数据传输服务

准备工作

产品文档

腾讯云

文档目录

准备工作
业务评估

最近更新时间：2024-04-30 17:07:33

说明：

本章节以 MySQL 到 MySQL 链路为例进行介绍。

1. DTS 在执行全量数据迁移/同步时，会将源库的全量数据全部读取一次，所以会增加源库的负载。如果您的数据库规格过低，建议您在业务低峰期进行迁移/同步，或者在任务启动前降低 DTS 的速率。

2. 源库的规格不同，DTS 任务配置不同，则对源库的性能影响也不同。以源库规格为 8 核 16G 为例，DTS 任务默认采用 8 线程并发（可调整），在网络无瓶颈的情况下，DTS 任务对源库的性能影响如下。

源库全量导出阶段：占用源库约 18%-45% 的 CPU，增加源库约 40-60MB/s 的查询压力，占用约 8 个活跃 session 连接数。

源库增量导出阶段：对源数据库基本无压力，只有一个连接实时监听源库的 binlog 日志。

3. 默认采用无锁迁移/同步来实现，任务过程中对源库不加全局锁（FTWRL），仅对无主键的表加表锁，其他不加锁。

4. 进行数据一致性校验时，DTS 会使用执行任务的账号在源库中写入系统库 `__tencentdb__` ，用于记录任务过程中的数据对比信息，请勿删除该系统库。

为保证后续数据对比问题可定位，DTS 任务结束后不会删除源库中的 `__tencentdb__` 。

`__tencentdb__` 系统库占用空间非常小，约为源库存储空间的千分之一到万分之一（例如源库为50GB，则 `__tencentdb__` 系统库约为5MB-50MB），并且采用单线程，等待连接机制，所以对源库的性能几乎无影响，也不会抢占资源。

网络准备
网络准备概述

最近更新时间：2024-08-13 14:53:49

操作场景

使用 DTS 可实现本地 IDC、腾讯云、其他第三方云厂商，这些不同部署形态的数据库之间的同步，方便企业用户进行数据库搬迁、数据库备份、构建云上云下多活架构等。
DTS 服务归属于腾讯云网络中，如果使用 DTS 进行数据库的同步，需要分别将源/目标数据库所在的网络与 DTS 所属的腾讯云网络进行打通，以便 DTS 可以连通源/目标数据库。

DTS 接入类型选择

源/目标数据库采用哪种方式与 DTS 所属的腾讯云打通，则在配置 DTS 任务时，接入类型选择对应的方式。

说明：

添加 DTS IP 地址到对接数据库的安全组或者白名单中，可能会对数据库造成一定的安全风险，请用户在使用过程中加强相关的安全防护，如规范账号密码管理、内部各 API 采用鉴权方式通讯、检查并限制不需要的网段等。使用 DTS 代表您已确认可能会存在的风险，如果用户对安全防护的要求较高，建议选择专线、VPN 接入、私有网络 VPC 的接入方式。

DTS 使用完毕后，建议用户及时删除安全组或防火墙中的 DTS IP 地址。

源/目标库部署类型	接入类型	适用场景	网络配置指引
IDC 自建数据库 其他云厂商数据库 腾讯云轻量应用服务器上的 轻量数据库	公网	数据库可以通过公网 IP 访问。 公网无法保证传输带宽，且存在安全隐患，适用于对传输要求不高的场景。	添加 DTS IP 地址至对接数据库白名单（自建数据库通常在防火墙中配置，其他云厂商数据库在安全组中配置）。
	VPN 接入	数据库通过 VPN 连接 与腾讯云私有网络打通。 VPN 接入方式采用加密传输，带宽有一定保证，可以满足绝大多数网络传输安全性要求。	1. 配置通过 VPN 网关实现 VPC 与 IDC 之间的互通。 2. 添加 DTS IP 地址至对接数据库白名单。
	专线接入	数据库通过 专线接入 与腾讯云私有网络打通。 专线接入方式网络链路用户独占，无数据泄露风险，安全性高，满足金融、政企等高等级网络连接要求。	1. 配置通过专线网关实现 VPC 与 IDC 之间的互通。 2. 添加 DTS IP 地址至对接数据库白名单。
	云联网	数据库通过 云联网 与腾讯云私有网络打通。	1. 配置通过云联网实现 VPC 和 IDC 之间的互通。 2. 添加 DTS IP 地址至对接数据库白名单。
腾讯云 CVM 自建数据库	云主机自建	数据库部署在 腾讯云服务器 CVM 上。	添加 DTS IP 地址至对接数据库白名单。

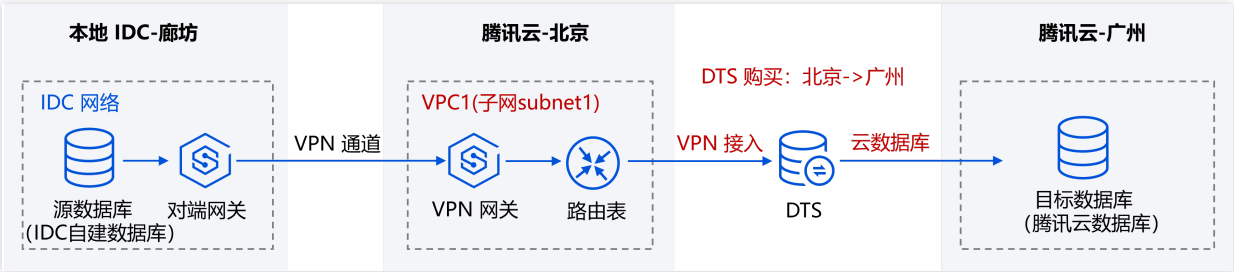
腾讯云数据库实例	云数据库	数据库属于腾讯云数据库实例。	添加 DTS IP 地址至对接数据库白名单。
CVM 自建数据库/轻量数据库/腾讯云数据库实例	私有网络 VPC	数据库和目标数据库都部署在腾讯云上，且有私有网络。	1. 如果需要使用 VPC 接入类型，请 提交工单 申请。 2. 添加 DTS IP 地址至对接数据库白名单。

本地 IDC 与腾讯云的互通
VPN 接入

最近更新时间：2024-04-30 17:13:55

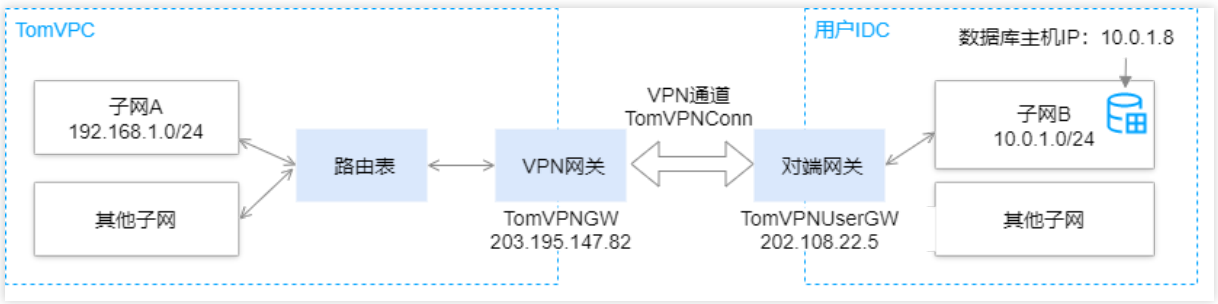
操作场景

使用 VPN 接入方式，需要用户购买一个腾讯云 VPC 和 VPN 网关，建立 VPN 和 IDC 之间的通道，将本地 IDC 数据库就近接入腾讯云 VPC 中，然后通过 DTS 进行传输任务。



操作步骤

建立 VPN 通道的操作，请参考 建立 VPC 到 IDC 的连接。
本场景中，用户所属的 VPC 网络为“TomVPC”，子网为“子网A”，子网A的网段为 `192.168.1.0/24` 。新建 VPN 网关为“TomVPNGW”，VPN 网关的公网 IP 为 `203.195.147.82` 。用户 IDC 数据库的主机IP地址为 `10.0.1.8` 。



后续步骤

1. VPN 与 IDC 连通后，在DTS 配置任务页面选择 **VPN 接入**。

参数	说明	参数示例
VPN 网关	在 VPC 网络中新建的 VPN 网关名称。	TomVPNGW

私有网络	用户所属的 VPC 网络名称。	TomVPC
子网	用户 VPC 网络的子网名称。	子网 A
主机地址	源数据库的主机 IP 地址。	10.0.1.8
端口	源数据库使用的端口。常见数据库默认端口如下：（如用户修改了默认端口，请按实际情况填写） MySQL：3306 SQL Server：1433 PostgreSQL：5432 MongoDB：27017 Redis：6379	3306

2. 单击**测试连通性**。如果出现测试不通过，请按照如下指导进行排查。

Telnet 测试不通过。

在新建的 VPC 网络中（本例中为 TomVPC）购买一个云服务器 CVM，在 CVM 上 ping 源数据库主机地址：

如果不能 ping 通。

源数据库设置了安全组或防火墙。

源数据库对 SNAT IP 地址进行了限制。

源数据库端口设置问题。

如果可以 ping 通。

请 提交工单 处理。

Telnet 测试通过，Database Connect 失败。

迁移账号授权问题。请参考 数据迁移、数据同步 中的对应场景，重新对迁移账号授权。

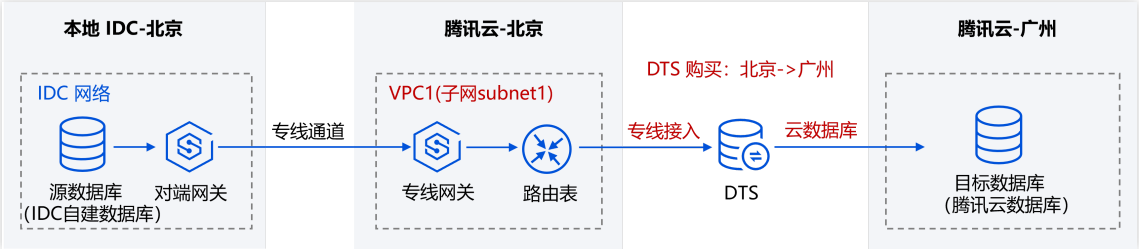
账号密码不正确。

专线接入

最近更新时间：2024-04-30 17:08:30

操作场景

使用专线接入方式，需要用户购买一个腾讯云 VPC 和专线网关，并申请专线通道，将本地 IDC 数据库**就近接入**到腾讯云 VPC 中，然后通过 DTS 进行传输任务。
DTS 支持将本地 IDC 数据库作为源/目标进行数据传输，如下示例场景为：本地 IDC 数据库（专线接入） -> 腾讯云数据库（云数据库）。



专线接入网络打通

请参考 通过专线建立 VPC 与 IDC 的连接。

DTS 任务配置

1. 购买 DTS 任务

购买 DTS 任务时，**源实例地域**选择源库接入的腾讯云 VPC1 所属地域，即北京地域。**目标实例地域**选择目标数据库所属地域，即广州地域。

2. 配置 DTS 任务

源库设置中，**接入类型**选择“专线接入”，**私有网络**选择“VPC1”，并选择其中的一个子网“subnet1”；目标库设置中，**接入类型**选择“云数据库”。

3. 测试连通性

如果数据库及所属网路配置了安全访问规则，如安全组、防火墙、IP 访问限制等，需要放通 DTS 服务 IP，否则，会出现连通性测试不通过。

放通 DTS 服务 IP

1. 连通性测试不通过时，根据弹窗中的提示，获取“DTS 服务 IP”。
2. 依次检查数据库是否设置了如下网络规则，如果有，请在对应规则中放通 DTS 服务 IP。

数据库所属网络层级是否设置了网络 ACL 或安全组。

数据库所在服务器层级是否设置防火墙（如 Linux 系统的 iptables 规则）。

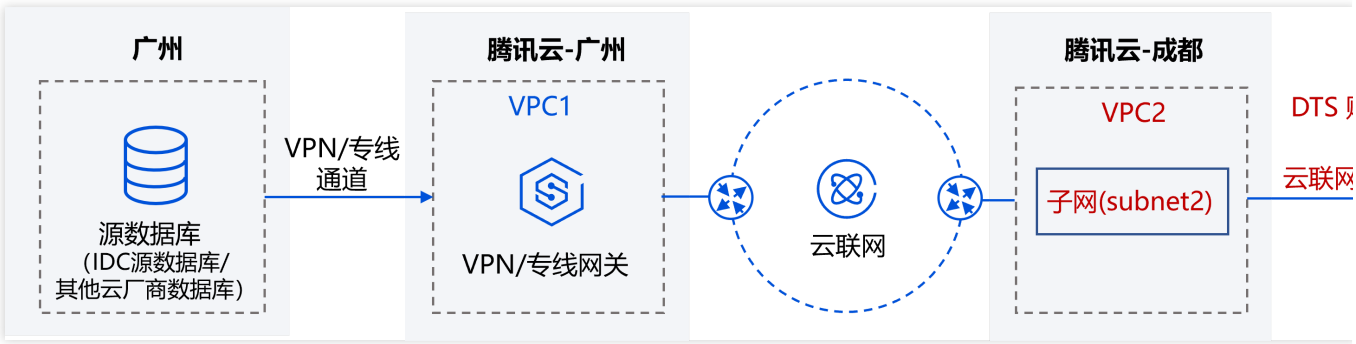
源数据库层级是否设置了 IP 访问限制。

云联网接入

最近更新时间：2024-04-30 17:18:34

操作场景

使用云联网接入方式，需要用户提前将本地 IDC 数据库通过 VPN/专线就近接入腾讯云 VPC 中（如 VPC1），再通过云联网打通 VPC1 和接入 VPC2。
这里的云联网，可以选择执行 DTS 任务账号（即目标库所属主账号）名下的云联网，也可以选择其他账号名下的云联网。使用其他账号云联网功能，适用于多个公司之间的资源共享，例如云联网资源归属集团公司的主账号 A，用户使用的 DTS、目标数据库资源都归属子公司主账号 B， 账号 B 下没有云联网资源，可以使用账号 A 下的云联网资源打通自建数据库，然后进行 DTS 任务。
本章节以同账号云联网为例，跨账号云联网配置详情请参考 通过云联网方式迁移自建 MySQL 至腾讯云 MySQL。



云联网接入网络打通

1. 建立自建 IDC 与 VPC 之间的互通，请参考 建立 VPC 到 IDC 的连接。
2. 建立 VPC 之间的互通，请参考 通过云联网建立不同网络之间的互通。

说明：
云联网仅提供所有地域间 10Kbps 以下的免费带宽，使用 DTS 数据传输时需要更高带宽，所以链接中的配置带宽是必选操作。

DTS 任务配置

1.购买 DTS 任务

购买 DTS 任务时，**源实例地域**选择接入 VPC（VPC2）的所属地域，即成都地域。**目标实例地域**选择目标库所属地域，即广州地域。

2.配置 DTS 任务

源库设置

接入类型选择“云联网”，**云联网实例所属账号**选择“我的账号”，**云联网关联 VPC**选择“VPC2”并选择一个子网“subnet2”；目标库设置中，**接入类型**选择“云数据库”。

“云联网关联 VPC”指的是云联网中接入 DTS 链路的 VPC，需要在云联网打通的所有 VPC 中，选择除源库接入的 VPC 外的其他 VPC。

选择子网时，如果无法拉取，则可能是账号问题，“云联网关联 VPC”所属账号和 DTS 任务账号需要一致。例如，要把 A 账号的数据库实例迁到 B 账号下面，使用 B 账号进行任务创建，所以“云联网关联 VPC”一定要是 B 账号下的。

VPC 所属地域：无需配置，但要求用户购买任务时选择的源实例地域与上述“云联网实例关联 VPC”中选择的 VPC 地域要保持一致，如果不一致，DTS 会将地域修改为一致。

目标库设置

接入类型：选择“云数据库”。

3.测试连通性

如果数据库及所属网路配置了安全访问规则，如安全组、防火墙、IP 访问限制等，需要放通 DTS 服务 IP，否则，会出现连通性测试不通过。

放通 DTS 服务 IP

1. 连通性测试不通过时，根据弹窗中的提示，获取“DTS 服务 IP”。
2. 依次检查数据库是否设置了如下网络规则，如果有，请在对应规则中放通 DTS 服务 IP。

数据库所属网络层级是否设置了网络 ACL 或安全组。

数据库所在服务器层级是否设置防火墙（如 Linux 系统的 iptables 规则）。

源数据库层级是否设置了 IP 访问限制。

公网接入

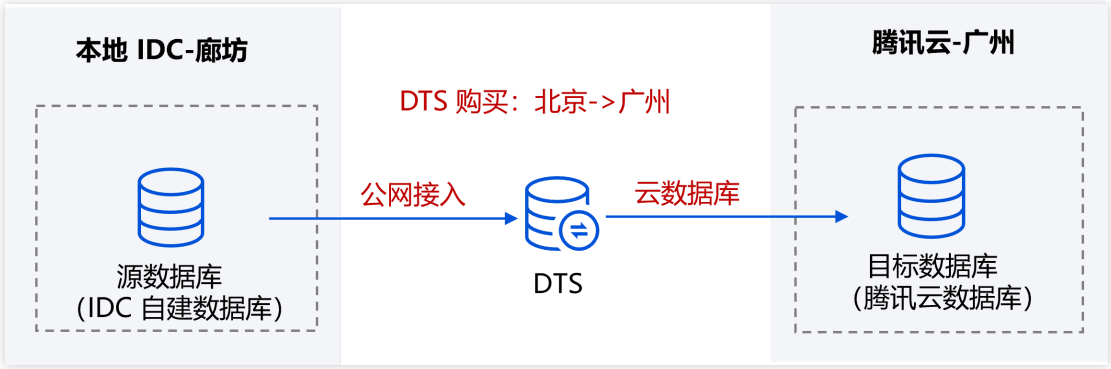
最近更新时间：2024-04-30 17:10:59

操作场景

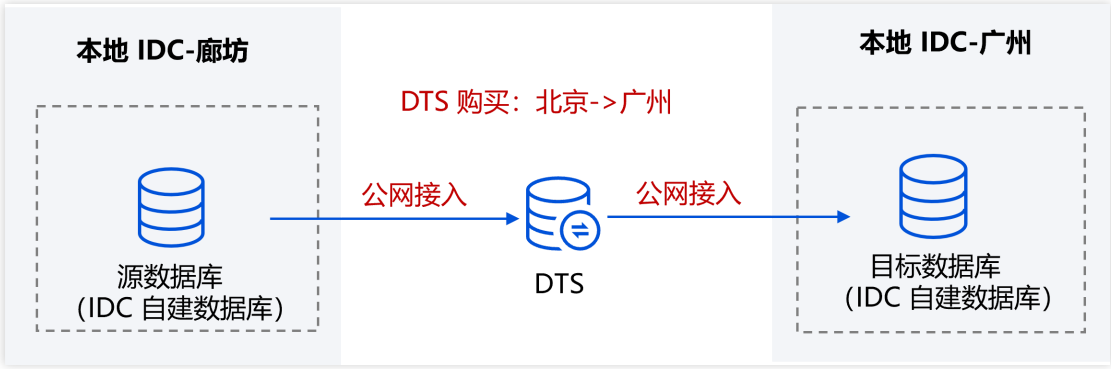
使用公网接入方式，需要用户在购买 DTS 任务时，选择离物理数据库地域最近的地域，然后通过 DTS 进行传输任务。例如，物理地域在廊坊，DTS 服务没有廊坊地域，则选择最近的北京地域，这样 DTS 的传输路径最优，可以降低数据传输时长。

DTS 支持将本地 IDC 数据库作为源/目标进行数据传输，示例如下。

场景一：本地 IDC 数据库（公网接入） -> 腾讯云数据库（云数据库）



场景二：本地 IDC 数据库（公网接入） -> 本地 IDC 数据库（公网接入）



DTS 任务配置

如下以场景一为例进行配置说明。

1. 购买 DTS 任务时，**源实例地域**选择离源库最近的 DTS 地域，离廊坊最近的为北京，所以选择北京地域。**目标实例地域**选择目标库所属地域，即广州地域。
2. 配置 DTS 任务时，源库设置中，**接入类型**选择“公网”；目标库设置中，**接入类型**选择“公网”。
3. 测试连通性

如果数据库及所属网路配置了安全访问规则，如安全组、防火墙、IP 访问限制等，需要放通 DTS 服务 IP，否则，会出现连通性测试不通过。

放通 DTS 服务 IP

1. 连通性测试不通过时，根据弹窗中的提示，获取“DTS 服务 IP”。
2. 依次检查数据库是否设置了如下网络规则，如果有，请在对应规则中放通 DTS 服务 IP。

数据库所属网络层级是否设置了网络 ACL 或安全组。
数据库所在服务器层级是否设置防火墙（如 Linux 系统的 iptables 规则）。
源数据库层级是否设置了 IP 访问限制。

其他云厂商与腾讯云的互通

最近更新时间：2024-04-30 17:17:37

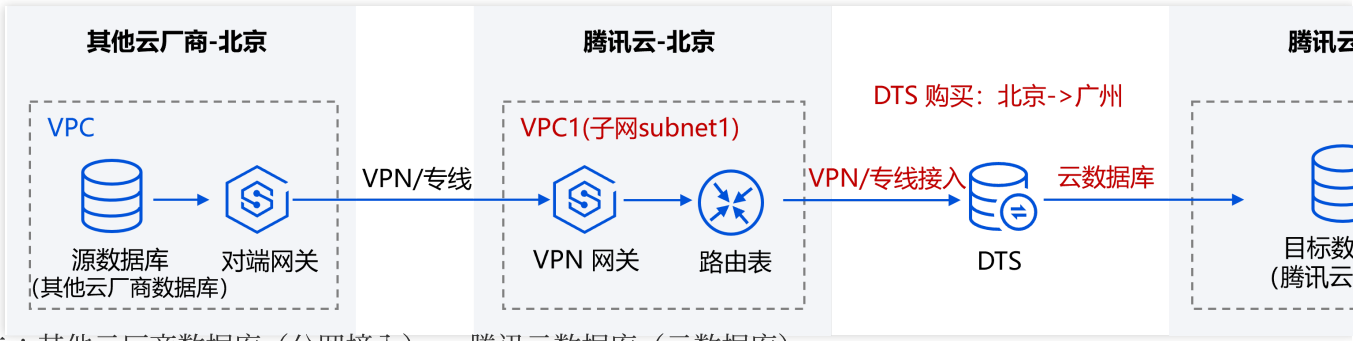
操作场景

DTS 支持将其他第三方云厂商数据库作为源/目标库进行数据同步，使用 DTS 进行数据库的同步，需要分别将源/目标数据库所在的网络与 DTS 所属的腾讯云网络进行打通，以便 DTS 可以连通源/目标数据库。

网络打通操作

如下图中仅展示了第三方云厂商数据库作为源库的接入方式，作为目标库的接入方式类似。

场景一：其他云厂商数据库（VPN/专线接入） -> 腾讯云数据库（云数据库）



场景二：其他云厂商数据库（公网接入） -> 腾讯云数据库（云数据库）

DTS 接入数据库的方式支持“公网/VPN 接入/专线接入/云联网”。

选择“公网”方式，只需要在源/目标库上放通 DTS IP 的访问，不需要其他网络打通操作。

选择“VPN 接入”方式，需要用户提前通过 VPN 通道方式，将第三方云厂商数据库所在的网络与 DTS 所属的腾讯云网络进行打通。

选择“专线接入”方式，需要用户提前通过专用通道方式，将第三方云厂商数据库所在的网络与 DTS 所属的腾讯云网络进行打通。

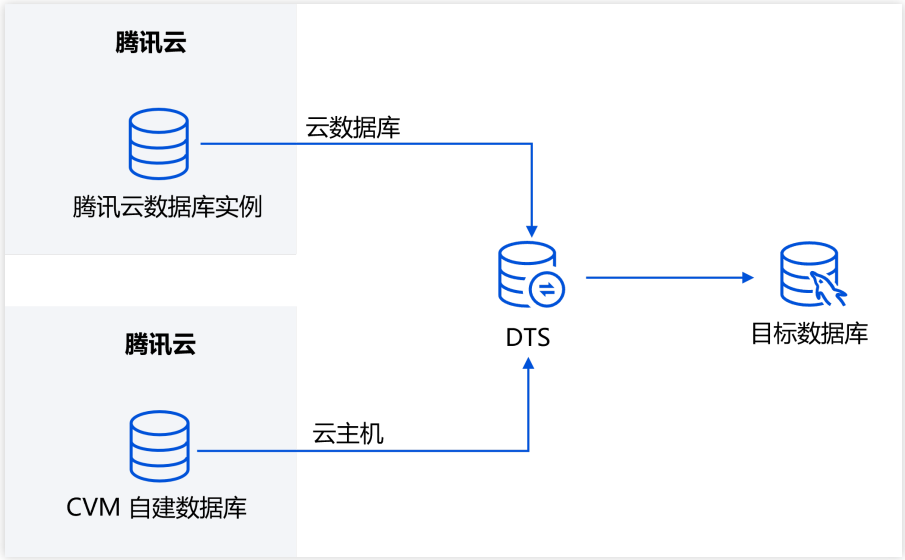
“云联网”方式，适合网络较多场景的打通，如果您已使用云联网进行了网络打通，DTS 也可选择云联网方式接入。

具体的网络打通操作，与本地 IDC 场景类似，请参考 本地 IDC 与腾讯云的互通。

腾讯云之间的互通

最近更新时间：2024-04-30 17:20:14

如果您的数据库为腾讯云数据库实例，或者为腾讯云 CVM 上自建的数据库，您只需要在源/目标数据库中，放通 DTS 访问 IP 地址即可，不需要其他网络打通操作。
如下图中仅展示了云数据库作为源端的接入方式，作为目标端的接入方式类似。



添加 DTS IP 地址至对接数据库白名单
单个任务，放通 DTS 访问 IP

最近更新时间：2024-04-30 17:25:10

操作场景

数据迁移、数据同步、数据订阅任务中，需要将 DTS 访问 IP 分别添加到源数据库和目标数据库的白名单中，以便 DTS 可以访问源/目标数据库，否则会出现连通性测试失败。

操作步骤

1. 在配置 DTS 任务时，**设置源和目标数据库**页面中，参数输入完成后，先进行连通性测试。
2. 如果您的数据库及所属网络设置了安全访问规则，如网络 ACL 和安全组、防火墙（iptables 规则）、数据库账号访问 IP 限制，您需要根据场景分别放通 DTS 访问 IP，否则会出现如下报错，图中提示的地址即为 DTS 服务 IP。
如果连通性测试通过，则说明数据库没有设置网络限制，可以继续后续任务，无需进行放通操作。

3. 添加 DTS 访问 IP 到数据库的安全规则中。
不同的接入方式，需要的网络放通操作不同。如下仅提供概要，详细的操作指导参见 连通性测试不通过。

接入方式	网络放通排查	说明
公网/VPN/专线/云联网	检查数据库所属网络层级，是否设置了网络 ACL 和安全组规则	在相应规则中，放通 DTS 服务 IP。

	检查数据库部署服务器层级，是否设置了防火墙（如 iptables）规则 检查数据库层级，是否设置了访问 IP 规则（如仅限制授权内的主机地址才可访问数据库）	
云主机自建 私有网络 VPC （CVM 自建数据库）	检查数据库部署服务器层级，是否设置了防火墙（如 iptables）规则 检查数据库层级，是否设置了访问 IP 规则（如 限制授权内的主机地址可访问数据库）	在相应规则中，放通 DTS 服务 IP。
云数据库 私有网络 VPC（云数据库）	检查数据库层级，是否设置了访问 IP 规则（如 限制授权内的主机地址可访问数据库）	在相应规则中，放通 DTS 服务 IP。

批量任务，放通 DTS 访问 IP 所属网段

最近更新时间：2024-09-02 14:52:08

操作场景

进行批量 DTS 任务时，如果采用“放通单独 DTS 访问地址”的方法（先对任务进行连通性测试，获得 DTS IP，再逐一添加到源数据库和目标数据库的白名单中），效率较低，本章节为您提供一种高效的方法，一次性放开 DTS 访问 IP 所属网段。

说明：

本章节提供的放通 IP 网段范围比较大，除 DTS 访问 IP 外，网段内其他 IP 也可以访问源/目标数据库，**可能会有数据暴露风险，请慎重选择**。

放通方式对比

批量任务放通 IP 操作，与放通单独任务 IP 的差异对比如下，请慎重选择方式二。

方式	说明
方式一（推荐）：放通单独 DTS 访问 IP	先进行连通性测试，失败后根据弹窗提示放通具体的 IP。 优点：**安全性高**，保证源/目标数据库会只会放通 DTS 访问 IP 的访问，其他 IP 不可访问。 缺点：需要每个任务分别先进行连通性测试，然后再一一添加对应的 IP，任务数量较多时操作比较繁琐。
方式二：放通 DTS 访问 IP 所属网段	放通 DTS 任务所属网段。 优点：创建多个 DTS 任务时，一次添加 IP 地址即可，操作方便。 缺点：放通的 IP 网段范围比较大，除 DTS 访问 IP 外，网段内其他 IP 也可以访问源/目标数据库，**可能会有数据暴露风险，请慎重选择**。

注意事项

使用 DTS 对同一个数据库进行多个同步任务时，在 DTS 的任务配置中，请选择相同的**接入类型**、**VPC** 和 **subnet** 等参数，否则可能会导致网络打通出现异常，DTS 无法连接数据库。

操作概览

不同的接入方式，需要排查的网络安全规则不同，具体如下。

接入方式	网络放通排查	处理说明
公网	检查数据库所属网络层级，是否设置了网络 ACL 和安全组规则 检查数据库部署的服务器层级，是否设置了防火墙（如 iptables） 检查数据库层级，是否设置了访问 IP 限制规则（如仅授权内的主机地址可访问数据库）	如果设置了安全规则，则在相应规则中，放通接入 DTS 服务地域的 IP。
VPN 接入/专线接入/云联网	检查数据库所属网络层级，是否设置了网络 ACL 和安全组规则 检查数据库部署的服务器层级，是否设置了防火墙（如 iptables） 检查数据库层级，是否设置了访问 IP 限制规则（如仅授权内的主机地址可访问数据库）	如果设置了安全规则，则在相应规则中，放通接入 VPC 下的一个子网。
云主机自建 私有网络 VPC （CVM自建数据库）	检查数据库部署的服务器层级，是否设置了防火墙（如 iptables） 检查数据库层级是否设置了访问 IP 限制规则（如仅授权内的主机地址可访问数据库）	如果设置了安全规则，则放通 169.254.1.1/16,11.163.1.1/16
云数据库 私有网络 VPC （云数据库）	检查数据库层级是否设置了访问 IP 限制规则（如 限制授权内的主机地址可访问数据库）	如果设置了安全规则，则放通 169.254.1.1/16,11.163.1.1/16

操作步骤

公网接入

使用公网接入方式，需要用户在购买 DTS 任务时，选择离物理数据库最近的 DTS 地域进行接入，然后通过 DTS 进行传输任务。

1. 获取需要放通的网段。

请根据您的接入地域，找到对应地域的 DTS 服务 IP。

例如，您的源数据库地域在廊坊，则就近选择 DTS 北京地域进行接入，需要在源数据库所属网络中放通北京地域 DTS 服务 IP；目标数据库地域在广州，选择广州地域进行接入，需要在目标数据库所属网络中放通广州地域 DTS 服务 IP。

DTS 地域	DTS 服务 IP 地址
广州	111.230.198.143,118.89.34.161,123.207.84.254,139.199.74.159
上海	111.231.139.59,111.231.142.94,115.159.71.186,182.254.153.245

北京	123.207.145.84,211.159.157.165,211.159.160.104,58.87.92.66
成都	111.231.225.99,118.24.42.158
重庆	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
杭州ec	111.231.139.59,111.231.142.94,115.159.71.186,182.254.153.245
南京	129.211.166.117,129.211.167.130
天津	154.8.246.150,154.8.246.48
深圳	118.126.124.6,118.126.124.83
中国香港	119.29.180.130,119.29.208.220,124.156.168.151,150.109.72.54
北京金融	62.234.240.36,62.234.241.241
深圳金融	118.89.251.206,139.199.90.75
上海金融	115.159.237.246,211.159.242.74
新加坡	119.28.103.40,119.28.104.184,119.28.116.123,150.109.11.113
雅加达	43.129.33.41,43.129.35.144
曼谷	150.109.164.203,150.109.164.82
孟买	119.28.246.130,119.28.246.18
首尔	119.28.150.71,119.28.157.173
东京	150.109.195.201,150.109.196.137
硅谷	49.51.38.216,49.51.39.189,170.106.177.233,170.106.81.114,170.106.81.79,170.106.98.28,170.106.98.4
弗吉尼亚	170.106.2.63,49.51.85.120
法兰	49.51.132.38,49.51.133.85

克福	

2. 排查数据库相关的安全设置规则，如果有如下设置，则需要在相应规则中放通 DTS 服务 IP。
2.1 数据库所属网络层级，是否设置了网络 ACL 和安全组。
如果有，则将 DTS 服务 IP 添加到数据库所属网络的 ACL 和安全组规则中。
2.2 自建数据库部署的服务器上是否设置了防火墙（如 iptables）。
如果有，则在防火墙规则中放通 DTS 服务 IP。
2.3 数据库层级，是否设置了访问 IP 限制（如限制仅授权内的主机地址可访问数据库）。
如果有，则在访问限制中放通 DTS 服务 IP。

VPN 接入/专线接入

使用 VPN 接入方式，需要用户购买一个腾讯云 VPC 和 VPN 网关，将本地 IDC 数据库就近接入腾讯云 VPC 中，然后通过 DTS 进行传输任务。
1. 获取需要放通的网段。
您在配置 DTS 任务时会选择接入 VPC 下的一个子网，这个子网就是需要放通的网段。源数据库需要放通的 DTS 访问 IP 网段为 subnet1，目标数据库需要放通的 DTS 访问 IP 网段为 subnet2。
2. 排查数据库相关的安全设置规则，如果有如下设置，则需要在相应规则中放通 DTS 访问 IP 网段。
2.1 数据库所属网络层级，是否设置了网络 ACL 和安全组。
如果有，则将 DTS 访问 IP 网段添加到数据库所属网络的 ACL 和安全组规则中。
2.2 自建数据库部署的服务器上是否设置了防火墙（如 iptables）
如果有，则在防火墙规则中放通 DTS 访问 IP 网段。
2.3 数据库层级，是否设置了访问 IP 限制（如限制仅授权内的主机地址可访问数据库）。
如果有，则在访问限制中放通 DTS 访问 IP 网段。

云联网接入

使用云联网接入方式，需要用户将本地 IDC 数据库就近接入腾讯云 VPC 中（如 VPC1），再通过云联网打通 VPC1 和接入 VPC2。
1. 获取需要放通的网段。
您在配置 DTS 任务时会选择**云联网关联 VPC（即 VPC2）** 下的一个子网，这个子网就是需要放通的网段。源数据库需要放通子网 subnet2 的访问。
2. 排查数据库相关的安全设置规则，如果有如下设置，则需要在相应规则中放通 DTS 访问 IP 网段。
2.1 数据库所属网络层级，是否设置了网络 ACL 和安全组。
如果有，则将 DTS 访问 IP 网段添加到数据库所属网络的 ACL 和安全组规则中。
2.2 自建数据库部署的服务器上是否设置了防火墙（如 iptables）。
如果有，则在防火墙规则中放通 DTS 访问 IP 网段。
2.3 数据库层级，是否设置了访问 IP 限制（如限制仅授权内的主机地址可访问数据库）。
如果有，则在访问限制中放通 DTS 访问 IP 网段。

云主机自建

源/目标库为腾讯云 CVM 上的自建数据库，接入方式选择“云主机自建”。当用户发起 DTS 任务时，可自动进行网络 ACL 和安全组的放通，用户只需排查其他安全规则并进行放通。

1. 获取需要放通的网段。

云主机自建数据库与 DTS 的连通都是在腾讯云内网中，统一网段为169.254.1.1/16,11.163.1.1/16。

2. 排查数据库的安全规则，如果有如下设置，则需要在相应规则中放通 DTS 访问 IP 网段。

2.1 自建数据库部署的服务器上，是否设置了防火墙（如 iptables）。

如果有，则在防火墙规则中放通 DTS 访问 IP 网段。

云数据库

源/目标库为腾讯云数据库实例，接入方式选择“云数据库”。当用户发起 DTS 任务时，可自动进行网络 ACL 和安全组的放通，用户只需排查其他安全规则并进行放通。

1. 获取需要放通的网段。

云数据库与 DTS 的连通都是在腾讯云内网中，统一网段为169.254.1.1/16,11.163.1.1/16。

2. 排查数据库的安全规则，如果有如下设置，则需要在相应规则中放通 DTS 访问 IP 网段。

2.1 检查数据库层级，是否设置了访问 IP 限制规则。

部分腾讯云数据库实例（如 MySQL），支持限制账号的访问 IP，设置后，账号只能通过授权内的主机地址访问数据库，MySQL 的功能详情可参见修改授权访问的主机地址。

如果有类似设置，则需要放通 DTS 访问 IP 网段。

私有网络 VPC

使用私有网络 VPC 接入，根据数据库的部署形态为 CVM 自建数据库（参考上述“云主机自建”），还是云数据库（参考上述“云数据库”），参考对应的场景操作即可。

DTS 服务权限准备
创建子用户并授权使用 DTS

最近更新时间：2024-07-08 21:04:47

操作场景

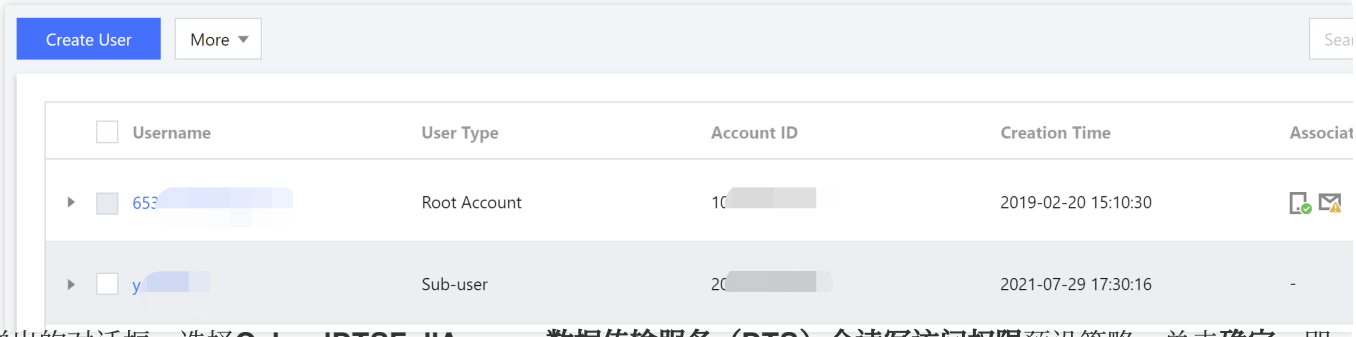
如果您在腾讯云中使用到了云服务器、私有网络、云数据库等多项服务，这些服务由不同的人管理，但都共享您的云账号密钥，这样会存在泄密风险，因此建议您创建子用户，通过子用户实现不同的人管理不同的服务来规避泄密风险。
默认情况下，子用户没有使用 DTS 的权利，因此用户需要创建策略来允许子用户使用 DTS。
若您不需要对子用户进行 DTS 相关资源的访问管理，您可以跳过此章节。

创建子用户并授权使用 DTS

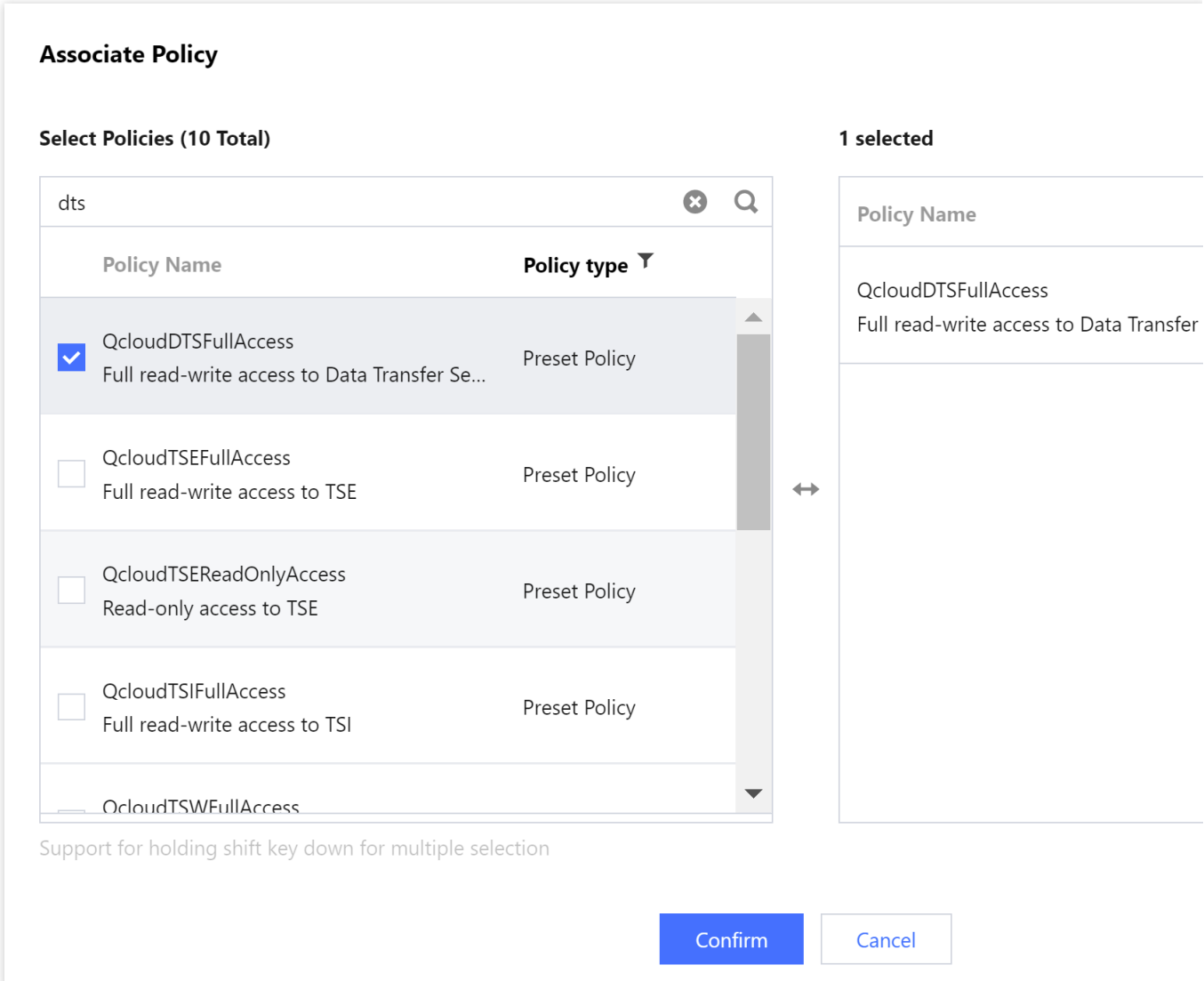
1. 使用主账号登录 访问管理控制台。
2. 在左侧导航栏中，选择**用户 > 用户列表**，进入用户列表管理页面。
3. 单击**新建用户**，进入新建用户页面。
4. 在新建用户页面，选择创建方式。
5. 在**快速新建用户**页面，设置子用户名称、访问方式、用户权限等。
控制台登录：可选择**控制台登录访问**和**编程访问**。
用户权限：用户可根据情况选择，如果选择 **QcloudDTSFullAccess**，表示授权子用户访问 DTS 服务的全部读写权限。如果选择 **QcloudDTSReadOnlyAccess**，表示仅授权读访问权限。
6. 单击**创建用户**。
7. 进入成功新建用户页面，您可以通过以下两种方法获取子用户信息。
单击**复制**，可直接获取复制子用户登录信息。
单击**发送至**填写邮箱信息，系统将把完整的子用户信息发送至邮箱。

已有子用户，给子用户授权使用 DTS

1. 使用主账号登录 访问管理控制台，在用户列表选择对应子用户，单击**授权**。



2. 在弹出的对话框，选择**QcloudDTSFullAccess 数据传输服务（DTS）全读写访问权限**预设策略，单击**确定**，即可完成子用户授权。



授权子用户财务权限

最近更新时间：2024-07-08 21:07:00

操作场景

子用户一般没有财务权限，在购买 DTS 包年包月实例时，提交订单会出现如下提示，需要主账号来支付订单。对子用户授权财务权限后，子用户可以自行购买包年包月实例，同时可使用主账号的账户金额进行支付。

前提条件

已完成 创建子用户并授权。

操作步骤

1. 使用主账号登录 访问管理控制台。
2. 在左侧导航单击**策略**，然后在右侧单击**新建自定义策略**，并选择**按策略语法创建**。
3. 选择**空白模板**，然后单击**下一步**。
4. 创建一个策略，策略的名称以及描述可以根据自己的需求填写，策略内容复制示例代码。
 策略语法示例：

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

5. 单击**完成**后返回到策略列表页，在列表页中单击**关联用户/组**。
6. 选择需要授权的子用户（上述步骤中新创建的子用户），单击**确定**。

授权 DTS 访问其他云服务资源

最近更新时间：2024-08-13 14:55:49

操作场景

DTS 接入源/目标数据库时，接入方式选择云联网，云联网资源可以是迁移账号名下的，也可以是其他账号下。
使用其他账号云联网功能，适用于多个公司之间的资源共享，例如云联网资源归属集团公司的主账号A，用户使用的DTS、目标数据库资源都归属子公司主账号B， 账号B下没有云联网资源，可以使用账号A下的云联网资源进行 DTS 任务。
本场景为您介绍使用其他账号云联网的授权操作，总体的原则为，使用其他云联网资源所属的主账号登录访问管理，创建角色并授权允许 DTS 访问。

操作步骤

1. 使用其他云联网资源所属的腾讯云主账号登录 访问管理控制台（如果子账号子有 CAM 和角色相关的权限，也可以使用子账号登录）。
2. 左侧导航单击**角色**，进入角色管理页面，然后单击**新建角色**。
3. 在选择角色载体页面，选择**腾讯云产品服务**方式。
4. 进入**输入角色载体信息**页面，勾选**数据传输服务（dts）**后，单击**下一步。**
5. 在**配置角色策略**页面，输入 **QcloudAccessForDTSRole**，勾选对应策略后单击**下一步。**
6. 在**配置角色标签**页面，可自定义标签配置，如不需要配置可以跳过进行下一步。
7. 在**审阅**页面，输入角色名称后**单击**完成。这里的角色名称必须输入 **DTS_QCSRole**，不能定义为其他名称，否则在 DTS 任务界面，无法拉取到其他账号下的云联网资源。

后续操作

授权后，通过云联网方式进行数据传输的操作指导，详细的指导请参考 通过云联网方式迁移自建 MySQL 至腾讯云 MySQL。

数据库及权限准备

最近更新时间：2024-04-30 17:29:01

1. 准备源和目标数据库。
2. 分别在源和目标数据库中，创建 DTS 任务账号并授权。

建议创建单独用于 DTS 任务的数据库账号，便于区分会话信息以及提升数据安全性。

不同链路的授权要求不同，您可以在后续进行 DTS 任务配置时，参考每个链路的配置指导进行授权。

数据迁移

数据同步

数订订阅（Kafka版）

配置自建MySQL系的Binlog

最近更新时间：2023-06-09 11:03:55

操作场景

当数据迁移、数据同步、数据订阅任务的源库为自建 MySQL/TDSQL MySQL/TDSQL-C MySQL 时，需要用户在自建数据库上设置 Binlog，以满足校验项阶段对源库的要求。

操作影响

本操作需要重启数据库，会对业务造成一定影响，建议在业务低峰阶段操作。

操作步骤

1. 登录源数据库。

2. 参考如下内容修改配置文件 `my.cnf` 。

> 说明：
>
> - `my.cnf` 配置文件的默认路径为 `/etc/my.cnf` ，现场以实际情况为准。
> - 建议源端 Binlog 日志至少保留3天及以上，否则可能会因任务暂停/中断时间大于 Binlog 日志保留时间，造成任务无法续传，进而导致任务失败。
>   - 在 `my.cnf` 配置文件中修改会永久生效，如果用户仅想临时生效，请执行 `set global expire_logs_days=3` 命令修改。
>   - MySQL 8.0版本及以上也可以使 `binlog_expire_logs_seconds` 来修改 Binlog 保留时间，该参数精确到秒级。

```
log_bin = MYSQL_BIN
binlog_format = ROW
server_id = 2 //建议设为大于1的整数，此处仅为示例。
binlog_row_image = FULL
expire_logs_days=3 //修改 binlog 的保留时间，建议大于等于3天
```

3. 重启 MySQL 进程。

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

说明：

[$Mysql_Dir] 指源数据库的安装路径，请替换为实际的源数据库安装目录。