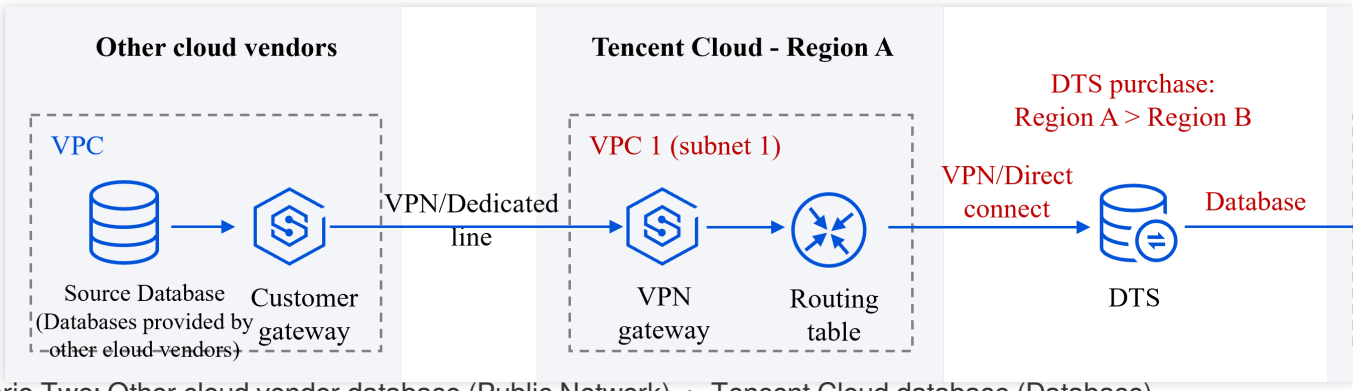
Last updated：2024-04-30 17:17:18

Overview

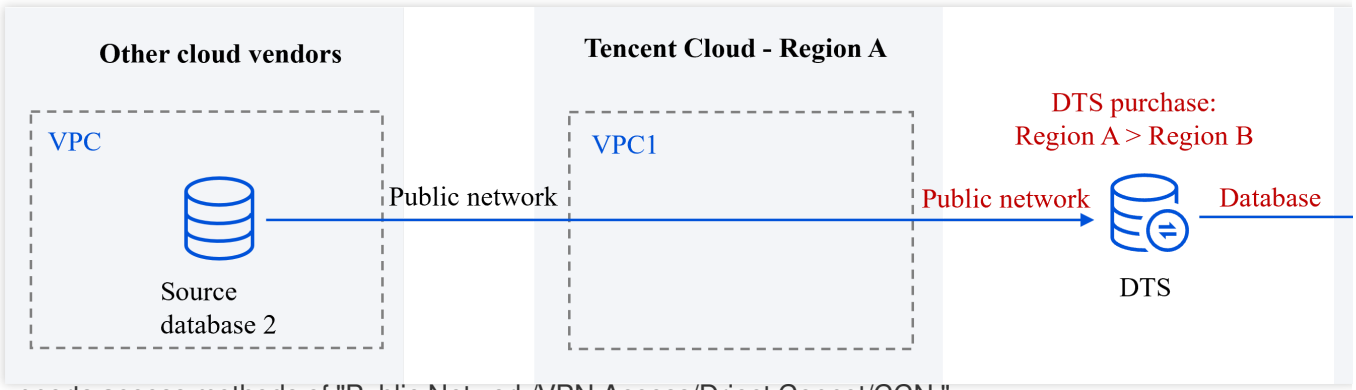
DTS supports the use of databases from other third-party cloud vendors as source/target databases for data synchronization. To synchronize databases using DTS, it is necessary to interconnect the networks where the source/target databases are located with the Tencent Cloud network to which DTS belongs, in order to enable DTS to connect to the source/target databases.

Network Interconnection Operation

The graph below shows the approach of using a third-party cloud vendor database as the source database only. The approach for accessing as a target database is similar.
Scenario One: Other cloud vendor database (VPN Access/Driect Connect) -> Tencent Cloud database (Database).



Scenario Two: Other cloud vendor database (Public Network) -> Tencent Cloud database (Database)



DTS supports access methods of "Public Network/VPN Access/Driect Connet/CCN ".

When using the Public Network method, you only need to allow DTS IP access in the source/target database, without any other network interconnection operations.

When using the VPN Connection method, users need to interconnect the network where the third-party cloud vendor database resides with the Tencent Cloud network that DTS belongs to in advance through a VPN tunnel.

When using the Direct Connect method, users need to interconnect the network where the third-party cloud vendor database resides with the Tencent Cloud network that DTS belongs to in advance through Direct Connect.

The CCN method is suitable for scenarios with multiple networks. If you have already used CCN for network interconnection, it can also be used for DTS connection.

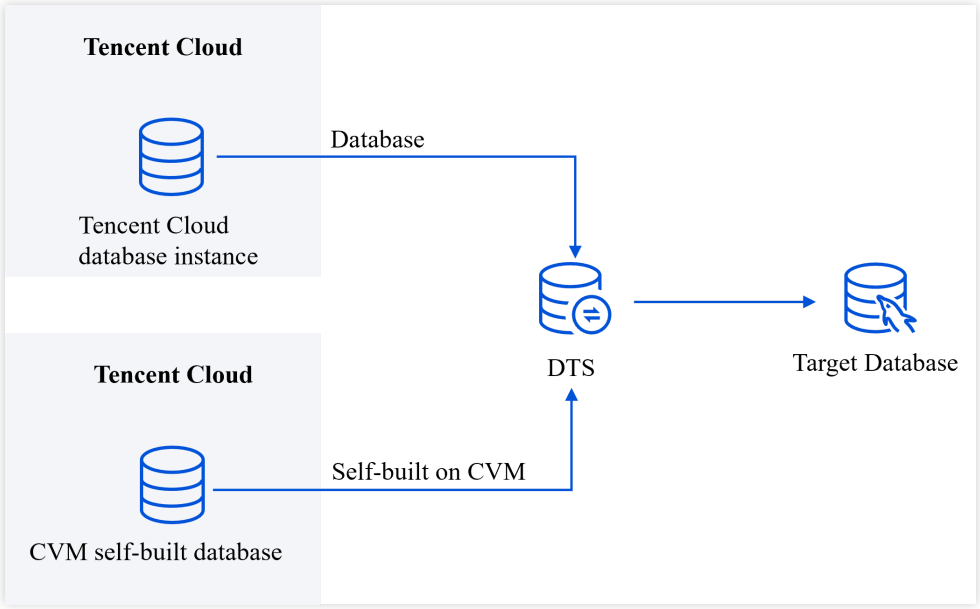
For specific network interconnection operations, which are similar to local IDC scenarios, see Interconnection between Local IDC and Tencent Cloud.

Interworking in Tencent Cloud

Last updated：2024-04-30 17:20:55

If your database is a Tencent Cloud database instance, or a self-built database on Tencent Cloud CVM, you only need to allow the DTS access IP address in the source/target database. No other network interconnection operations are required.

The following figure only shows the connection method when the cloud database acts as the source end. The connection method when it acts as the target end is similar.



Adding DTS IP Addresses to the Allowlist of the Corresponding Databases
Granting DTS Access IP for a Single Task

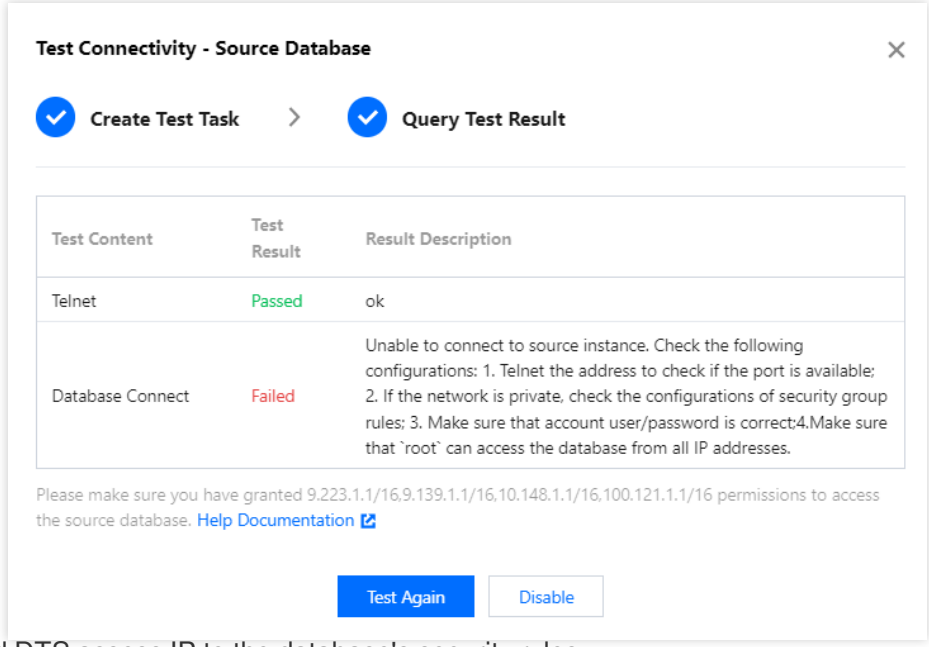
Last updated：2024-04-30 17:24:40

Overview

In data migration, data synchronization, and data subscription tasks, it is necessary to add the DTS assess IP to the allowlist of both the source and target databases so that DTS can access the source/target database. Otherwise, connectivity tests will fail.

Directions

1. When the DTS task is configured, on the **Set source and target databases** page, conduct a connectivity test first after entering the parameters.
2. If your database and its network have set security access rules, such as network ACLs and security groups, firewalls (iptables rules), and IP access restriction on database account, you need to grant the DTS assess IP according to the scenario. Otherwise, you will encounter the following error, where the address prompted in the image is the DTS service IP.
If the connectivity test result is Passed, it means the database has not set network restrictions. You can proceed with subsequent tasks without needing to grant access.



3. Add DTS assess IP to the database's security rules.

Different connection methods require different network access operations. The following only provides a summary. For detailed instructions, see Connectivity Test Failed.

Connection Method	Network Access Troubleshooting	Description
Public network/VPN Access/Direct Connect/CCN	Check the network layer of the database to see whether network ACL and security group rules have been set. Check the database deployment server layer to see whether firewall rules (such as iptables) have been set. Check the database layer to see whether IP access rules (e.g., only host addresses within authorization can access the database) have been set.	In relevant rules, grant the DTS Service IP.
Self-built on CVM VPC (Self-built on CVM)	Check the database deployment server layer to see whether firewall rules (such as iptables) have been set Check the database layer to see whether IP access rules (such as Check the database layer to see whether IP access rules) have been set.	In the corresponding rules, grant the DTS Service IP.
Database VPC (Database)	Check the database layer to see whether IP access rules (such as Only Authorized Host Addresses Can Access Database) have been set.	In the corresponding rules, grant the DTS Service IP.

Granting IP Range of DTS Access IP for Batch Tasks

Last updated：2024-04-30 17:27:00

Overview

When performing batch DTS tasks, if you opt to method for granting access to individual DTS access addresses (first conducting a connectivity test to obtain the DTS access IP address, then adding it to the allowlist of the source and destination databases one by one), the efficiency is lower. This section provides you with a more efficient method, adding the DTS access IP range at once.

Note:

The range of accessible IP ranges provided in this section is relatively large. In addition to the DTS access IPs, other IPs within the range can also access the source/target database, **and there might be a risk of data exposure, so choose carefully**.

Comparison of Access Methods

The differences between granting a batch of task IPs at once and granting individual task IP are as follows. Consider method 2 carefully.

Method	Description
Method 1 (Recommended): Granting access to individual DTS access IPs	First, perform a connectivity test, and upon failure, grant access to the specific IP as indicated by the pop-up notification. Advantages: **High Security**, ensuring that only DTS access IPs can access the source/target database, and other IPs cannot access. Disadvantages: Requires separate connectivity testing for each task, followed by adding the respective IPs one by one. The process can be cumbersome when there are many tasks.
Method 2: Granting access to the range where the DTS access IPs belong	Grant access to the range of the DTS Task. Advantages: You can add the IP addresses at once and create multiple DTS tasks, which is convenient. Disadvantages: The granting IP range is relatively wide. Besides the DTS access IPs, other IPs in the range can also access the source/target database, **and there may be a risk of data exposure, so choose carefully**.

Notes

When using DTS for multiple synchronization tasks on the same database, in the DTS task configuration, select the same parameters for **Access Type**, **VPC**, and **subnet**. Failure to do so may cause issues with network connection, preventing DTS from connecting to the database.

Operation Overview

Different connection methods require different network security investigation rules as follows.

Connection Method	Network Access Troubleshooting	Processing Description
Public Network	Check the network layer of the database to see if network ACL and security group rules have been set. Check the server layer of the database deployment to see if a firewall (such as iptables) has been set. Check the database layer to see if IP access restriction rules (e.g., only host addresses within authorization can access the database) have been set.	If security rules have been set, grant access to the IP of the DTS service region in the corresponding rules.
VPN Access/Direct Connect/CCN	Check the network layer of the database to see if network ACL and security group rules have been set. Check the server layer of the database deployment to see if a firewall (such as iptables) has been set. Check the database layer to see if IP access restriction rules (e.g., only host addresses within authorization can access the database) have been set.	If security rules have been set, grant access to a subnet under the VPC in the corresponding rules.
Self-Build on CVM VPC (Self-built on CVM)	Check the server layer of database deployment to see if a firewall (such as iptables) has been set. Check database layer to see if IP access restriction rules (e.g., only authorized host addresses can access the database) have been set.	If security rules have been set, then grant access to 169.254.1.1/16, 11.163.1.1/16
Database VPC (Database)	Check if IP access restriction rules (e.g., restrict database access to host addresses within the authorization) have been set in the database layer.	If security rules have been set, then grant access to 169.254.1.1/16, 11.163.1.1/16

Directions

Public Network Access

When using public network access, users need to select the DTS region closest to the physical database when purchasing a DTS task, and then use DTS for the transfer task.

1. Obtain the ranges that need to be granted.

Locate the DTS IP address in the corresponding region according to your connection region.

For example, if your source database region is in region M, then choose the nearest DTS region X for access. You need to grant the X region DTS service IP in the network that the source database belongs to. If the target database region is in region Y, choose the region N for access, and grant the Y region DTS IP address in the network that the target database belongs to.

DTS 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	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	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
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	49.51.38.216,49.51.39.189,170.106.177.233,170.106.81.114,170.106.81.79,170.106.98.28,170.10
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

2. Troubleshoot database-related security settings. If there are settings like the ones described, you need to grant the DTS IP address in the corresponding rules.
2.1 Check if network ACLs and security groups have been set in the network layer where the database belongs.
If yes, add the DTS IP address to the ACL and security group rules of the database's network.
2.2 Check if a firewall (such as iptables) has been set on the server where the self-built database is deployed.
If yes, grant the DTS IP address in the firewall rules.
2.3 Check if there are IP access restrictions (such as restricting access to the database to only host addresses within the authorization) set in the database layer.
If yes, grant the DTS IP address in the access restrictions.

VPN Access/Direct Connect

When using VPN for connection, users need to purchase a Tencent Cloud VPC and VPN gateway to connect their local IDC database to Tencent Cloud VPC via nearby access, then transfer tasks through DTS.
1. Obtain the ranges that need to be granted.
When configuring a DTS task, you will choose to access a subnet under the VPC, which indicates the IP address range that needs to be opened. The range of DTS access IP that needs to be granted for the source database is subnet1, and the range of DTS access IP that needs to be granted for the target database is subnet2.
2. Investigate the database-related security setting rules. If there are such settings as follows, the DTS access IP range needs to be granted in the corresponding rules.
2.1 Check if network ACLs and security groups have been set in database network layer.
If yes, add the DTS access IP range to the ACL and security group rules of the database's network.
2.2 Check if a firewall (such as iptables) has been set on the server where the self-built database is deployed.
If yes, grant the DTS access IP range in the firewall rules.

2.3 Check if there are IP access restrictions (such as restricting access to the database to only host addresses within the authorization) set in the database layer.
If yes, grant the DTS access IP range in the access restrictions.

CCN

When using CCN for connection, users need to connect their local IDC database to the Tencent Cloud VPC (such as VPC1) via nearby access, and then use CCN to connect VPC1 and access VPC2.
1. Obtain the ranges that need to be granted.
When configuring a DTS task, you will choose **CCN-Associated VPC (i.e., VPC2)** under a subnet, which is the IP range that needs to be granted. The source database needs to grant access to the subnet subnet2.
2. Investigate the database-related security setting rules. If there are such settings as follows, the DTS access IP range needs to be granted in the corresponding rules.
2.1 Check if network ACLs and security groups have been set in the database network layer.
If yes, add the DTS access IP range to the ACL and security group rules of the database's network.
2.2 Check if a firewall (such as iptables) has been set on the server where the self-built database is deployed.
If yes, grant the DTS access IP range in the firewall rules.
2.3 Check if there are IP access restrictions (such as restricting access to the database to only host addresses within the authorization) set in the database layer.
If yes, grant the DTS access IP range in the access restrictions.

Self-Build on CVM

If the source/target database is a self-built database on Tencent Cloud CVM, select Self-Build on CVM as access method. When a user initiates a DTS task, network ACLs and security groups can be automatically granted, and the user only need to check other security rules and grant them.
1. Obtain the ranges that need to be granted.
The connection between the Self-Build on CVM and DTS occurs within the Tencent Cloud private network, sharing common IP ranges of 169.254.1.1/16, 11.163.1.1/16.
2. Investigate the database's security rules. If there are settings as follows, grant the DTS access IP range in the corresponding rules.
2.1 Check if a firewall (such as iptables) is set on the server where the self-built database deployment is.
If yes, grant the DTS access IP range in the firewall rules.

Database

The source/target database is a Tencent Cloud database instance, with the connection method selected as "cloud database". When a user initiates a DTS task, network ACLs and security groups can be automatically granted, and the user only needs to check other security rules and grant them.
1. Obtain the ranges that need to be granted.

The connectivity between cloud database and DTS occurs within the Tencent Cloud private network, sharing common IP ranges of 169.254.1.1/16, 11.163.1.1/16.

2. Investigate the database's security rules. If there are settings as follows, grant the DTS access IP range in the corresponding rules.

2.1 Check the database layer to see if IP access restriction rules have been set.

For some TencentDB instances (like MySQL), there's support for limiting access IPs for accounts. Once set up, accounts can only access the database through host addresses within the authorization. For details on this MySQL feature, see Modifying Authorized Access Host Address.

If there are similar settings, you need to grant the DTS access IP range.

VPC

For VPC access, depending on the database's deployment mode as either a self-built database on CVM (see above "Self-Build on CVM") or cloud database (see above "Database"), just follow the corresponding scenario operations.

DTS Service Permission Preparation
Create sub users and authorize the use of DTS

Last updated：2024-07-08 21:05:26

Overview

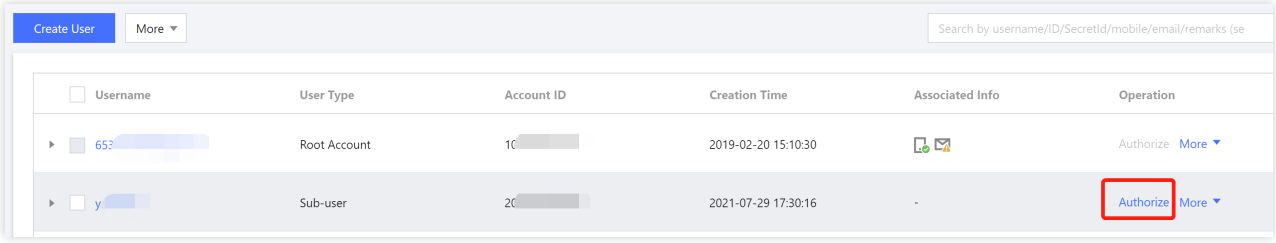
If you have multiple users managing different Tencent Cloud services such as CVM, VPC, and TencentDB, and they all share your Tencent Cloud account access key, you may face the risk of your key being compromised. Therefore, we recommend you create sub-users and let them manage different services to avoid such risk.
By default, sub-users have no permission to use DTS. Therefore, you need to create policies to allow them to use it.
You can skip this section if you don't need to manage the permissions of DTS resources for sub-users.

Creating and Authorizing Sub-user to Use DTS

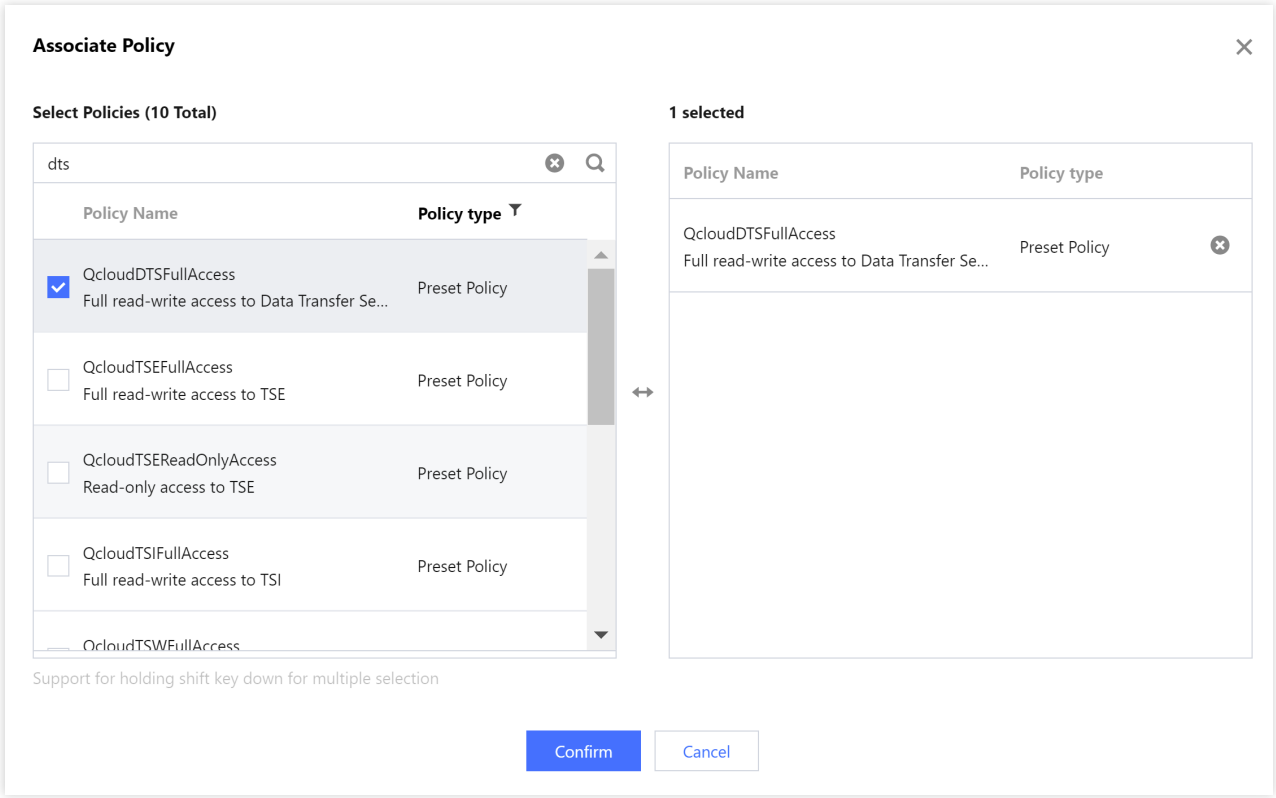
1. Log in to the CAM console as the root account.
2. On the left sidebar, select **User** > **User List** to enter the user list management page.
3. Click **Create User** to enter the user creation page.
4. On the user creation page, select the creation method.
5. On the **Quick User Creation** page, set the sub-user name, access method, user permission, etc.
Console Login: Select **Console access** or **Programming access**.
User permission: Select the permission as needed. If you select **QcloudDTSFullAccess**, the sub-user will be granted all read/write permissions of the DTS service. If you select **QcloudDTSReadOnlyAccess**, only the read-only permission will be granted.
6. Click **Create User**.
7. You will be redirected to the page prompting that the user is successfully created, and you can get the sub-user information in the following two methods:
Click **Copy** to directly get and copy the login information of the sub-user.
Click **Send**, enter the email address, and the system will send the complete sub-user information to the specified email address.

Authorizing Existing Sub-user to Use DTS

1. Log in to the CAM console with the root account, locate the target sub-user in the user list, and click **Authorize**.



2. In the pop-up window, select the **QcloudDTSFullAccess** preset policy and click **OK** to complete the authorization.



Authorize sub users with financial permissions

Last updated：2024-07-08 21:07:44

Overview

Sub-users generally don't have financial permissions. When they purchase a monthly subscribed DTS instance, the system will prompt that only the root account can pay the order. After the root account grants financial permissions to them, they can purchase such instances by themselves and use the account balance of the root account to make payments.

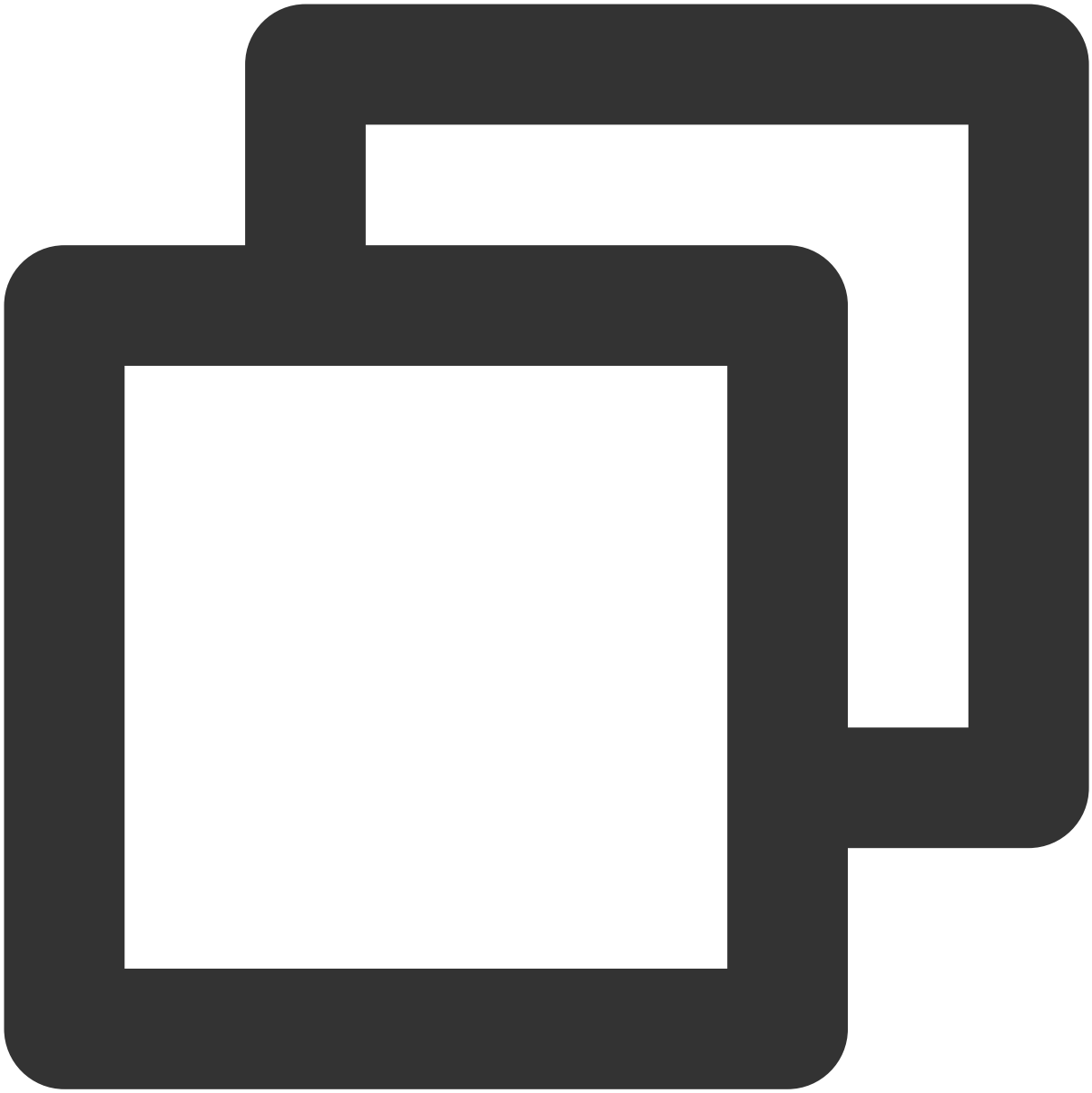
Prerequisites

You have created and authorized a sub-user as instructed in Creating and Authorizing Sub-user.

Directions

1. Log in to the CAM console as the root account.
2. Click **Policies** on the left sidebar. Then, click **Create Custom Policy** on the right and select **Create by Policy Syntax**.
3. Select **Blank Template** and click **Next**.
4. Create a policy, enter the policy name and description as needed, and copy the sample code to the **Policy Content**.

Sample policy syntax:



```
{
 "version": "2.0",
 "statement": [
     {
         "effect": "allow",
         "action": "finance:*",
         "resource": "qcs::dts:::*"
     }
 ]
}
```

5. Click **Complete**, return to the **Policy List** page, and click **Associate Users/Groups**.
6. Select the sub-user to be authorized (i.e., the sub-user created above) and click **OK**.

Authorizing DTS to Access Other Cloud Service Resources

Last updated：2024-08-13 14:56:22

Overview

You can select CCN as the access type when DTS connects to the source/target database. The CCN resources can be under the migration account or other Tencent Cloud accounts.
Using the CCN under other accounts is suitable for resource sharing among multiple companies. For example, the CCN resources belong to the root account A of the parent company, and the DTS and target database resources used by users belong to the subsidiary's root account B, and there are no CCN resources under the root account B. Then, you can use the CCN resources under the root account A to access the self-built databases and perform DTS tasks.
This document describes how to authorize DTS to access CCN resources under other Tencent Cloud accounts. Generally, you need to log in to the CAM console with the root account of the CCN resources, create a role, and authorize DTS to access the CCN resources under other accounts.

Directions

1. Log in to the CAM console with the Tencent Cloud root account of the CCN resources. If a sub-account has CAM and role permissions, you can also log in with the sub-account.
2. Click **Roles** on the left sidebar to enter the **Role Management** page. Then, click **Create Role**.
3. On the **Select Role Entity** page, select **Tencent Cloud Product Service**.
4. In the **Enter Role Entity Info** step, select **Data Transfer Service (dts)** and click **Next**.
5. In the **Configure Role Policy** step, enter **QcloudAccessForDTSRole** in the search box, select the displayed policy, and click **Next**.
6. In the **Set Role Tag** step, you can configure role tags as needed or skip this step.
7. In the **Review** step, enter the role name and click **Complete**. You must enter **DTS_QCSRole** rather than a custom role name, otherwise you cannot pull CCN resources under other accounts on the DTS task page.

Subsequent Operations

For subsequent directions after the authorization, see Migrating Data from Self-Built MySQL to TencentDB for MySQL Through CCN.

Database and Permission Preparation

Last updated：2024-04-30 17:28:27

1. Prepare source database and target database.
2. Create DTS task accounts and authorize them in both source database and target database.
It is recommended to create a separate database account for DTS tasks to easily distinguish session information and enhance data security.
The authorization requirements differ for each link. You can refer to the configuration guide of each link for authorization when configuring the DTS task later.

Data Migration
Data Sync
Data Subscription (Kafka Edition)

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.