云数据库 RDS

最佳实践

文档版本 01

发布日期 2025-02-28

华为云计算技术有限公司

商标声明


和其他华为商标均为华为技术有限公司的商标。
本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为云计算技术有限公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为云计算技术有限公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

目 录

1 RDS 最佳实践汇总

本文汇总了云数据库RDS常见应用场景的操作实践，并为每个实践提供详细的方案描述和操作指导，帮助您轻松使用RDS。

RDS for MySQL 最佳实践

表 1-1 RDS for MySQL 最佳实践

相关文档	说明
自建MySQL迁移到RDS for MySQL	介绍通过自建MySQL如何迁移到云数据库 RDS for MySQL。
RDS for MySQL通过DRS搭建异地单主灾备	RDS for MySQL实例如何通过DRS服务搭建异地单主灾备。
其他云MySQL迁移到云数据库RDS for MySQL	介绍通过其他云MySQL如何迁移到云数据库 RDS for MySQL。
使用RDS for MySQL搭建WordPress	介绍通过华为云虚拟私有云、弹性云服务器和RDS for MySQL数据库，在LAMP环境下搭建WordPress。
使用RDS for MySQL搭建Discuz!论坛	介绍通过华为云虚拟私有云、弹性云服务器和RDS for MySQL数据库，在LAMP环境下搭建Discuz!。
innodb_flush_log_at_trx_commit和sync_binlog参数详解	介绍innodb_flush_log_at_trx_commit和sync_binlog参数，对性能，安全方面的影响。
提高RDS for MySQL数据库查询速度的方法	介绍提高RDS for MySQL数据库查询速度的方法。
RDS for MySQL长事务排查和处理	介绍如何排查RDS for MySQL长事务，并kill长事务。
RDS for MySQL安全最佳实践	提供RDS for MySQL安全配置的规范性指导。

RDS for PostgreSQL 最佳实践

表 1-2 RDS for PostgreSQL 最佳实践

相关文档	说明
RDS for PostgreSQL搭建跨区域容灾关系	介绍如何搭建RDS for PostgreSQL实例跨区域容灾。
RDS for PostgreSQL发布与订阅	介绍RDS for PostgreSQL提供的发布和订阅功能。
RDS for PostgreSQL自定义数据类型转换	介绍RDS for PostgreSQL自定义数据类型转换的语法使用。
使用客户端驱动程序实现故障转移和读写分离	介绍如何使用PostgreSQL客户端驱动程序实现故障转移和读写分离。
PoWA插件使用最佳实践	介绍如何使用PoWA插件，用于对RDS for PostgreSQL数据库进行性能监控。
pg_dump使用最佳实践	介绍pg_dump备份工具的使用方法。
PgBouncer使用最佳实践	介绍PgBouncer连接池工具的安装配置和使用方法。
RDS for PostgreSQL安全最佳实践	提供RDS for PostgreSQL安全配置的规范性指导。

RDS for SQL Server 最佳实践

表 1-3 RDS for SQL Server 最佳实践

相关文档	说明
恢复备份文件到RDS for SQL Server实例的版本限制	介绍RDS for SQL Server恢复备份时的版本限制。
使用导入导出功能将ECS上的SQL Server数据库迁移到RDS for SQL Server	介绍如何将ECS自建的SQL Server数据库迁移到RDS for SQL Server。
修改RDS for SQL Server实例的参数	介绍如何修改RDS for SQL Server数据库实例的参数组。
RDS SQL Server支持DMV动态管理视图	介绍RDS for SQL Server如何通过DMV动态管理视图。
使用导入导出功能将本地SQL Server数据库迁移到RDS for SQL Server	介绍如何将本地的SQL Server数据库迁移到RDS for SQL Server。
在rdsuser主账号下创建子账号	介绍rdsuser主账号的权限和如何在rdsuser主账号下创建并管理子账号。

相关文档	说明
创建tempdb临时数据文件	介绍RDS for SQL Server如何创建tempdb临时数据文件。
Microsoft SQL Server发布与订阅	介绍云数据库 RDS for SQL Server如何提供订阅功能。
RDS for SQL Server添加c#CLR程序集的使用方法	介绍RDS for SQL Server如何添加c#CLR程序集。
RDS for SQL Server添加链接服务器	介绍RDS for SQL Server数据库实例如何创建链接服务器访问另外一个RDS for SQL Server数据库实例。
RDS for SQL Server 如何将线下SSRS报表服务部署上云	介绍RDS for SQL Server如何使用SSRS（Reporting Services）报表服务。
RDS for SQL Server收缩数据库	介绍RDS for SQL Server如何使用存储过程收缩指定数据库的数据文件和日志文件的大小，以释放磁盘部分空间。
使用DAS在RDS for SQL Server主备实例上分别创建和配置Agent Job和Dblink	介绍如何使用DAS在RDS for SQL Server主备实例上分别创建和配置Agent Job和Dblink。
创建实例定期维护job	介绍如何创建定期执行的SQL agent job，定期执行索引重建、统计信息更新及数据库收缩。
RDS for SQL Server安全最佳实践	提供RDS for SQL Server安全配置的规范性指导。

2 RDS for MySQL

2.1 自建 MySQL 迁移到 RDS for MySQL

2.1.1 方案概述

场景描述

本实践主要包含以下内容：

- 介绍如何将自建MySQL迁移到RDS for MySQL实例。

RDS for MySQL 产品优势

- **低成本 享更多的服务**
  只需支付实例费用，无需其他硬件、托管等费用。
- **超高性能 极致用户体验**
  - 100%兼容MySQL应用。
  - 高并发性能满足苛刻性能要求。
  - 支持大量连接，响应更快速。
- **高安全性 保证数据库安全**
  - 网络隔离、访问控制、传输加密、存储加密、防DDos攻击，全系列的数据库高安全等级，保证数据库安全。
  - 华为云的108项关键安全能力，在国内首家通过NIST CSF网络安全框架的最高等级认证。
- **高可靠性 多种部署及容灾方案**
  数据备份、数据恢复、双机热备、异地容灾、同城容灾，多种部署及容灾方案，为数据可靠性保驾护航。

服务列表

- 虚拟私有云 VPC

- 弹性云服务器 ECS
- 云数据库RDS
- 数据复制服务 DRS

使用说明

- 本实践的资源规划仅作为演示，实际业务场景资源以用户实际需求为准。
- 本实践端到端的数据为测试数据，仅供参考；更多关于MySQL数据迁移须知请单击**这里**了解。

前提条件

- 拥有华为云账号。
- 账户余额大于等于0美元。

2.1.2 资源规划

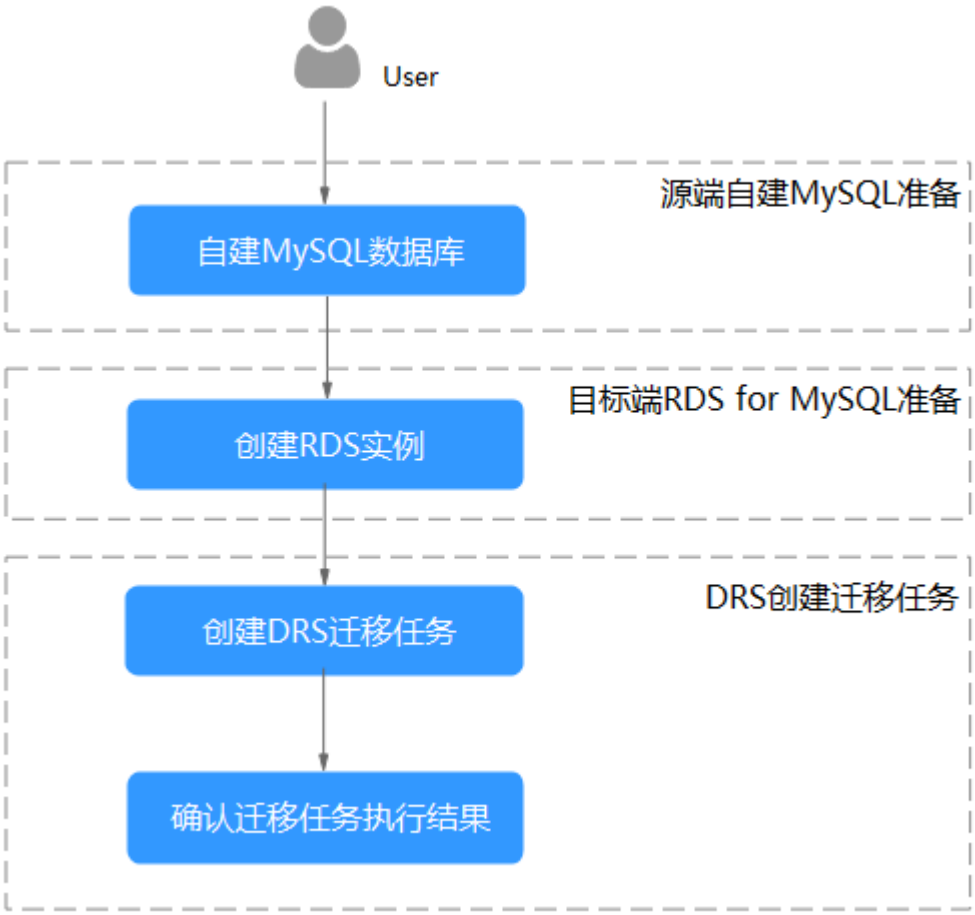
表 2-1 资源规划

类别	子类	规划	备注
RDS	RDS实例名	rds-mysql	自定义，易理解可识别。
	数据库版本	MySQL 5.7	-
	实例类型	单机	本示例中为单机。 实际使用时，为提升业务可靠性，推荐选择主备RDS实例。
	存储类型	SSD云盘	-
	可用区	可用区3	本示例中为单机。 实际业务场景推荐选择主备RDS实例，此时建议将两个实例创建在不同的可用区，提升业务可靠性。
	规格	通用型 4 vCPUs | 8GB	-
DRS迁移任务	迁移任务名	DRS-mysql	自定义
	源数据库引擎	MySQL	本示例中源数据库为自建MySQL，即在华为云弹性云服务器上安装社区版MySQL。
	目标数据库引擎	MySQL	本示例中目标数据库也是MySQL，使用的云数据库 RDS for MySQL实例。
	网络类型	VPC网络	本示例中采用“VPC网络”。

2.1.3 操作流程

构建MySQL服务器、购买RDS实例，并且将MySQL服务器数据迁移到RDS实例的整个流程的主要任务流如图2-1所示。

图 2-1 流程图



2.1.4 上云操作

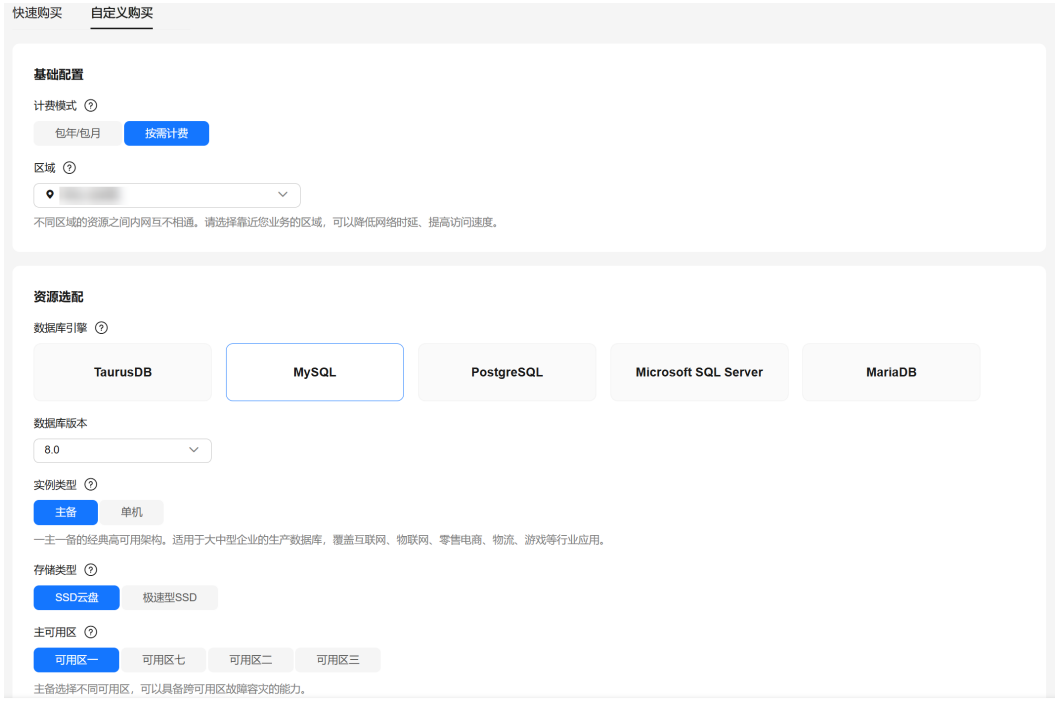
2.1.4.1 创建 RDS for MySQL 实例

本章节介绍创建RDS for MySQL实例，该实例选择和自建MySQL服务器相同的VPC和安全组。

步骤1 进入**购买云数据库RDS页面**。

步骤2 配置实例基本信息。选择区域“中国-香港”。

图 2-2 基本信息



步骤3 选择实例规格，其他参数默认配置。

图 2-3 实例规格

步骤4 单击“立即购买”。

步骤5 进行规格确认。

- 如果需要重新选择实例规格，单击“上一步”，回到上个页面修改实例信息。
- 如果规格确认无误，单击“提交”，完成购买实例的申请。

步骤6 返回云数据库实例列表。

当RDS实例运行状态为“正常”时，表示实例创建完成。

----结束

2.1.4.2 创建迁移任务

本章节介绍创建DRS迁移任务，将自建MySQL服务器上的loadtest数据库迁移到RDS for MySQL实例。

迁移前检查

在创建任务前，需要针对迁移环境进行手工自检，以确保您的迁移任务更加顺畅。

本示例中，为MySQL到RDS for MySQL的入云迁移，您可以参考**入云使用须知**获取相关信息。

操作任务

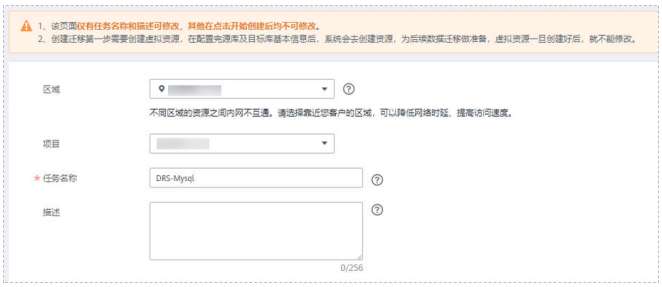
介绍自建MySQL服务器上的loadtest数据库迁移到RDS for MySQL实例的详细操作过程。

步骤1 进入**创建迁移任务页面**。

步骤2 填写迁移任务参数：

1. 配置迁移任务名称。选择区域“中国-香港”。

图 2-4 迁移任务



2. 填写迁移数据并选择模板库。

这里的目标库选择**创建RDS for MySQL实例**创建的RDS实例。

图 2-5 迁移实例信息

3. 企业项目选择“default”。

步骤3 单击“开始创建”。

迁移实例创建中，大约需要5-10分钟。

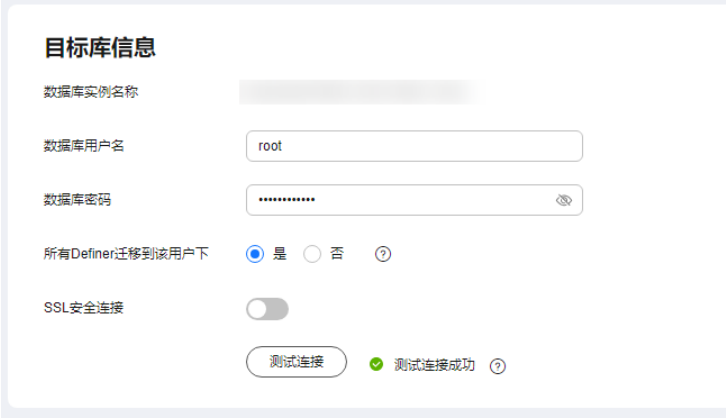
步骤4 配置源库信息和目标库数据库密码，单击“下一步”。

1. 配置源库信息。
2. 单击“测试连接”。
   当界面显示“测试成功”时表示连接成功。

图 2-6 源库信息

3. 配置目标库数据库用户名和密码。
4. 单击“测试连接”。
   当界面显示“测试成功”时表示连接成功。

图 2-7 目标库信息



步骤5 在“迁移设置”页面，设置迁移用户和迁移对象，单击“下一步”。

本次选择：全部迁移。

步骤6 在“预检查”页面，进行迁移任务预校验，校验是否可进行迁移。

预检查完成后，且预检查通过率为100%时，单击“下一步”。

步骤7 进入“参数对比”页面，可跳过该步骤，单击页面右下角“下一步”按钮，继续执行后续操作。

步骤8 在“任务确认”页面，设置迁移任务的启动时间、任务异常通知设置、SMN主题、时延阈值、任务异常自动结束时间，并确认迁移任务信息无误后，单击“启动任务”，提交迁移任务。

步骤9 迁移任务提交后，您可在“实时迁移管理”页面，查看并管理自己的任务。

----结束

2.1.4.3 确认数据迁移结果

确认升级迁移结果有两种方式：

方式一：（自动）**在DRS管理控制台查看迁移结果**。DRS会针对迁移对象、用户、数据等维度进行对比，从而给出迁移结果。

方式二：（手工）**在RDS管理控制台查看迁移结果**。直接登录数据库查看库、表、数据是否迁移完成。手工确认数据迁移情况。

在 DRS 管理控制台查看迁移结果

步骤1 登录**华为云控制台**。

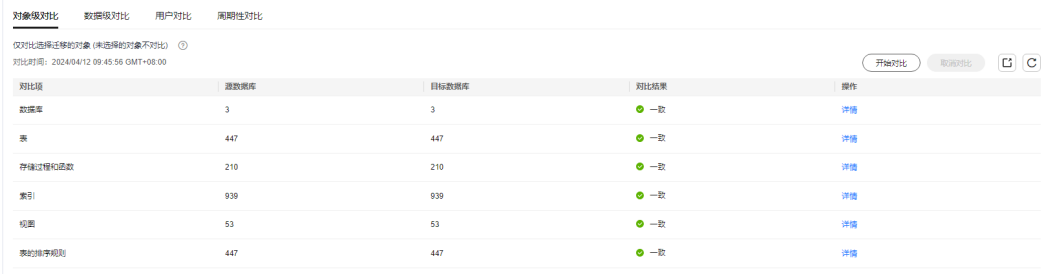
步骤2 单击管理控制台左上角的，选择区域“中国-香港”。

步骤3 单击左侧的服务列表图标，选择“数据库 > 数据复制服务 DRS”。

步骤4 单击DRS实例。

步骤5 单击“迁移对比”。

图 2-8 迁移对比



步骤6 然后选择“数据对比 全面检查”和“数据对比 割接复查”确认迁移结果。

预检查不通过项可以参考**预检查不通过项修复方法**查询解决方法。

----结束

在 RDS 管理控制台查看迁移结果·

步骤1 登录**华为云控制台**。

步骤2 单击管理控制台左上角的 ，选择区域“中国-香港”。

步骤3 单击左侧的服务列表图标，选择“数据库 > 云数据库RDS”。

步骤4 单击RDS实例后的“登录”。

步骤5 在弹出的对话框中输入密码，单击“测试连接”。

步骤6 测试连接成功后，单击“登录”。

步骤7 查看并确认目标库名和表名等。确认相关数据是否迁移完成。

----结束

2.2 RDS for MySQL 通过 DRS 搭建异地单主灾备

2.2.1 方案概述

场景描述

本实践主要包含以下内容：

- 介绍如何创建RDS for MySQL实例。
- 介绍RDS for MySQL实例如何通过DRS服务搭建异地单主灾备。

前提条件

- 拥有华为云账号。
- 账户余额大于等于0美元。

实现原理

RDS跨Region容灾实现原理说明：

在两个数据中心独立部署RDS for MySQL实例，通过DRS服务将生产中心RDS for MySQL库中的数据同步到灾备中心RDS for MySQL库中，实现RDS for MySQL主实例和跨Region灾备实例之间的实时同步。

服务列表

- 虚拟私有云 VPC
- 弹性公网IP EIP
- 云数据库 RDS
- 数据复制服务 DRS

使用说明

- 本实践的资源规划仅作为演示，实际业务场景资源以用户实际需求为准。
- 本实践端到端的数据为测试数据，仅供参考；更多关于RDS for MySQL实例灾备须知请单击**这里**了解。

2.2.2 资源规划

表 2-2 资源规划

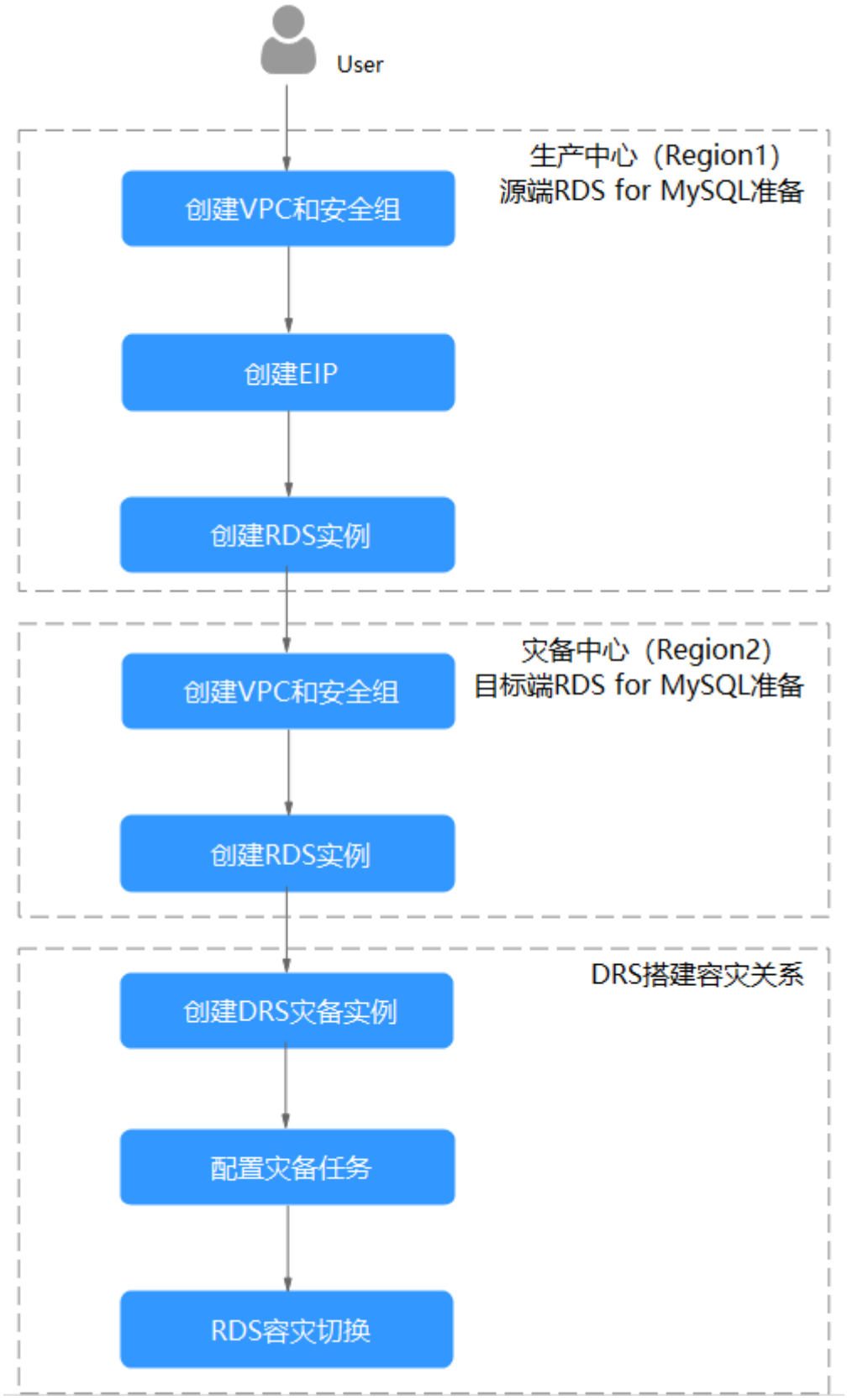
类别	子类	规划	备注
生产中心VPC	VPC名称	vpc-01	自定义，易理解可识别。
	所属Region	中国-香港	选择和自己业务区最近的Region，减少网络时延。
	可用区	可用区二	-
	子网网段	192.168.0.0/24	子网选择时建议预留足够的网络资源。
	子网名称	subnet-3c29	自定义，易理解可识别。
灾备中心VPC	VPC名称	vpc-DR	自定义，易理解可识别。
	所属Region	亚太-新加坡	选择和自己业务区最近的Region，减少网络时延。
	可用区	可用区一	-
	子网网段	192.168.0.0/24	子网选择时建议预留足够的网络资源。
	子网名称	subnet-ac27	自定义，易理解可识别。
生产中心RDS for MySQL实例	RDS实例名称	rds-database-01	自定义，易理解可识别。
	所属Region	中国-香港	选择和自己业务区最近的Region，减少网络时延。
	数据库版本	MySQL 8.0	-

类别	子类	规划	备注
	实例类型	单机	本示例中为单机。 实际使用时，为提升业务可靠性，推荐选择主备RDS实例。
	存储类型	超高IO	-
	可用区	可用区二	本示例中为可用区二。 实际业务场景推荐选择主备RDS实例，此时建议将两个实例创建在不同的可用区，提升业务可靠性。
	性能规格	通用增强型 2 vCPUs | 4GB	-
灾备中心RDS for MySQL实例	RDS实例名称	rds-DR	自定义，易理解可识别。
	所属Region	亚太-新加坡	选择和自己业务区最近的Region，减少网络时延。
	数据库版本	MySQL 8.0	-
	实例类型	单机	本示例中为单机。 实际使用时，为提升业务可靠性，推荐选择主备RDS实例。
	存储类型	SSD云盘	-
	可用区	可用区一	本示例中为可用区一。 实际业务场景推荐选择主备RDS实例，此时建议将两个实例创建在不同的可用区，提升业务可靠性。
	性能规格	通用型 2 vCPUs | 8GB	-
DRS灾备任务	灾备任务名称	DRS-DR-Task	自定义，易理解可识别。
	源数据库引擎	MySQL	本示例中源数据库为在“中国-香港”创建的业务实例。
	目标数据库引擎	MySQL	本示例中目标数据库为在“亚太-新加坡”创建的灾备实例。
	网络类型	公网网络	本示例中采用“公网网络”。

2.2.3 操作流程

创建RDS业务实例以及灾备实例，并且将业务实例数据迁移到灾备实例的整个流程的主要任务流如下图所示。

图 2-9 流程图



2.2.4 生产中心 RDS for MySQL 实例准备

2.2.4.1 创建 VPC 和安全组

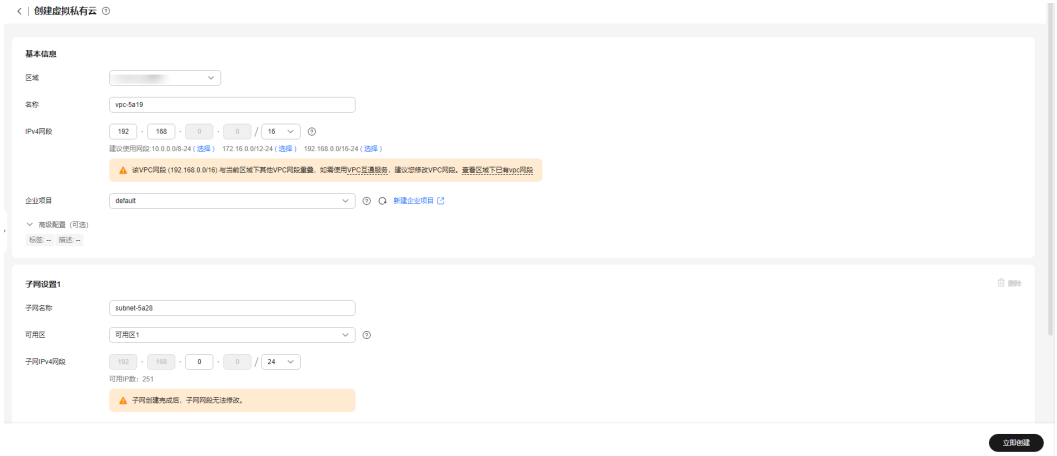
本章节介绍创建在生产中心创建RDS实例所属VPC和安全组。

创建 VPC

步骤1 进入**创建虚拟私有云页面**。

步骤2 在“创建虚拟私有云”页面，选择区域“中国-香港”。根据界面提示完成基本信息、子网配置和地址配置。

图 2-10 创建 VPC



步骤3 单击“立即创建”，完成生产VPC创建。

----结束

创建安全组

步骤1 登录**华为云控制台**。

步骤2 单击管理控制台左上角的，选择区域“中国-香港”。

步骤3 单击左侧的服务列表图标，选择“网络 > 虚拟私有云 VPC”。

步骤4 在左侧导航树，选择“访问控制 > 安全组”。

步骤5 单击“创建安全组”。

图 2-11 创建安全组

步骤6 单击“立即创建”，完成生产安全组创建。

----结束

2.2.4.2 创建 EIP

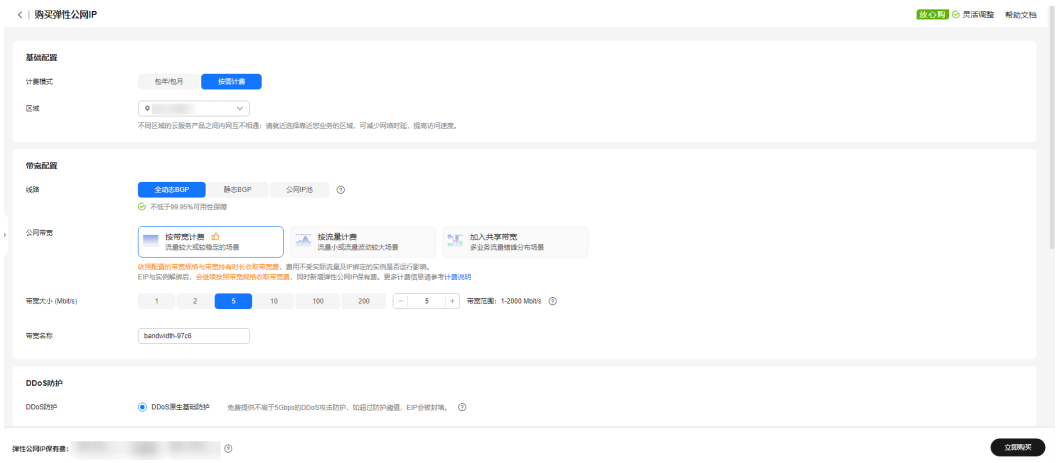
外部通过EIP访问应用系统，DRS通过EIP连接源数据库，需要为源数据库绑定EIP。

创建 EIP

步骤1 进入**购买弹性公网IP页面**。

步骤2 在“购买弹性公网IP”页面，选择区域“中国-香港”。根据界面提示完成基本信息和带宽配置。

图 2-12 购买 EIP



步骤3 单击“立即购买”。

步骤4 确认信息无误，单击“提交”，完成EIP购买。

----结束

2.2.4.3 创建 RDS for MySQL 实例

本章节介绍创建RDS for MySQL业务实例，选择已规划的业务实例所属VPC，并为业务实例（源实例）绑定EIP。

创建 RDS for MySQL 实例

步骤1 进入**购买云数据库RDS页面**。

步骤2 选择区域“中国-香港”。填选实例信息后，单击“立即购买”。

图 2-13 选择引擎版本信息

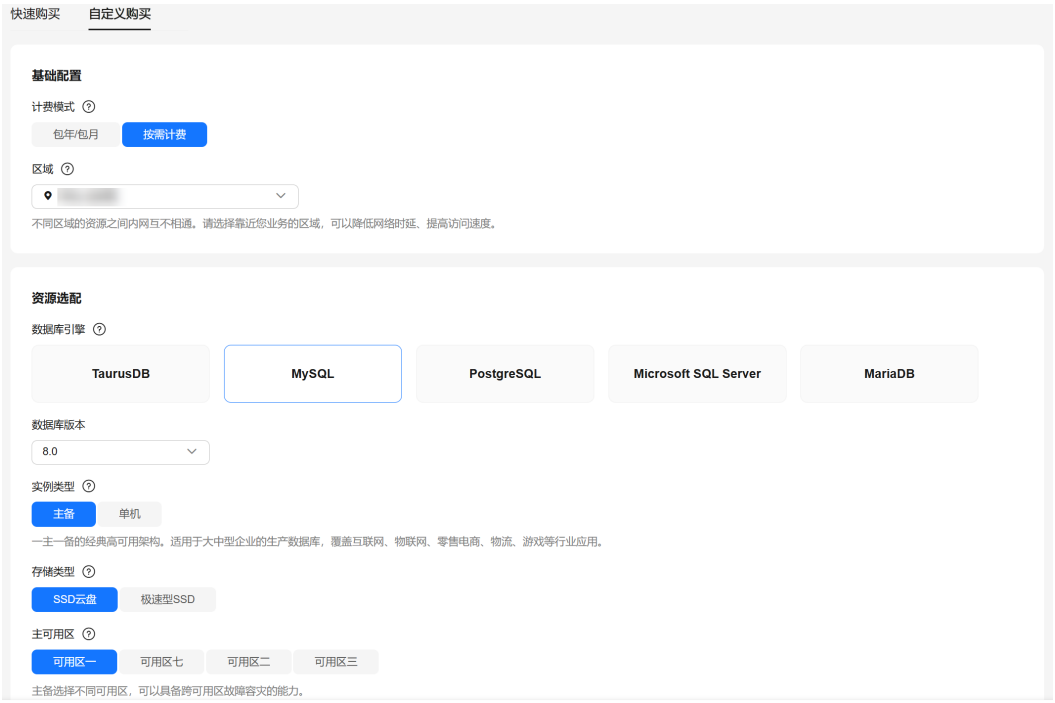
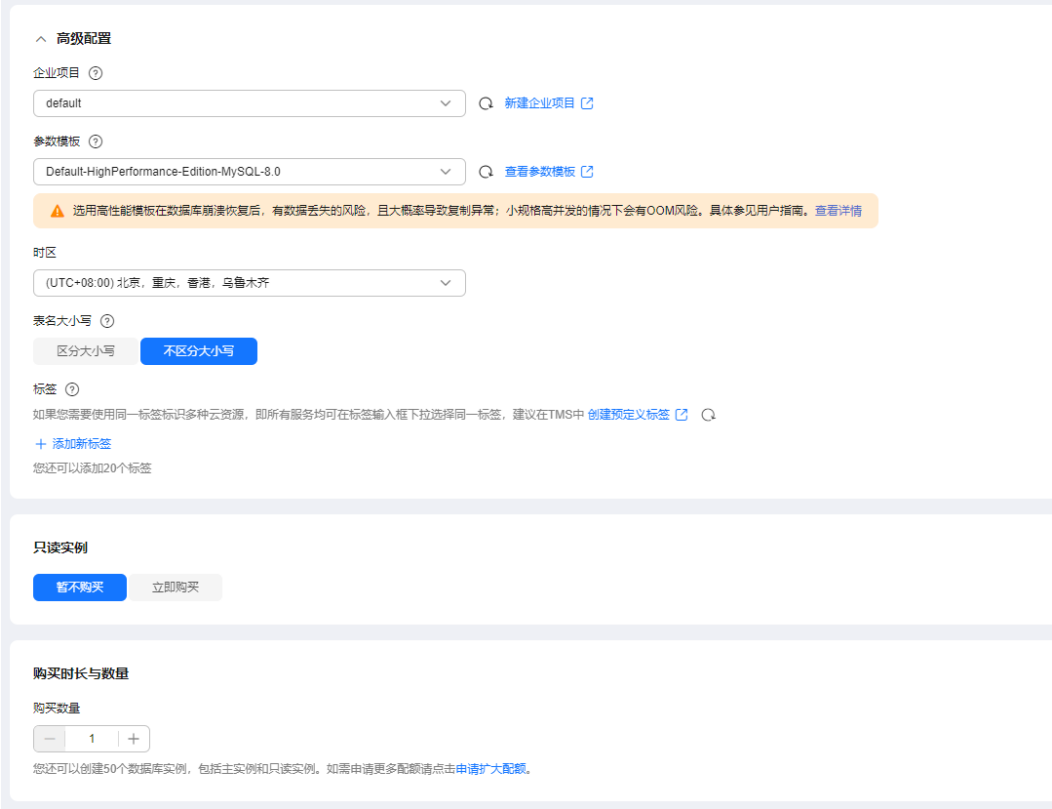


图 2-14 选择规格信息

图 2-15 选择已规划的网络信息

图 2-16 高级配置



步骤3 进行规格确认。

- 如果需要重新选择实例规格，单击“上一步”，回到上个页面修改实例信息。
- 如果规格确认无误，单击“提交”，完成购买实例的申请。

步骤4 参考如下步骤，在RDS实例管理界面，为**步骤3**创建的RDS实例绑定弹性公网IP。

1. 在“实例管理”页面，选择指定的实例，单击实例名称，进入实例概览页面。

   图 2-17 实例管理

2. 选择“连接管理”页签，单击“公网地址”处的“绑定”。
3. 在弹出框中，显示“未绑定”状态的弹性公网IP，选择已规划的弹性公网IP，单击“确定”，提交绑定任务。

图 2-18 绑定弹性公网 IP

----结束

2.2.5 灾备中心 RDS for MySQL 实例准备

2.2.5.1 创建 VPC 和安全组

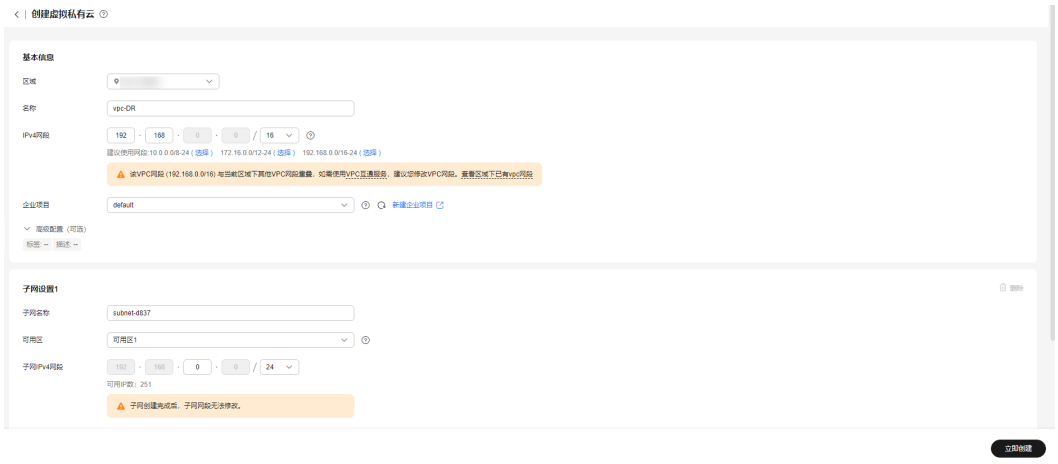
灾备中心的实例和生产中心实例在不同区域，本章节介绍创建在灾备中心创建RDS实例所属VPC和安全组。

创建 VPC

步骤1 进入**创建虚拟私有云页面**。

步骤2 在“创建虚拟私有云”页面，选择区域“亚太-新加坡”。根据界面提示完成基本信息、子网配置和地址配置。

图 2-19 创建灾备 VPC



步骤3 单击“立即创建”，完成灾备VPC创建。

----结束

创建安全组

步骤1 登录**华为云控制台**。

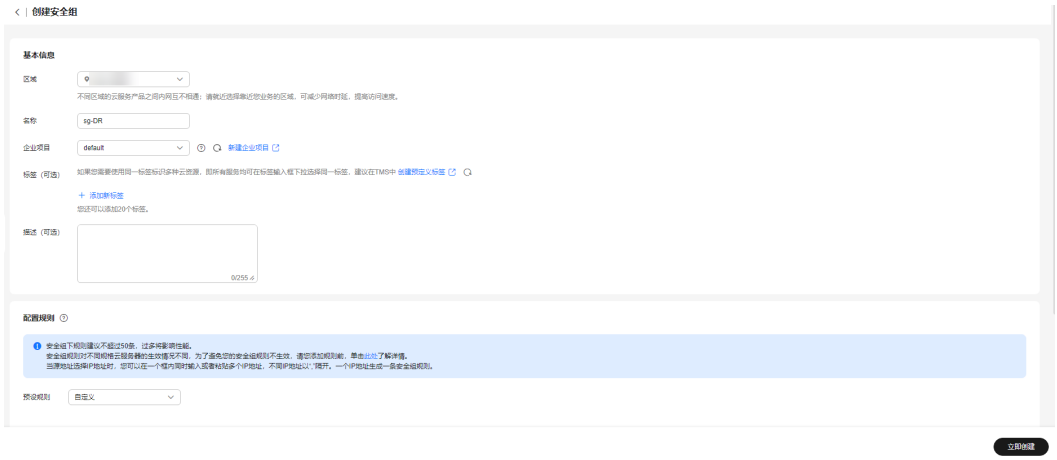
步骤2 单击管理控制台左上角的 ，选择区域“亚太-新加坡”。

步骤3 单击左侧的服务列表图标，选择“网络 > 虚拟私有云 VPC”。

步骤4 在左侧导航树，选择“访问控制 > 安全组”。

步骤5 单击“创建安全组”。

图 2-20 创建安全组



步骤6 单击“立即创建”，完成灾备安全组创建。

----结束

2.2.5.2 创建 RDS for MySQL 实例

本章节介绍创建RDS for MySQL灾备实例，选择已规划的灾备实例所属VPC。

创建 RDS for MySQL 实例

步骤1 进入**购买云数据库RDS页面**。

步骤2 选择区域“亚太-新加坡”。填选实例信息后，单击“立即购买”。

图 2-21 选择灾备实例引擎版本信息

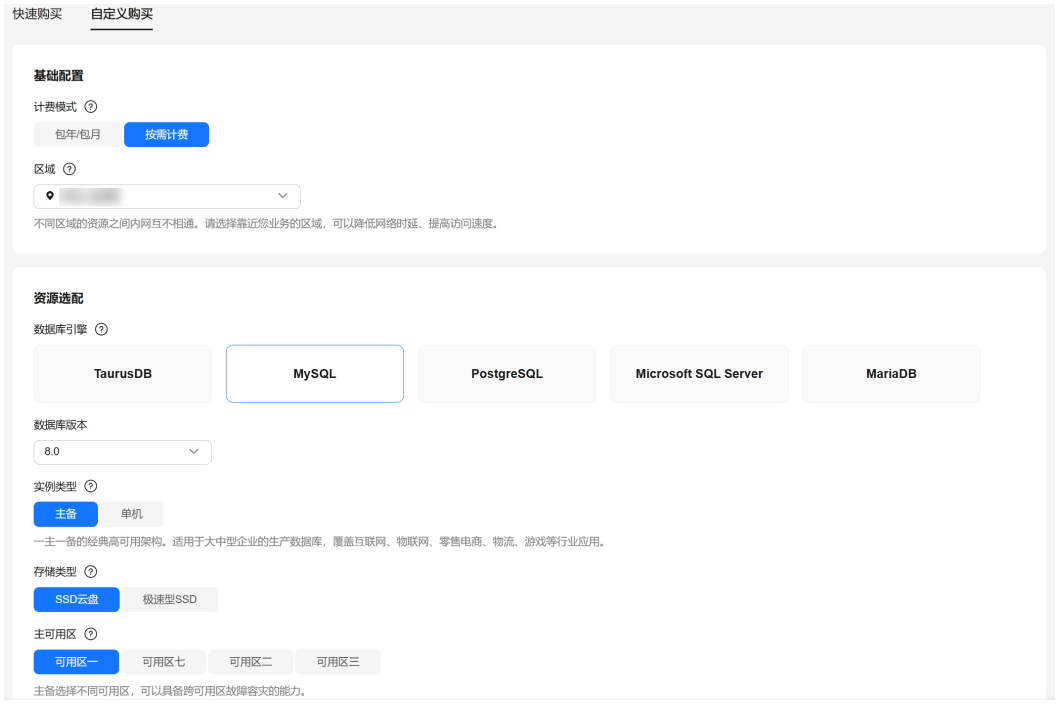


图 2-22 选择灾备实例规格信息

图 2-23 选择灾备实例已规划的网络信息

图 2-24 高级配置

步骤3 进行规格确认。

- 如果需要重新选择实例规格，单击“上一步”，回到上个页面修改实例信息。
- 如果规格确认无误，单击“提交”，完成购买实例的申请。

----结束

2.2.6 搭建容灾关系

2.2.6.1 创建 DRS 灾备实例

本章节介绍创建DRS灾备实例，创建时选择灾备中心创建的RDS for MySQL实例。

操作步骤

步骤1 进入**创建灾备任务页面**。

步骤2 选择区域“亚太-新加坡”。灾备关系选择“本云为备”，灾备数据库实例选择在“亚太-新加坡”新创建的RDS for MySQL灾备实例，单击“开始创建”，开始创建灾备实例。

图 2-25 设置灾备实例信息

步骤3 返回“实时灾备管理”页面，可以看到新创建的灾备实例。

----结束

2.2.6.2 配置灾备任务

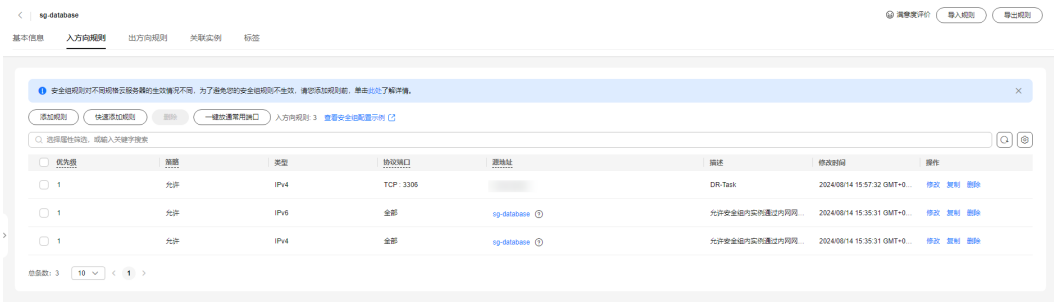
本章节介绍配置DRS灾备实例，包含源库和目标库的配置。

操作步骤

步骤1 在“实时灾备管理”页面，选择已创建的灾备任务，单击“编辑”。

步骤2 根据界面提示，将灾备实例的弹性公网IP加入生产中心RDS for MySQL实例所属安全组的入方向规则，选择TCP协议，端口为生产中心RDS for MySQL实例的端口号。

图 2-26 添加安全组规则

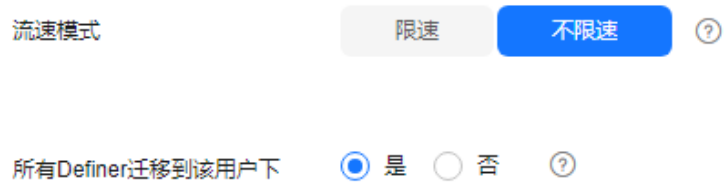


源库信息中的“IP地址或域名”填写生产中心RDS for MySQL实例绑定的EIP，“端口”填写生产中心RDS for MySQL实例的端口号。测试通过后，单击“下一步”。

图 2-27 编辑灾备任务

步骤3 设置流速模式后，单击“下一步”。

图 2-28 设置流速模式



步骤4 查看预检查100%通过，单击“下一步”。

步骤5 设置参数后，单击“下一步”。

图 2-29 设置参数

步骤6 单击“启动任务”。

图 2-30 启动任务

步骤7 查看任务状态为“灾备中”。

对于灾备中的任务，您可通过**数据对比**功能查看灾备前后数据是否一致。

----结束

2.2.6.3 RDS 容灾切换

生产中心数据库故障时，需要手动将灾备数据库实例切换为可读写状态。切换后，将通过灾备实例写入数据，并同步到源库。

操作步骤

步骤1 生产中心源库发生故障，例如：源库无法连接、源库执行缓慢、CPU占比高。

步骤2 收到SMN邮件通知。

步骤3 查看灾备任务时延异常。

步骤4 用户自行判断业务已经停止。具体请参考**如何确保业务数据库的全部业务已经停止**。

步骤5 选择“批量操作 > 主备倒换”，将灾备实例由只读状态更改为读写状态。

图 2-31 主备倒换

步骤6 在应用端修改数据库连接地址后，可正常连接数据库，进行数据读写。

----结束

2.3 其他云 MySQL 迁移到云数据库 RDS for MySQL

2.3.1 方案概述

场景描述

本实践主要包含以下内容：

- 介绍如何创建RDS for MySQL实例。
- 介绍如何将其他云MySQL迁移到RDS for MySQL实例。

前提条件

- 拥有华为云账号。
- 账户余额大于等于0美元。

服务列表

- 虚拟私有云 VPC
- 云数据库RDS
- 数据复制服务 DRS

使用说明

- 本实践的资源规划仅作为演示，实际业务场景资源以用户实际需求为准。
- 本实践端到端的数据为测试数据，仅供参考；更多关于MySQL数据迁移须知请单击**这里**了解。

2.3.2 资源规划

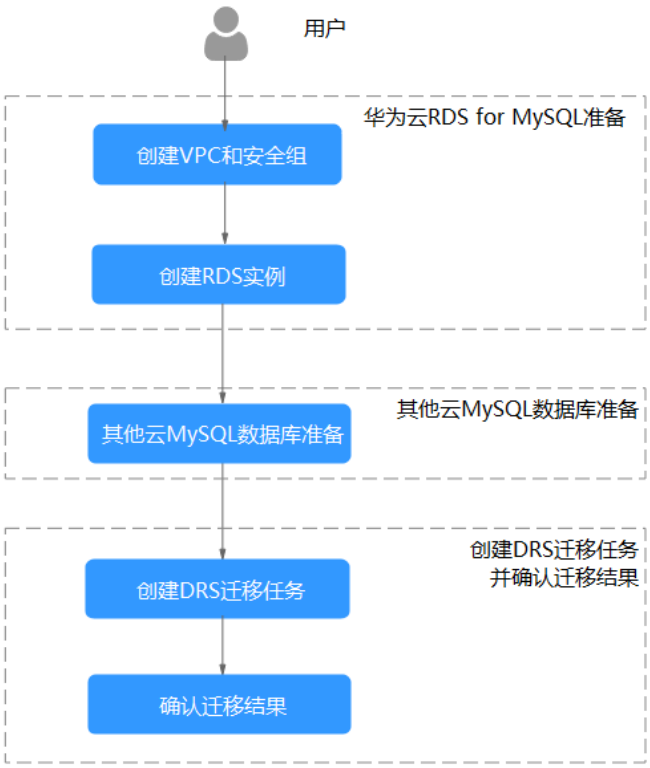
表 2-3 资源规划

类别	子类	规划	备注
VPC	VPC名称	vpc-src-172	自定义，易理解可识别。
	所属Region	测试Region	现网实际选择时建议选择和自己业务区最近的Region，减少网络时延。
	可用区	可用区3	-
	子网网段	172.16.0.0/16	子网选择时建议预留足够的网络资源。
	子网名称	subnet-src-172	自定义，易理解可识别。
其他云MySQL	数据库版本	MySQL 5.7	-
	IP地址	10.154.217.42	仅作为示例。

类别	子类	规划	备注
	端口	3306	-
RDS for MySQL实例	RDS实例名称	rds-mysql	自定义，易理解可识别。
	数据库版本	MySQL 5.7	-
	实例类型	单机	本示例中为单机。 实际使用时，为提升业务可靠性，推荐选择主备RDS实例。
	存储类型	SSD云盘	-
	可用区	可用区一	本示例中为可用区一。 实际业务场景推荐选择主备RDS实例，此时建议将两个实例创建在不同的可用区，提升业务可靠性。
	性能规格	通用型 2 vCPUs | 8GB	-
DRS迁移任务	迁移任务名	DRS-mysql	自定义。
	源数据库引擎	MySQL	-
	目标数据库引擎	MySQL	-
	网络类型	公网网络	本示例中采用公网网络。

2.3.3 操作流程

图 2-32 流程图



2.3.4 创建 VPC 和安全组

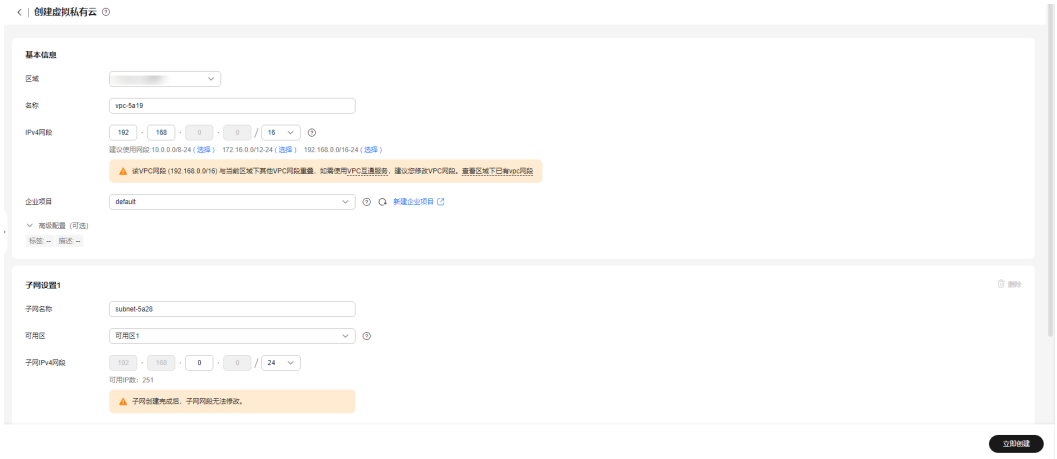
创建VPC和安全组，为创建RDS for MySQL实例准备好网络资源和安全组。

创建 VPC

步骤1 进入**创建虚拟私有云页面**。

步骤2 在“创建虚拟私有云”页面，根据页面完成基本信息、子网配置和地址配置。

图 2-33 创建虚拟私有云



步骤3 单击“立即创建”。

步骤4 返回VPC列表，查看创建VPC是否创建完成。

当VPC列表的VPC状态为“可用”时，表示VPC创建完成。

----结束

创建安全组

步骤1 登录**华为云控制台**。

步骤2 单击管理控制台左上角的，选择区域“中国-香港”。

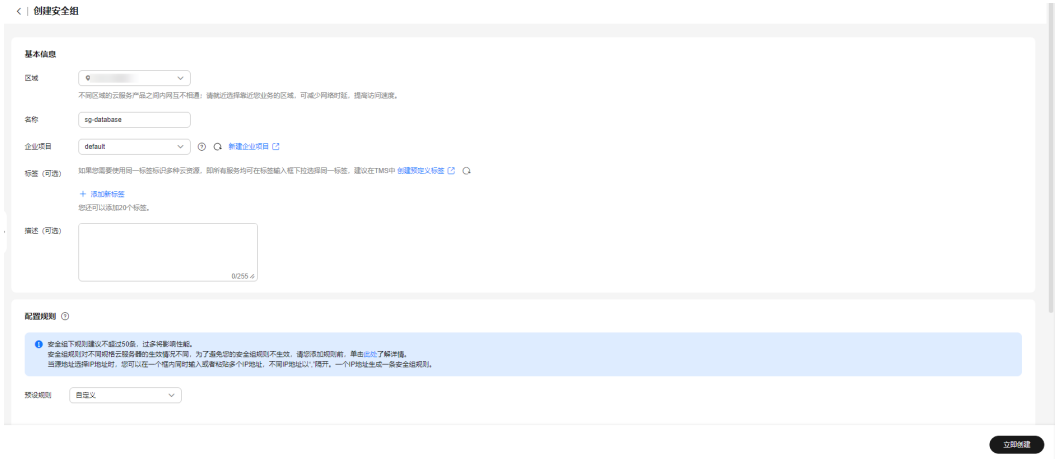
步骤3 单击左侧的服务列表图标，选择“网络 > 虚拟私有云 VPC”，进入虚拟私有云信息页面。

步骤4 选择“访问控制 > 安全组”。

步骤5 单击“创建安全组”。

步骤6 填写安全组名称等信息。

图 2-34 创建安全组



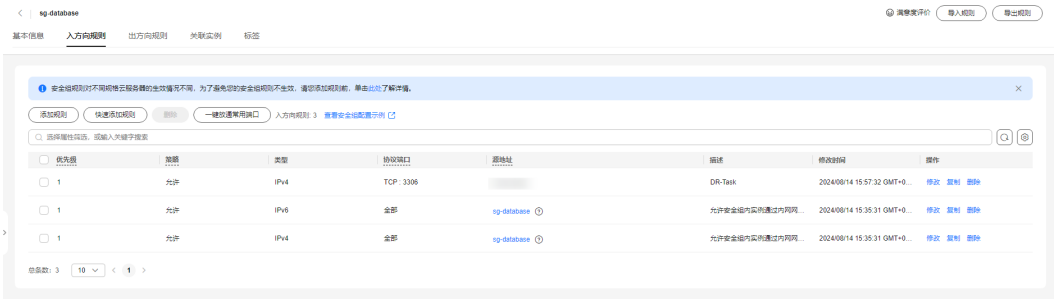
步骤7 单击“立即创建”。

步骤8 返回安全组列表，单击安全组名称。

步骤9 选择“入方向规则”，单击“添加规则”。

步骤10 配置入方向规则，放通数据库3306端口。

图 2-35 入方向规则



----结束

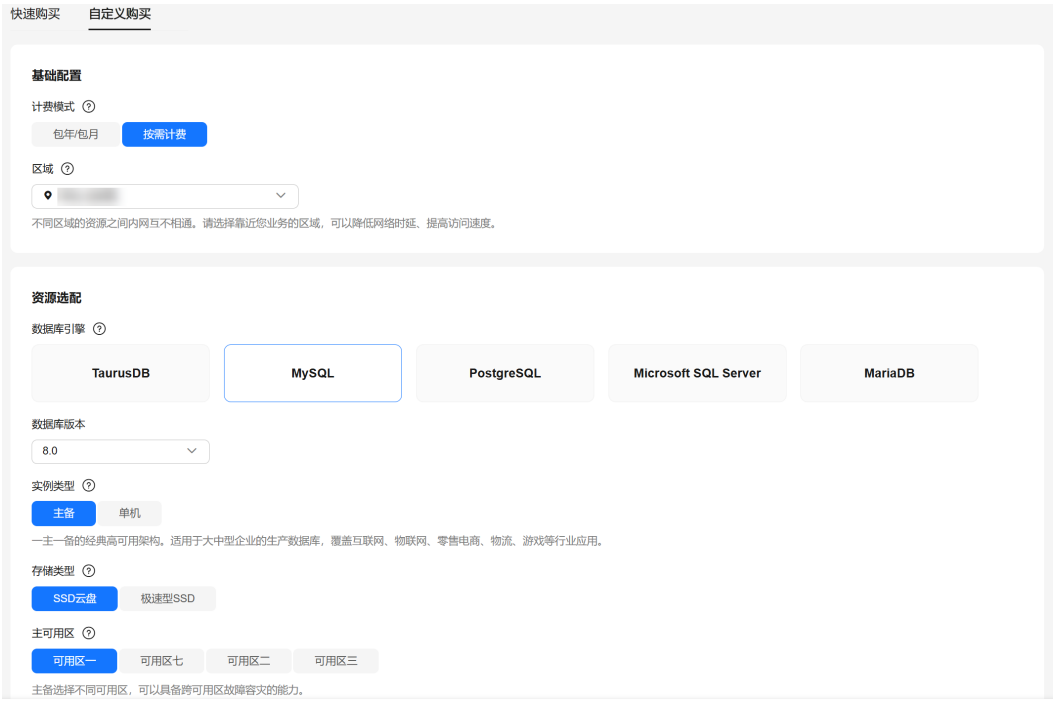
2.3.5 创建 RDS for MySQL 实例

本章节介绍创建RDS for MySQL实例。

步骤1 进入**购买云数据库RDS页面**。

步骤2 配置实例基本信息。选择区域“中国-香港”。

图 2-36 基本信息



步骤3 选择实例规格。

图 2-37 实例规格

步骤4 选择实例所属的VPC和安全组、配置数据库端口。

VPC和安全组已在**创建VPC和安全组**中准备好。

图 2-38 选择网络

步骤5 高级配置。

图 2-39 高级配置

步骤6 单击“立即购买”。

步骤7 进行规格确认。

- 如果需要重新选择实例规格，单击“上一步”，回到上个页面修改实例信息。
- 如果规格确认无误，单击“提交”，完成购买实例的申请。

步骤8 返回云数据库实例列表。当RDS实例运行状态为“正常”时，表示实例创建完成。

----结束

2.3.6 其他云 MySQL 实例准备

前提条件

- 已购买其他云MySQL实例。
- 账号权限符合要求，具体见**账号权限要求**。

账号权限要求

当使用DRS将其他云MySQL数据库的数据迁移到云数据库 RDS for MySQL实例时，账号权限要求如**表2-4**所示，授权的具体操作请参考**授权操作**。

表 2-4 迁移账号权限

迁移类型	全量迁移	全量+增量迁移
源数据库（MySQL）	SELECT、SHOW VIEW、EVENT。	SELECT、SHOW VIEW、EVENT、LOCK TABLES、REPLICATION SLAVE、REPLICATION CLIENT。

网络设置

源数据库MySQL实例需要开放外网域名的访问。

白名单设置

其他云MySQL实例需要将目标端DRS迁移实例的弹性公网IP添加到其网络白名单中，目标端DRS迁移实例的弹性公网IP在创建完DRS迁移实例后可以获取到，参考**创建DRS迁移任务**的**步骤3**，确保源数据库可以与DRS实例互通，各厂商云数据库添加白名单的方法不同，请参考各厂商云数据库官方文档进行操作。

2.3.7 上云操作

2.3.7.1 创建 DRS 迁移任务

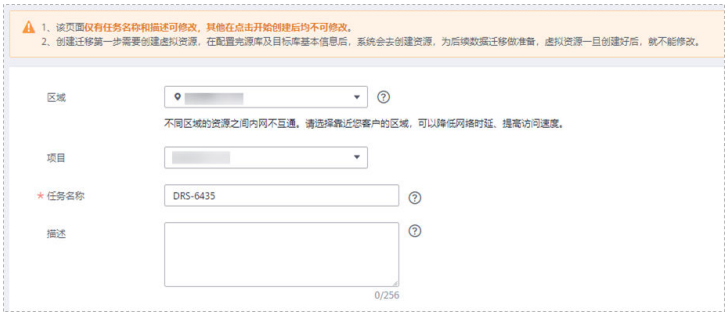
创建迁移任务

步骤1 进入**创建迁移任务页面**。

步骤2 填写迁移任务参数：

1. 配置迁移任务名称。选择区域，即为目标实例所在的区域。

图 2-40 迁移任务



2. 填写迁移数据并选择模板库。
   这里的目标库选择**创建RDS for MySQL实例**创建的RDS实例。

图 2-41 填写迁移实例信息

步骤3 单击“开始创建”。

迁移实例创建中，大约需要5-10分钟。迁移实例创建完成后可获取弹性公网IP信息。

迁移实例创建成功，其弹性公网IP为10.154.218.89。请在源数据库网络白名单中加入上述IP，确保源数据库与此IP可连通。

步骤4 配置源库信息和目标库数据库密码。

图 2-42 配置源库和目标库

步骤5 单击“下一步”。

步骤6 在“迁移设置”页面，设置流速模式、迁移用户和迁移对象。

- 流速模式：不限速
- 迁移对象：全部迁移

步骤7 单击“下一步”，在“预检查”页面，进行迁移任务预校验，校验是否可进行任务迁移。

- 查看检查结果，如有不通过的检查项，需要修复不通过项后，单击“重新校验”按钮重新进行迁移任务预校验。
- 预检查完成后，且所有检查项结果均成功时，单击“下一步”。

步骤8 参数对比。

- 如果您选择不进行参数对比，可跳过该步骤，单击页面右下角“下一步”按钮，继续执行后续操作。
- 如果您选择进行参数对比，对于常规参数，如果源库和目标库存在不一致的情况，建议将目标数据库的参数值通过“一键修改”按钮修改为和源库对应参数相同的值。

步骤9 单击“提交任务”。

返回DRS实时迁移管理，查看迁移任务状态。

启动中状态一般需要几分钟，请耐心等待。

当状态变更为“已结束”，表示迁移任务完成。

----结束

2.3.7.2 确认迁移结果

确认迁移结果可参考如下两种方式：

1. DRS会针对迁移对象、用户、数据等维度进行对比，从而给出迁移结果，详情参见**在DRS管理控制台查看迁移结果**。
2. 直接登录数据库查看库、表、数据是否迁移完成。手工确认数据迁移情况，详情参见**在RDS管理控制台查看迁移结果**。

在 DRS 管理控制台查看迁移结果

步骤1 登录**华为云控制台**。

步骤2 单击管理控制台左上角的 ，选择目标区域。

步骤3 单击左侧的服务列表图标，选择“数据库 > 数据复制服务 DRS”。

步骤4 单击DRS实例名称。

步骤5 单击“迁移对比”，选择“对象级对比”，单击“开始对比”，校验数据库对象是否缺失。

步骤6 选择“数据级对比”，单击“创建对比任务”，查看迁移的数据库和表内容是否一致。

步骤7 选择“用户对比”，查看迁移的源库和目标库的账号和权限是否一致。

----结束

在 RDS 管理控制台查看迁移结果

步骤1 登录华为云控制台。

步骤2 单击管理控制台左上角的，选择目标区域。

步骤3 单击左侧的服务列表图标，选择“数据库 > 云数据库RDS”。

步骤4 单击迁移的目标实例的操作列的“登录”。

步骤5 在弹出的对话框中输入密码，单击“测试连接”。

步骤6 测试连接成功后，单击“登录”。

步骤7 查看并确认目标库名和表名等。确认相关数据是否迁移完成。

----结束

进行性能测试

迁移完成后，可以根据需要进行性能测试。

2.4 使用 RDS for MySQL 搭建 WordPress

WordPress是使用PHP语言开发的博客平台，用户可以在支持PHP和RDS for MySQL数据库的服务器上搭建属于自己的网站，本文教您通过华为云虚拟私有云、弹性云服务器和RDS for MySQL数据库，轻松几步，在LAMP环境下搭建WordPress。

1. **设置网络**
2. **购买弹性云服务器**
3. **搭建LAMP环境**
4. **购买并配置RDS**
5. **安装WordPress**

准备工作

在搭建过程中，您会使用以下服务或工具：

- 云服务：华为云弹性云服务器ECS和关系型数据库 RDS for MySQL。
- MySQL客户端：配置数据库工具。
- PuTTY：远程登录工具。

说明

以上软件来自第三方网站，仅作示例。若搭建的网站做商业用途，建议自行获取需要的版本软件，以应对不同需求。

设置网络

步骤1 登录华为云控制台。

步骤2 单击管理控制台左上角的，选择区域。

步骤3 选择“网络>虚拟私有云”。进入虚拟私有云信息页面。

步骤4 在“虚拟私有云”页面，单击“创建虚拟私有云”购买VPC，以vpc-01为例。

步骤5 在基本信息页面进行设置，自定义VPC及子网名称，根据实际需求选择可用分区等，IPv4网段选择“192.168”，其他均可以保持默认配置，单击“立即创建”提交任务。创建成功后，返回控制台页面。

步骤6 在“网络控制台”选择“访问控制 > 安全组”，单击“创建安全组”，以sg-01为例。

步骤7 在安全组界面，单击操作列的“配置规则”，进入安全组详情界面。

步骤8 单击“添加规则”，将ECS绑定的**弹性公网IP**添加到入方向规则。

----结束

购买弹性云服务器

步骤1 登录**华为云控制台**。

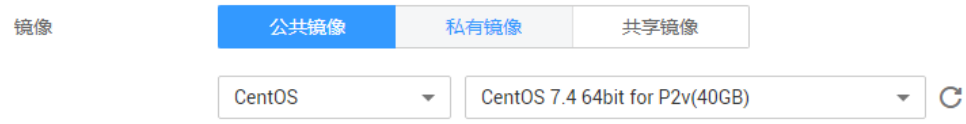
步骤2 单击管理控制台左上角的，选择区域。

步骤3 选择“计算 > 弹性云服务器”。进入弹性云服务器信息页面。

步骤4 在管理控制台购买ECS。

1. **完成基础配置：选择“按需计费”、“区域”和“镜像”，其他默认。**
   此处以公共镜像“CentOS7.4 64bit for P2v(40GB)”为例，如**图2-43**所示。

   图 2-43 选择镜像

2. **网络配置：选择VPC和安全组，购买弹性公网IP，其他默认。**
   a. 选择之前创建的虚拟私有云vpc-01。
   b. 选择之前步骤创建的安全组sg-01。
   c. 在“弹性公网IP”处选择“现在购买”。
3. **高级配置：设置ECS名称和密码，单击“下一步：确认订单”。**
   a. 云服务名称，以ecs-01为例。
   b. 设置密码。
4. **确认配置。确认无误，单击“立即购买”。**

步骤5 ECS创建成功后，您可通过华为云管理控制台，对其进行查看或管理。

----结束

搭建 LAMP 环境

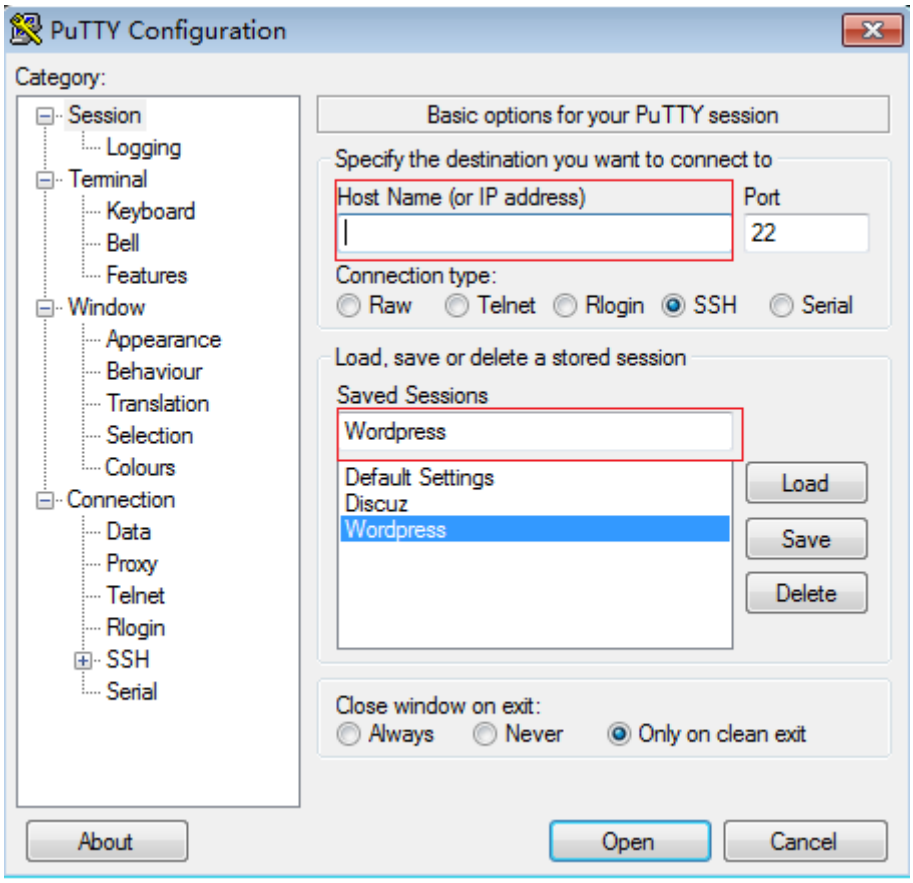
步骤1 下载PuTTY客户端。

步骤2 解压文件后，双击“putty”，显示配置界面。

步骤3 选择“Session”，配置相关信息后，如图2-44，单击“Open”。

1. 在“Host Name (or IP address)”下的输入框中输入ECS的弹性IP地址，其他配置均保持默认值。
2. 在“Saved Sessions”中输入名称，此处以Wordpress为例，单击“Save”，保存会话配置。

图 2-44 配置 PuTTY



步骤4 在登录界面中，输入ECS的用户名和密码，即可登录ECS。

步骤5 通过PuTTY登录云服务器，直接获取root权限，可以直接在PuTTY内输入命令。

请输入MySQL或PHP等软件安装命令，此处以安装PHP为例：

yum install -y httpd php php-fpm php-server php-mysql mysql

结果显示如下，表明安装完成。

```
Complete
```

步骤6 安装解压软件。

yum install -y unzip

步骤7 下载并解压WordPress安装文件。

wget -c https://cn.wordpress.org/wordpress-4.9.1-zh_CN.tar.gz

tar xzf wordpress-4.9.1-zh_CN.tar.gz -C /var/www/html

chmod -R 777 /var/www/html

步骤8 安装完成后，依次启动相关服务。

systemctl start httpd.service

systemctl start php-fpm.service

步骤9 设置服务开机自启动。

systemctl enable httpd.service

----结束

购买并配置 RDS

步骤1 请根据具体需求**购买华为云RDS for MySQL数据库实例**。

- 选择MySQL 5.7版本，创建以“rds-01”为例的数据库实例。
- 确保RDS和ECS使用同一个安全组，以便用户正常访问数据库。
- 设置root用户对应的密码，并妥善管理您的密码，因为系统将无法获取您的密码信息。

步骤2 进入RDS console，在“实例管理”页面，单击实例名称“rds-01”，进入实例的“概览”页签。

步骤3 选择“数据库管理”页签，单击“创建数据库”，在弹出框中输入数据库名称，以“wordpress”为例，选择字符集并授权数据库账号，单击“确定”。

图 2-45 创建数据库

步骤4 选中“账号管理”页签，单击“创建账号”。在“创建账号”弹出框中，输入数据库账号，以“tony”为例，授权数据库选择**步骤3**中创建的“wordpress”数据库，并输入密码和确认密码，单击“确定”。

图 2-46 创建账号

----结束

安装 WordPress

步骤1 单击弹性云服务器实例列表“操作”列下的“远程登录”，远程登录弹性云服务器。

步骤2 在本地windows浏览器里输入地址：**http://***弹性IP地址*/**wordpress**，访问WordPress，单击“现在就开始！”。

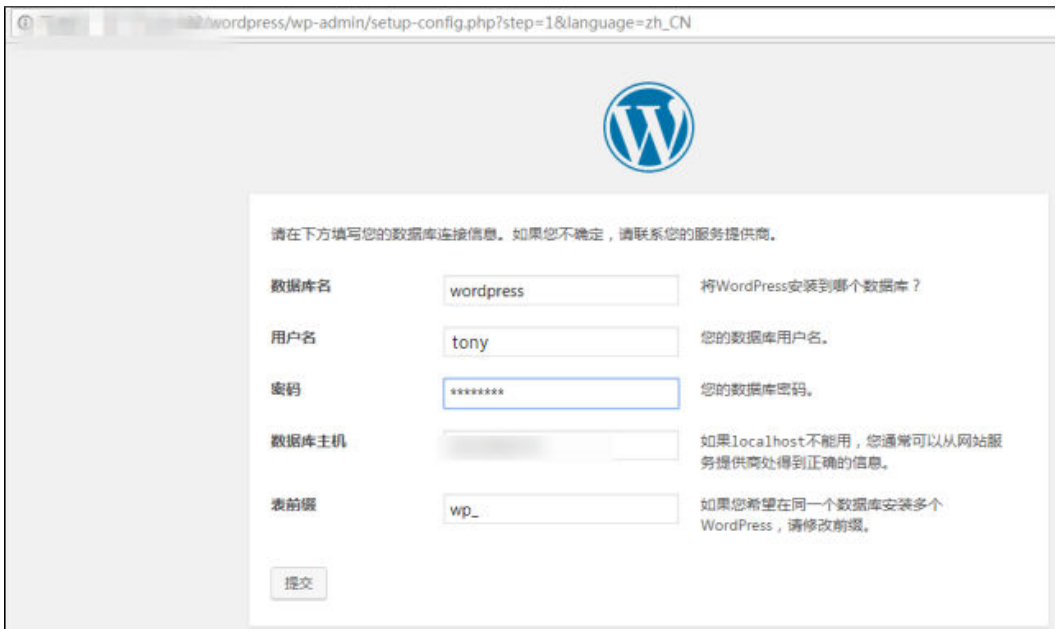
其中，*弹性IP地址*为**购买弹性云服务器**时所创建的弹性IP地址。

图 2-47 访问

步骤3 输入连接数据库的相关信息，单击“提交”。

- 数据库名为之前创建的“wordpress”数据库。
- 用户名为之前创建的“tony”数据库账号。
- 密码为创建“tony”账号时，您设置的密码。
- 数据库主机为数据库实例“rds-01”的内网IP。

图 2-48 输入连接信息



步骤4 数据库配置正确，通过验证后，单击“现在安装”。

图 2-49 数据库配置验证通过

步骤5 设置博客登录的“站点标题”、“用户名”和“密码”。

图 2-50 设置基本信息

步骤6 安装成功后，单击“登录”。

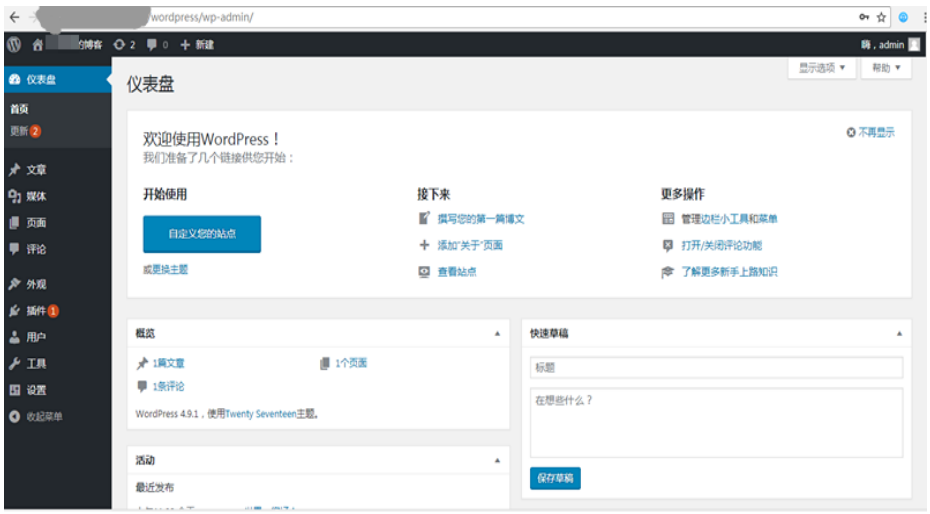
图 2-51 安装成功

步骤7 在登录页面，输入用户名和密码，单击“登录”。

图 2-52 登录

步骤8 您的WordPress搭建成功。

图 2-53 结果验证



----结束

2.5 使用 RDS for MySQL 搭建 Discuz!论坛

Crossday Discuz! Board（以下简称 Discuz!）是一套通用的社区论坛软件系统，用户可以通过简单的设置和安装，在互联网上搭建起具备完善功能、很强负载能力和可高

度定制的论坛服务。本文教您通过华为云虚拟私有云、弹性云服务器和RDS for MySQL数据库，轻松几步，在LAMP环境下搭建Discuz!。

1. **设置网络**
2. **创建ECS**
3. **搭建LAMP环境**
4. **购买并配置RDS**
5. **安装Discuz!**

准备工作

在搭建过程中，您会使用以下服务或工具：

- 云服务：华为云ECS和RDS。
- PuTTY：远程登录工具。
- 安装包版本。
  - Apache：2.4.6
  - MySQL：5.4.16
  - PHP：5.4.16

说明

以上软件来自第三方网站，仅作示例。若搭建的网站做商业用途，建议自行获取需要的版本软件，以应对不同需求。

设置网络

步骤1 登录**华为云控制台**。

步骤2 单击管理控制台左上角的，选择区域。

步骤3 选择“网络>虚拟私有云”。进入虚拟私有云信息页面。

步骤4 在“虚拟私有云”页面，单击“创建虚拟私有云”购买VPC，以vpc-01为例。

步骤5 在基本信息页面进行设置，自定义VPC及子网名称，根据实际需求选择可用分区等，IPv4网段选择“192.168”，其他均可以保持默认配置，单击“立即创建”提交任务。创建成功后，返回控制台页面。

步骤6 在“网络控制台”选择“访问控制 > 安全组”，单击“创建安全组”，以sg-01为例。

步骤7 在安全组界面，单击操作列的“配置规则”，进入安全组详情界面。

步骤8 单击“添加规则”，将ECS绑定的**弹性公网IP**添加到入方向规则。

----结束

购买弹性云服务器

步骤1 登录**华为云控制台**。

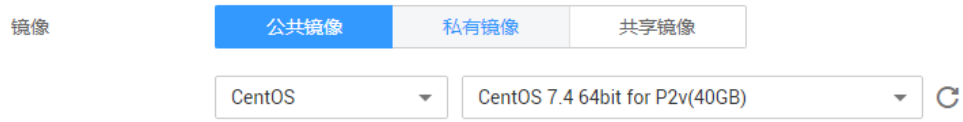
步骤2 单击管理控制台左上角的，选择区域。

步骤3 选择“计算 > 弹性云服务器”。进入弹性云服务器信息页面。

步骤4 在管理控制台购买ECS。

1. **完成基础配置：选择“按需计费”、“区域”和“镜像”，其他默认。**
   此处以公共镜像“CentOS7.4 64bit for P2v(40GB)”为例，如图2-54所示。

   图 2-54 选择镜像

2. **网络配置：选择VPC和安全组，购买弹性公网IP，其他默认。**
   a. 选择之前创建的虚拟私有云vpc-01。
   b. 选择之前步骤创建的安全组sg-01。
   c. 在“弹性公网IP”处选择“现在购买”。
3. **高级配置：设置ECS名称和密码，单击“下一步：确认订单”。**
   a. 云服务名称，以ecs-01为例。
   b. 设置密码。
4. **确认配置。确认无误，单击“立即购买”。**

步骤5 ECS创建成功后，您可通过华为云管理控制台，对其进行查看或管理。

----结束

搭建 LAMP 环境

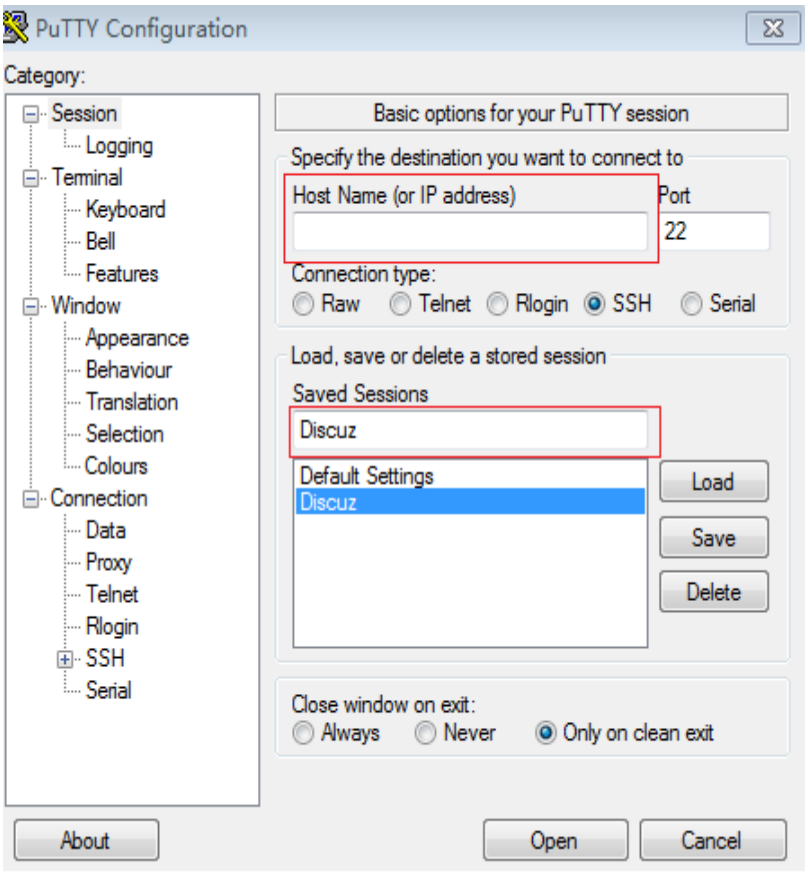
步骤1 下载PuTTY客户端。

步骤2 解压文件后，双击“putty”，显示配置界面。

步骤3 选择“Session”，配置相关信息后，如图2-55，单击“Open”。

1. 在“Host Name (or IP address)”输入ECS弹性IP地址，其他配置均保持默认值。
2. 在“Saved Sessions”中输入名称，此处以“Discuz”为例，单击“Save”，保存会话配置。

图 2-55 配置 PuTTY



步骤4 在登录界面中，输入ECS的用户名和密码，即可登录ECS。

步骤5 安装Apache、MySQL或PHP等软件。

通过PuTTY登录云服务器，直接获取root权限，可以直接在PuTTY内输入命令。

请输入软件安装命令，此处以PHP为例。

yum install -y httpd php php-fpm php-server php-mysql mysql

结果显示如下，表明安装完成。

```
Complete
```

步骤6 安装完成后，依次启动相关服务。

systemctl start httpd.service

systemctl start php-fpm.service

----结束

购买并配置 RDS

步骤1 请根据具体需求**购买华为云RDS for MySQL数据库实例**。

- 选择MySQL 5.7版本，创建以“rds-01”为例的数据库实例。
- 确保RDS和ECS使用同一个安全组，以便用户正常访问数据库。
- 设置root用户对应的密码，并妥善管理您的密码，因为系统将无法获取您的密码信息。

步骤2 云数据库RDS创建成功后，您可以登录**华为云管理控制台**，对其进行查看或管理。

----结束

安装 Discuz!

步骤1 下载**Discuz!软件**。

步骤2 使用数据传输工具将安装包上传到ECS。

1. 执行以下命令，解压Discuz!安装包。

   unzip Discuz_X3.3_SC_UTF8.zip

2. 执行以下命令，将解压后的“upload”中的所有文件，复制到“/var/www/html/”目录。

   cp -R upload/* /var/www/html/

3. 执行以下命令，将写入权限赋予给其他用户。

   chmod -R 777 /var/www/html

步骤3 在本地windows浏览器里输入地址：**http://***弹性IP地址***/install**，进入安装界面，按照Discuz!安装向导进行安装。

其中，*弹性IP地址*为**购买弹性云服务器**时所创建的弹性IP地址，“install”必须小写。

1. 确认协议，并单击“我同意”。
2. 开始安装后，检查安装环境并单击“下一步”。
3. 设置运行环境，并单击“下一步”。
4. 安装数据库，填写数据库信息，单击“下一步”完成安装。
   - 数据库服务器地址即为“rds-01”的私有IP地址。
   - 数据库密码是“rds-01”配置的数据库管理员root账号对应的密码。
   - 自定义管理员信息。

步骤4 Discuz!安装完成后，在浏览器中输入**http://***弹性IP地址***/forum.php**，可登录论坛主页，则说明网站搭建成功。

----结束

2.6 innodb_flush_log_at_trx_commit 和 sync_binlog 参数详解

“innodb_flush_log_at_trx_commit”和“sync_binlog”两个参数是控制RDS for MySQL磁盘写入策略以及数据安全性的关键参数。当两个参数为不同值时，在性能，安全角度下会产生不同的影响。

表 2-5 参数说明

参数名称	允许值	描述
innodb_flush_log_at_trx_commit	0, 1, 2	当重新安排并批量处理与提交相关的I/O操作时，可以控制磁盘的写入策略，严格遵守ACID合规性和高性能之间的平衡，该参数默认值为“1”，详情见**参数解析**。
sync_binlog	0～4,294,967,295	同步binlog（RDS for MySQL持久化到硬盘，或依赖于操作系统）。

参数解析

- **innodb_flush_log_at_trx_commit**：
  - 0：日志缓存区将每隔一秒写到日志文件中，并且将日志文件的数据刷新到磁盘上。该模式下在事务提交时不会主动触发写入磁盘的操作。
  - 1：每次事务提交时RDS for MySQL都会把日志缓存区的数据写入日志文件中，并且刷新到磁盘中，该模式为系统默认。
  - 2：每次事务提交时RDS for MySQL都会把日志缓存区的数据写入日志文件中，但是并不会同时刷新到磁盘上。该模式下，MySQL会每秒执行一次刷新磁盘操作。

    说明

    - 当设置为0，该模式速度最快，但不太安全，mysqld进程的崩溃会导致上一秒钟所有事务数据的丢失；
    - 当设置为1，该模式是最安全的，但也是最慢的一种方式。在mysqld服务崩溃或者服务器主机宕机的情况下，日志缓存区只有可能丢失最多一个语句或者一个事务；
    - 当设置为2，该模式速度较快，较取值为0情况下更安全，只有在操作系统崩溃或者系统断电的情况下，上一秒钟所有事务数据才可能丢失；

- **sync_binlog=1 or N**

  默认情况下，并不是每次写入时都将binlog日志文件与磁盘同步。因此如果操作系统或服务器崩溃，有可能binlog中最后的语句丢失。

  为了防止这种情况，你可以使用“sync_binlog”全局变量（1是最安全的值，但也是最慢的），使binlog在每N次binlog日志文件写入后与磁盘同步。

推荐配置组合

表 2-6 配置组合

innodb_flush_log_at_trx_commit	sync_binlog	描述
1	1	适合数据安全性要求非常高，而且磁盘写入能力足够支持业务。

innodb_flush_log_at_trx_commit	sync_binlog	描述
1	0	适合数据安全性要求高，磁盘写入能力支持业务不足，允许备库落后或无复制。
2	0/N(0<N<100)	适合数据安全性要求低，允许丢失一点事务日志，允许复制延迟。
0	0	磁盘写能力有限，无复制或允许复制延迟较长。

说明

- “innodb_flush_log_at_trx_commit”和“sync_binlog”两个参数设置为1的时候，安全性最高，写入性能最差。在mysqld服务崩溃或者服务器主机宕机的情况下，日志缓存区只有可能丢失最多一个语句或者一个事务。但是会导致频繁的磁盘写入操作，因此该模式也是最慢的一种方式。
- 当sync_binlog=N(N>1)，innodb_flush_log_at_trx_commit=2时，在当前模式下RDS for MySQL的写操作才能达到最高性能。

2.7 提高 RDS for MySQL 数据库查询速度的方法

可以参考如下建议：

- 如果产生了慢日志，可以通过查看慢日志来确定是否存在运行缓慢的SQL查询，以及各个查询的性能特征，从而定位查询运行缓慢的原因。查询RDS for MySQL日志，请参见**查看或下载慢日志**。
- 查看云数据库RDS实例的CPU使用率指标，协助定位问题。具体请参见**通过Cloud Eye监控**。
- 可以创建只读实例专门负责查询，减轻主实例负载，分担数据库压力。请参见**只读实例简介**。
- 创建只读实例后，您可以**开通读写分离**，通过RDS的读写分离连接地址，写请求自动访问主实例，读请求按照读权重设置自动访问各个实例。
- 如果是实例规格较小但负载过高，您可以提高CPU/内存规格，具体请参见**变更实例的CPU和内存规格**。也可以关闭会话临时降低负载，具体请参见**管理实时会话**。
- 多表关联查询时，关联字段要加上索引。
- 可以指定字段或者添加where条件进行查询，避免用select*语句进行全表扫描。

2.8 RDS for MySQL 长事务排查和处理

长事务有哪些潜在的影响?

1. 长事务会锁定资源，通常伴随着MDL锁、行锁指标的升高，导致其他事务无法访问这些资源，降低数据库的并发性能。

2. 长事务可能会占用大量的内存。
3. 长事务会导致日志文件增长，可能会导致日志文件过大，甚至导致磁盘打满。

排查长事务

- 连接实例查看长事务及其会话ID。

  连接实例后，通过以下命令查看执行时间超过3000秒的事务的事务ID、执行的SQL以及对应的会话ID。

  mysql> SELECT trx_id, trx_state, trx_started, trx_mysql_thread_id, trx_query, trx_rows_modified FROM information_schema.innodb_trx WHERE TIME_TO_SEC(timediff(now(),trx_started)) >3000;

  表 2-7 字段说明

字段名	说明
trx_id	事务ID。
trx_state	事务状态。包括RUNNING、LOCK WAIT、ROLLING BACK等。
trx_started	事务开始时间。
trx_mysql_thread_id	该事务所属的MySQL会话ID。
trx_query	事务执行的SQL语句。
trx_rows_modified	事务修改的行数。

- 通过查看监控指标确认存在长事务。

  a. **登录管理控制台**。

  b. 单击页面左上角的☰，选择“数据库 > 云数据库 RDS”，进入RDS信息页面。

  c. 在“实例管理”页面，选择目标实例，单击操作列中的“查看监控指标”，进入监控指标概览页。

  d. 查看“长事务指标”（指标ID：rds_long_transaction），当该指标呈线性上升且时间较大时说明存在长事务。

kill 长事务

1. 获取长事务对应的线程ID。

   通过执行**•连接实例查看长事务及其会话ID。**中的SQL语句，获取执行时间超过某一时间（例如：3000秒）的事务对应的会话ID。

   mysql> SELECT trx_mysql_thread_id FROM information_schema.innodb_trx WHERE TIME_TO_SEC(timediff(now(),trx_started)) >3000;

2. 获取到会话ID后，通过**kill**命令结束对应的事务。

   mysql> kill *trx_mysql_thread_id*

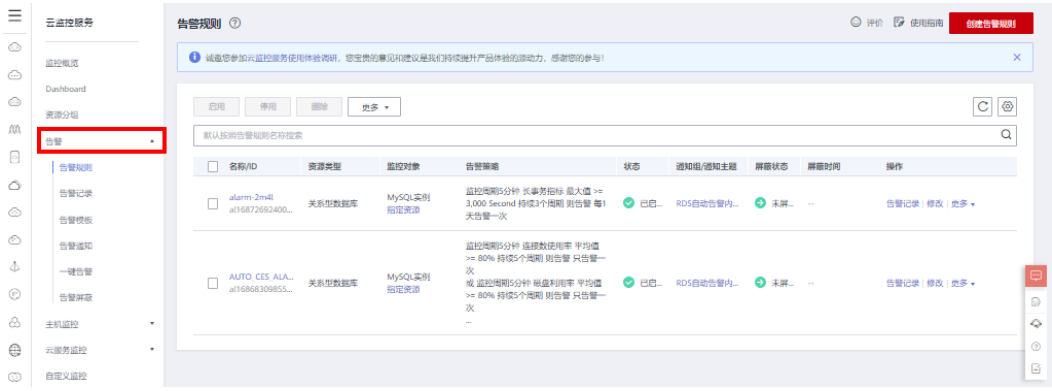
须知

kill长事务会导致事务回滚，请评估业务影响后执行。

设置长事务告警

1. 查看已设置的告警。
   a. 登录管理控制台。
   b. 单击页面左上角的☰，选择“管理与监管 > 云监控服务 CES”，进入CES信息页面。
   c. 选择“告警 > 告警规则”，查看已设置的告警。

图 2-56 查看告警规则

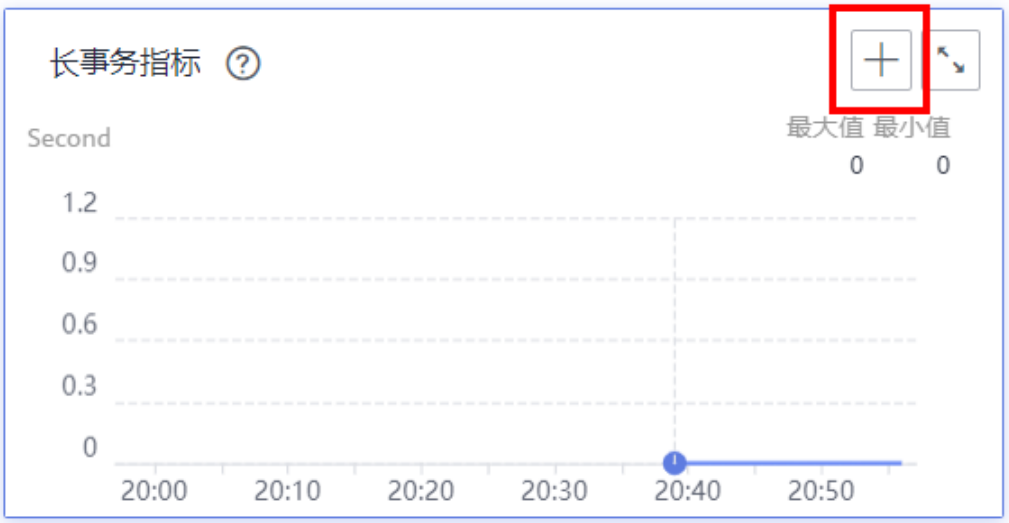


2. 设置长事务告警。
   a. 单击页面左上角的☰，选择“数据库 > 云数据库 RDS”，进入RDS信息页面。
   b. 在“实例管理”页面，选择目标实例，单击操作列中的“查看监控指标”，进入监控指标概览页。
   c. 查看“长事务指标”。

图 2-57 查看监控指标

   d. 单击“长事务指标”右上角的“+”，创建告警规则。

图 2-58 长事务指标



e. 在“创建告警规则”界面，填选相关信息。具体参数说明请参见**创建告警规则和通知**。

2.9 RDS for MySQL 设置循环执行事件

当您需要在RDS for MySQL中执行定时任务或周期性任务，例如定时同步数据、定期清理过期数据、或周期性插入数据等任务，您可以开启事件定时器，结合数据管理服务DAS的循环执行事件功能，根据预定计划自动执行数据库中定义的事件。本文介绍如何使用DAS服务为RDS for MySQL设置循环执行事件。

约束限制

- RDS for MySQL内核5.6.43.2、5.7.25.2和8.0.17.4及其以上版本可以开启事件定时器。若您的数据库版本不在该范围内但想使用该功能，请**升级内核小版本**。
- 只读实例不支持开启事件定时器。

步骤 1：开启事件定时器

步骤1 **登录管理控制台**。

步骤2 单击管理控制台左上角的，选择区域。

步骤3 单击页面左上角的，选择“数据库 > 云数据库 RDS”，进入RDS信息页面。

步骤4 在“实例管理”页面，单击主实例名称。

步骤5 在“概览”页面，在“事件定时器”处，单击“开启”。

----结束

步骤 2：设置循环执行事件

步骤1 在“实例管理”页面，选择目标实例，单击操作列的“登录”，进入数据管理服务实例登录界面。

图 2-59 登录实例

步骤2 输入root用户名和对应的密码，单击“登录”。

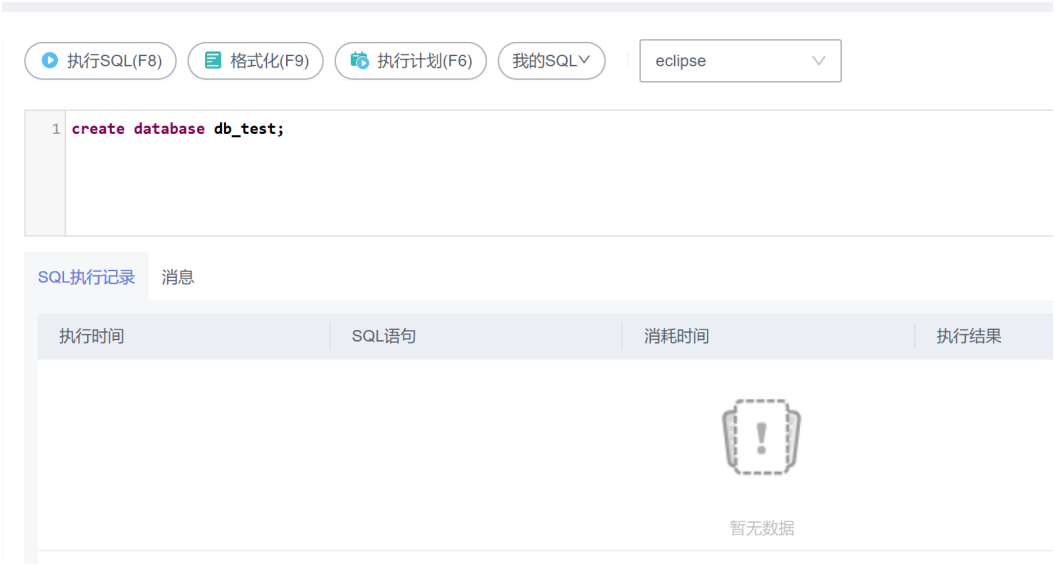
图 2-60 登录界面

步骤3 选择“SQL操作 > SQL查询”。

步骤4 在SQL窗口，创建数据库**db_test**。

```
create database db_test;
```

图 2-61 创建库



步骤5 在**db_test**库下，创建表**t_test**。

```
create table t_test(id int(4), name char(20), age int(4));
```

图 2-62 创建表

步骤6 在首页，单击数据库名称，进入对象列表。

图 2-63 首页

步骤7 在对象列表，选择“事件”，单击“新建事件”。

图 2-64 对象列表

步骤8 填写事件信息后，单击“立即创建”。

图 2-65 新建事件

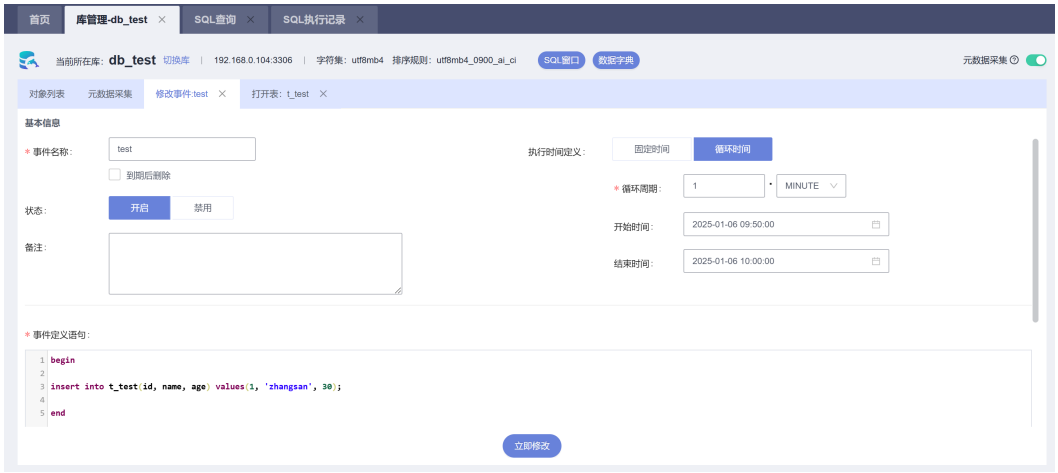


表 2-8 事件说明

参数	描述
事件名称	自定义事件名称。
到期后删除	• 不勾选，事件任务一直保留。 • 勾选后，事件任务到期后删除。 – 对于固定时间执行的事件，执行一次即删除。 – 对于循环时间执行的事件，将在设置的执行结束时间点删除。
状态	执行事件时，选择“开启”。
备注	事件任务的备注。

参数	描述
执行时间定义	• 固定时间 在指定的时间执行一次事件任务。 • 循环时间 在开始和结束时间范围内，每隔一个循环周期执行一次事件任务。 例如：在09:50~10:00之间，每隔1分钟执行一次事件。

事件定义语句	事件定时触发时执行的操作语句。
	例如：在表**t_test**中插入一条数据。
	begin
	insert into t_test(id, name, age) values(1, 'zhangsan', 30);
	end

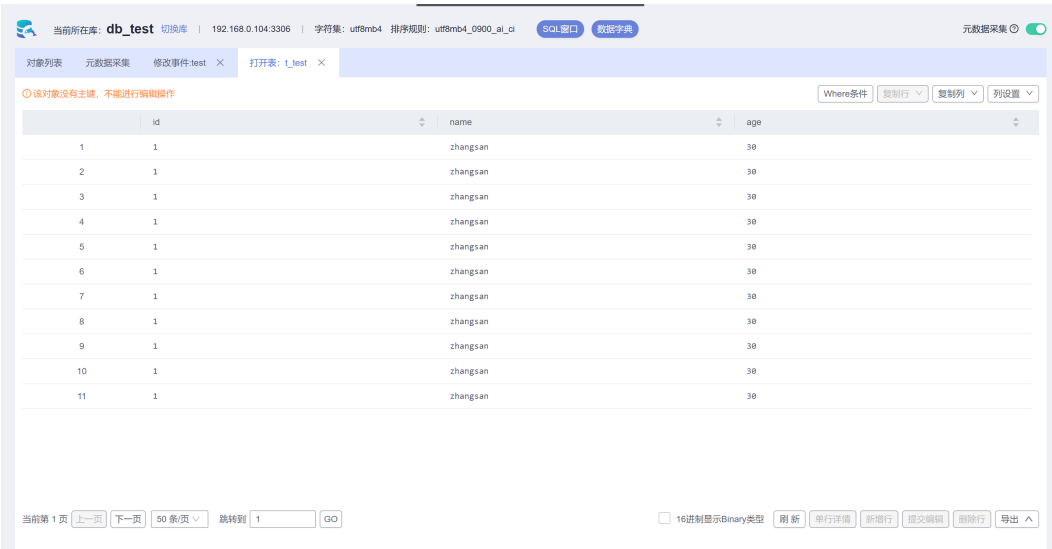
步骤9 在弹出框，单击“执行脚本”，将在设置的时间执行事件任务。

步骤10 在对象列表，选择“表”，单击“打开表”。

图 2-66 打开表

步骤11 查看循环事件执行结果。

图 2-67 查看执行结果



----结束

2.10 RDS for MySQL 安全最佳实践

安全性是华为云与您的共同责任。华为云负责云服务自身的安全，提供安全的云；作为租户，您需要合理使用云服务提供的安全能力对数据进行保护，安全地使用云。详情请参见**责任共担**。

本文提供了RDS for MySQL使用过程中的安全最佳实践，旨在为提高整体安全能力提供可操作的规范性指导。根据该指导文档您可以持续评估RDS for MySQL的安全状态，更好的组合使用RDS for MySQL提供的多种安全能力，提高对RDS for MySQL的整体安全防御能力，保护存储在RDS for MySQL的数据不泄露、不被篡改，以及数据传输过程中不泄露、不被篡改。

本文从以下几个维度给出建议，您可以评估RDS for MySQL使用情况，并根据业务需要在本指导的基础上进行安全配置。

- **完善数据库连接相关配置，减少被网络攻击的风险**
- **妥善进行数据库账号密码管理，减少数据泄露风险**
- **加强权限管理，减少相关风险**
- **开启数据库审计，便于事后回溯**
- **开启备份功能，完善备份相关配置，保障数据可靠性**
- **加密存储数据**
- **加固数据库敏感参数**
- **使用最新版本数据库获得更好的操作体验和更强的安全能力**
- **使用其他云服务进一步增强对数据的安全防护**

完善数据库连接相关配置，减少被网络攻击的风险

1. **建议避免绑定EIP直接通过互联网访问RDS for MySQL**

   避免RDS for MySQL部署在互联网或者DMZ里，应该将RDS for MySQL部署在公司内部网络，使用路由器或者防火墙技术把RDS for MySQL保护起来，避免直接绑定EIP方式从互联网访问RDS for MySQL。通过这种方式防止未授权的访问及DDos攻击等。建议**解绑弹性公网IP外部连接**，如果您的业务必须绑定EIP，请务必通过设置安全组规则限制访问数据库的源IP。

2. **避免使用默认端口号**

   MySQL的默认端口号为3306，此端口会更容易受到恶意人员的攻击。建议您为数据库实例**修改数据库端口**。

3. **确保限制数据库用户的可用资源**

   如果不限定数据库用户的可用资源，数据库在受到攻击时，可能会出现系统过载，导致服务DOS。限定数据库用户的可用资源，防止资源过度占用导致的资源过度消耗。您需要结合业务模型给出合理值，避免在高负载场景下影响业务可用性。

   配置SQL语句如下：

   ```
   alter user  '<user>'@'<hostname>' with max_queries_per_hour <queries_num>;
   alter user  '<user>'@'<hostname>' with max_user_connections <connections_num>;
   alter user  '<user>'@'<hostname>' with max_updates_per_hour <updates_num>;
   alter user  '<user>'@'<hostname>' with max_connections_per_hour
   <connections_per_hour>;
   ```

- <user>表示需要做资源设置的用户名。
- <hostname>表示需要做资源设置的用户hostname。
- <queries_num>表示设置的数据库允许用户的每小时最大查询数。
- <connections_num>表示设置的数据库允许用户的最大连接数。
- <updates_num>表示设置的数据库允许用户的每小时最大更新数。
- <connections_per_hour>表示设置的数据库允许用户的每小时最大连接数。

4. **确保用户主机名不使用通配符“%”**

   MySQL用户主机名指定用户可用于连接的主机，对应user表中的host字段。主机名设置为通配符“%”时，标识用户接受来自任何IP的连接，从而导致扩大数据库的攻击范围。为了减小受攻击范围，建议您**修改主机IP**为特定网段或具体IP。

5. **确保限制数据库连接闲置等待时间**

   MySQL服务器的每个连接建立都会消耗内存，且所支持的最大连接数也有上限，如果MySQL Server有大量的闲置连接，不仅会白白消耗内存，而且如果连接一直累加而不断开，最终会达到MySQL Server的连接上限数，新建连接就会报“too many connections”错误。所以应该设置闲置连接的等待时间，确保及时清除闲置连接。请参考**修改实例参数**修改“wait_timeout”和“interactive_timeout”，具体值需您根据业务自行审视。

6. **确保默认开启SSL**

   如未配置SSL加密通信，那么在MySQL客户端和服务器之间传输的数据，容易受到窃听、篡改和“中间人”攻击。为了提高数据传输的安全性，建议您为数据库用户添加REQUIRE SSL属性，同时**设置SSL数据加密**。

   配置SQL语句如下：

   ```
   create user '<user>'@'<hostname>' REQUIRE SSL;
   alter user '<user>'@'<hostname>' REQUIRE SSL;
   ```

妥善进行数据库账号密码管理，减少数据泄露风险

1. **建议定期修改管理员用户的密码**

   默认的数据库管理员账号root拥有较高的权限，建议您参考**重置管理员密码和root账号权限**定期修改root密码。

2. **设置密码复杂度**

   数据库系统作为信息的聚集体，易成为攻击者的目标。用户需要妥善保存数据账号与密码，避免泄漏。同时建议您配置数据库密码的复杂度，避免使用弱密码。详情请参见**数据库安全设置**中的“设置密码复杂度”。

3. **设置密码过期策略**

   长期使用同一个密码会增加被暴力破解和恶意猜测的风险。建议您**设置密码过期策略**限制使用同一个密码的时间。

加强权限管理，减少相关风险

1. **禁止以管理员用户创建存储过程和函数**

   存储过程和函数默认以创建者的身份运行，如果管理员用户创建的存储过程和函数存在提权或其他破坏操作，那么普通用户可以提权至管理员的身份运行，因此要避免使用管理员用户创建存储过程和函数。

2. **审视并加固权限相关配置**

   请用户审视如下权限配置是否符合安全要求，如有出入您需要自行完成配置加固：

- 确保mysql.user表只有管理员用户才能操作。
- 确保Process_priv权限只能赋予管理员用户。
- 确保Create_user_priv权限只能赋予管理员用户。
- 确保Grant_priv权限只能管理员管理员用户。
- 确保Reload_priv权限只能赋予管理员用户。
- 确保复制账号有且只能有replication slave权限。
- 确保数据库指标监控用户有且只能有replication client权限。

示例：如有非管理员用户拥有Process权限，请执行如下SQL取消Process权限。

```
revoke process on *.* from <your_account>;
```

其中，<your_account>表示需取消Process权限的用户名。

开启数据库审计，便于事后回溯

数据库审计功能可以实时记录用户对数据库的所有相关操作。通过对用户访问数据库行为的记录、分析和汇报，用来帮助您事后生成合规报告、事故追根溯源，提高数据资产安全性。详情请参见**开启SQL审计日志**。

开启备份功能，完善备份相关配置，保障数据可靠性

1. **开启数据备份**

   RDS for MySQL实例支持自动备份和手动备份，您可以定期对数据库进行备份，当数据库故障或数据损坏时，可以通过备份文件恢复数据库，从而保证数据可靠性。详情请参见**数据备份**。

2. **配置MySQL binlog日志清理策略**

   Binlog日志会随着业务的运行而持续膨胀，需要配置清零策略避免磁盘膨胀。请您参考**设置RDS for MySQL本地Binlog日志清理**设置Binlog保存时间。

加密存储数据

为提升用户数据的安全性，建议开启**服务端加密**，开启后您创建实例和扩容磁盘时，磁盘数据会在服务端加密成密文后存储，降低数据泄露的风险。

加固数据库敏感参数

1. **建议“local_infile”参数配置为OFF**

   “local_infile”设置为ON时，将允许数据库客户端通过load data local语法将客户端本地文件加载到数据库表中。例如，在web服务器作为数据库客户端连接数据库的场景，如果web服务器存在SQL注入漏洞，那么攻击者可用构造load data local命令将web服务器的敏感文件加载到数据库中，从而造成信息泄露。建议您参考**修改实例参数**配置“local_infile”的值为OFF。

2. **建议“sql_mode”参数包含“STRICT_ALL_TABLES”**

   攻击者在试图攻击时会试错性输入各种参数，若服务器自适应错误语句，将有可能泄漏数据库数据。因此推荐使用“STRICT_ALL_TABLES”，即使错误出现在首行后的其他行，一旦发现非法数据值就会放弃语句。这种用法能最大限度的保证数据库信息不被泄露。建议您参考**修改实例参数**配置“sql_mode”参数包含“STRICT_ALL_TABLES”。

使用最新版本数据库获得更好的操作体验和更强的安全能力

MySQL社区不定期披露新发现的漏洞，RDS for MySQL会评估数据库内核版本的实际风险，发布新的数据库内核版本。为了提升数据库系统的易用性和安全性，建议您**使用最新版本数据库**。

使用其他云服务进一步增强对数据的安全防护

如果您希望获得更智能的数据库安全服务，建议**使用数据安全服务DBSS**来扩展数据安全能力。

3 RDS for PostgreSQL

3.1 RDS for PostgreSQL 搭建跨区域容灾关系

3.1.1 方案概述

场景描述

当生产机发生损坏或因其他不可抗力造成业务系统宕机的情况下，异地跨区域容灾实例可以保证生产系统的数据不丢失，保持生产系统的业务不间断地运行，从而提高系统的可用性。

本实践主要包含以下内容：

- 介绍如何创建RDS for PostgreSQL实例。
- 介绍如何搭建RDS for PostgreSQL实例跨区域容灾。

前提条件

- 拥有华为云实名认证账号。
- 账户余额大于等于0美元。

约束条件

- 主实例和灾备实例状态正常，主实例和灾备实例在不同云或不同区域上，且主实例为主备实例，灾备实例为单机实例。
- 主实例配置容灾能力成功后才能配置灾备实例容灾能力，否则容灾关系会建立失败。
- 灾备实例的规格要大于等于主实例的规格。
- RDS for PostgreSQL 12及以上支持建立跨云或跨区域容灾关系。
- 不支持跨大版本建立跨云或跨区域容灾关系。
- 主实例和灾备实例的容灾关系已建立完成，才能进行灾备实例升主和查询容灾复制状态。
- 实施前确认需要搭建的主实例和灾备实例所在区域，处于云连接/虚拟专有网络服务已上线区域内。

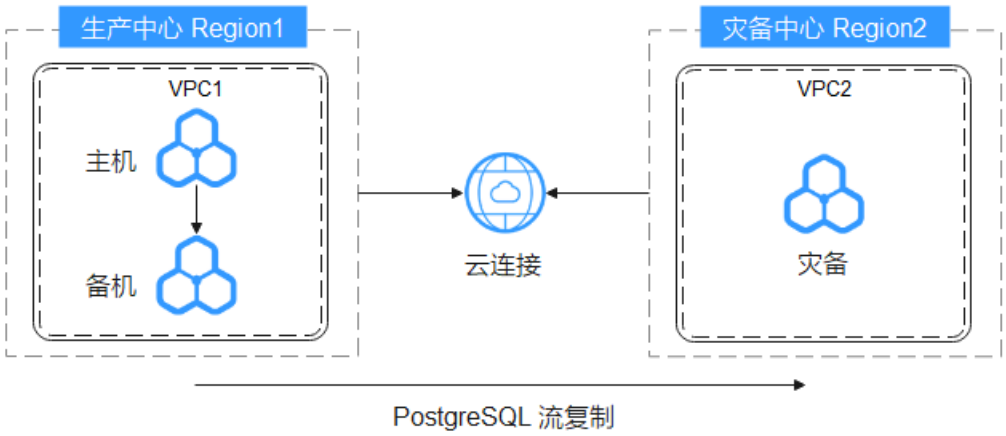
- 灾备实例不支持PITR恢复和CBR快照备份功能，如需使用此功能，请在主实例上完成。

实现原理

RDS for PostgreSQL跨区域容灾实现原理说明：

在两个数据中心独立部署RDS for PostgreSQL实例，通过RDS接口将生产中心RDS for PostgreSQL库中的数据同步到灾备中心RDS for PostgreSQL库中，实现RDS for PostgreSQL主实例和跨区域灾备实例之间的实时同步。使用该功能前，必须需要确认可以使用云连接服务完成跨区域网络连通。

图 3-1 原理图



服务列表

- 云连接 CC
- 虚拟私有云 VPC
- 云数据库 RDS

使用说明

- 本实践的资源规划仅作为演示，实际业务场景资源以用户实际需求为准。
- 本实践端到端的数据为测试数据，仅供参考。

3.1.2 资源规划

表 3-1 资源规划

类别	子类	规划	备注
生产中心VPC	VPC名称	vpc-pg-01	自定义，易理解可识别。
	所属Region	中国-香港	选择和自己业务区最近的Region，减少网络时延。
	可用区	可用区一	-

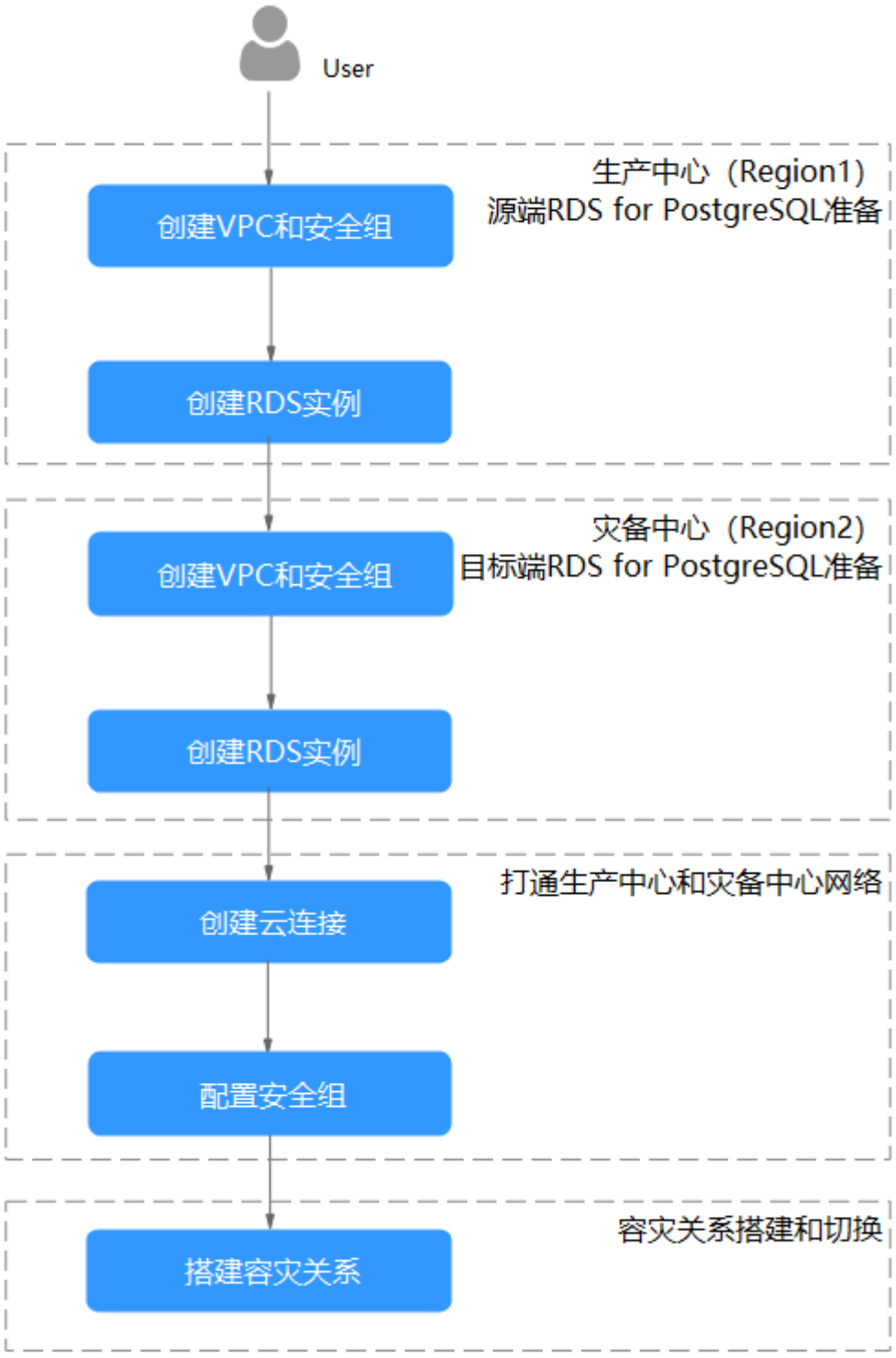
类别	子类	规划	备注
	子网网段	192.168.10.0/24	子网选择时建议预留足够的网络资源。
	子网名称	subnet-2aa1	自定义，易理解可识别。
灾备中心VPC	VPC名称	vpc-pg-02	自定义，易理解可识别。
	所属Region	亚太-新加坡	选择和自己业务区最近的Region，减少网络时延。
	可用区	可用区一	-
	子网网段	192.168.20.0/24	子网选择时建议预留足够的网络资源。
	子网名称	subnet-a388	自定义，易理解可识别。
生产中心RDS for PostgreSQL实例	RDS实例名称/ID	rds-pg-01 04**in03	自定义，易理解可识别。
	所属Region	中国-香港	选择和自己业务区最近的Region，减少网络时延。
	数据库版本	PostgreSQL 12	-
	内网IP	192.168.10.117	-
	实例类型	主备	生产中心实例为主备。
	存储类型	SSD云盘	-
	可用区	可用区一、可用区三	-
	性能规格	独享型 2 vCPUs | 4GB	-
	磁盘容量	40 GB	-
灾备中心RDS for PostgreSQL实例	RDS实例名称/ID	rds-pg-02 5f**in03	自定义，易理解可识别。
	所属Region	亚太-新加坡	选择和自己业务区最近的Region，减少网络时延。
	数据库版本	PostgreSQL 12	-
	内网IP	192.168.20.69	-
	实例类型	单机	灾备中心实例为单机。
	存储类型	SSD云盘	-
	可用区	可用区一	-

类别	子类	规划	备注
	性能规格	独享型 8 vCPUs | 16GB	灾备中心实例的CPU和内存规格要大于或等于主实例的规格。
	磁盘容量	100 GB	灾备中心实例的磁盘容量要大于或等于主实例的磁盘容量。

3.1.3 操作流程

创建RDS for PostgreSQL业务实例以及灾备实例，并且将业务实例数据迁移到灾备实例的整个流程的主要任务流如下图所示。

图 3-2 流程图



3.1.4 生产中心 RDS for PostgreSQL 实例准备

本章节介绍在生产中心创建RDS for PostgreSQL实例所属VPC和安全组，然后创建RDS for PostgreSQL业务实例。

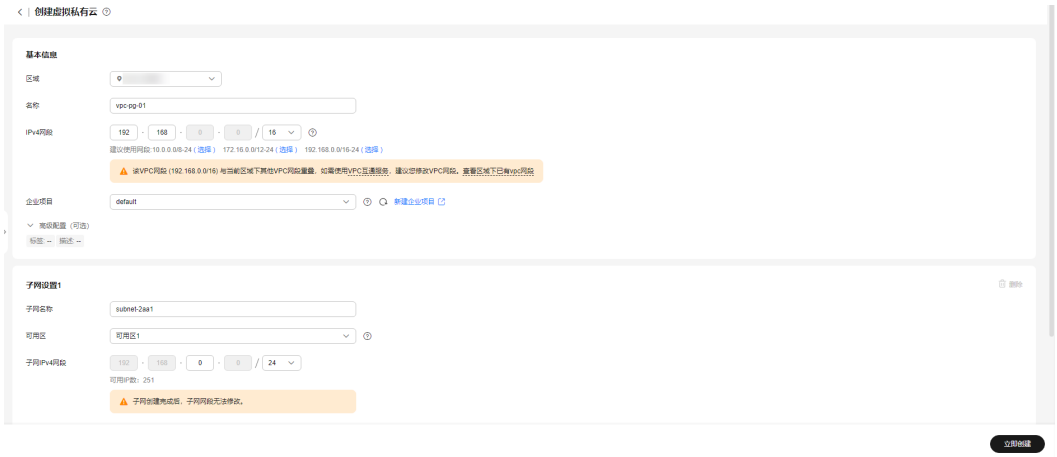
- 步骤1：创建VPC和安全组
- 步骤2：创建RDS for PostgreSQL实例

步骤 1：创建 VPC 和安全组

步骤1 进入创建虚拟私有云页面。

步骤2 在“创建虚拟私有云”页面，根据页面完成基本信息、子网配置和地址配置。选择区域“中国-香港”。

图 3-3 创建 VPC

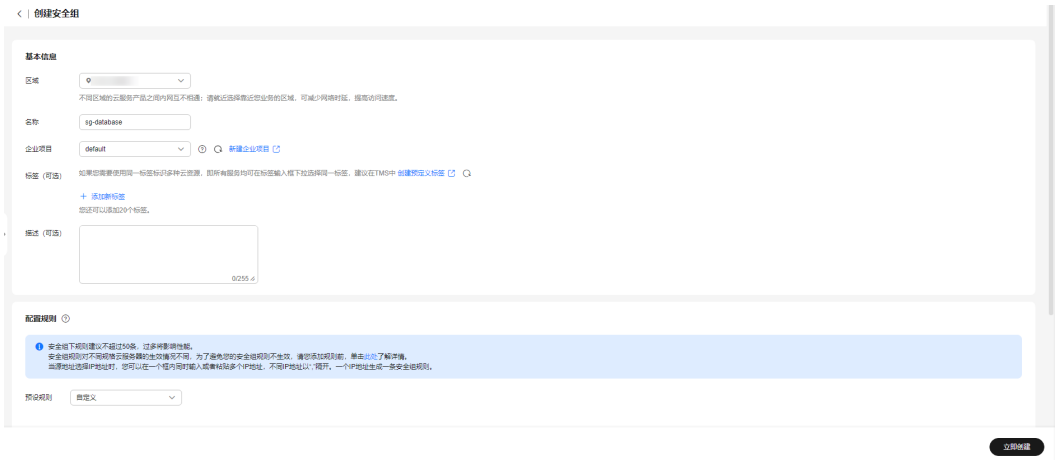


步骤3 单击“立即创建”，完成生产VPC创建。

步骤4 在网络控制台左侧导航树，选择“访问控制 > 安全组”。

步骤5 单击“创建安全组”。

图 3-4 创建安全组



步骤6 单击“立即创建”，完成生产安全组创建。

----结束

步骤 2：创建 RDS for PostgreSQL 实例

步骤1 进入**购买云数据库RDS页面**。

步骤2 选择区域“中国-香港”。填选实例信息后，单击“立即购买”。

图 3-5 选择引擎版本信息

图 3-6 选择规格信息

图 3-7 选择已规划的网络信息

图 3-8 设置管理员密码

步骤3 进行规格确认。

- 如果需要重新选择实例规格，单击“上一步”，回到上个页面修改实例信息。
- 如果规格确认无误，单击“提交”，完成购买实例的申请。

----结束

3.1.5 灾备中心 RDS for PostgreSQL 实例准备

本章节介绍在灾备中心创建RDS for PostgreSQL实例所属VPC和安全组，然后创建RDS for PostgreSQL业务实例。

须知

- 灾备中心实例的VPC子网网段需与生产中心VPC子网网段不同，这是实现跨区域网络连接的前提。
- 生产中心和灾备中心的安全组需要相互放通实例所属VPC子网网段的数据库端口。

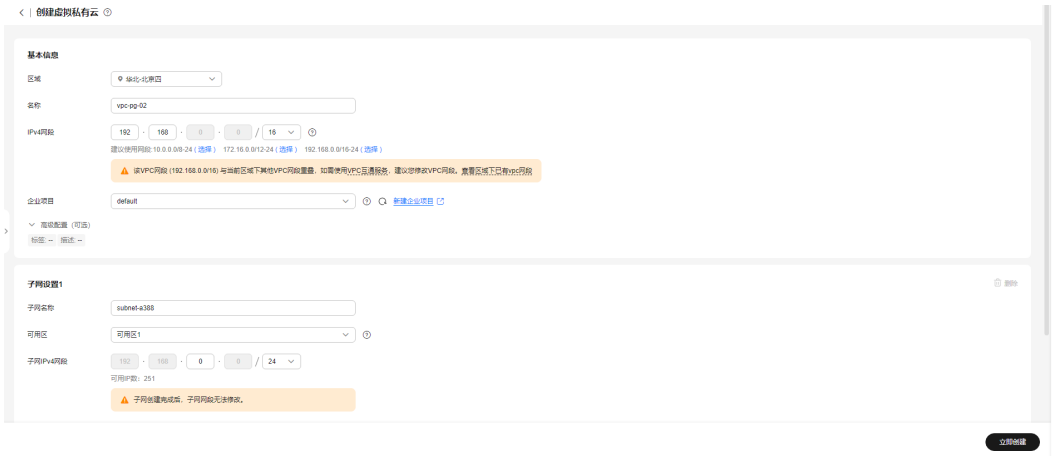
- 步骤1：创建VPC和安全组
- 步骤2：创建RDS for PostgreSQL实例

步骤 1：创建 VPC 和安全组

步骤1 进入创建虚拟私有云页面。

步骤2 在“创建虚拟私有云”页面，根据页面完成基本信息、子网配置和地址配置。选择区域“亚太-新加坡”。

图 3-9 创建 VPC



步骤3 单击“立即创建”，完成生产VPC创建。

步骤4 在网络控制台左侧导航树，选择“访问控制 > 安全组”。

步骤5 单击“创建安全组”。

图 3-10 创建安全组

步骤6 单击“立即创建”，完成生产安全组创建。

----结束

步骤 2：创建 RDS for PostgreSQL 实例

步骤1 进入**购买云数据库RDS页面**。

步骤2 选择区域“亚太-新加坡”。填选实例信息后，单击“立即购买”。

图 3-11 选择引擎版本信息

图 3-12 选择规格信息

图 3-13 选择已规划的网络信息

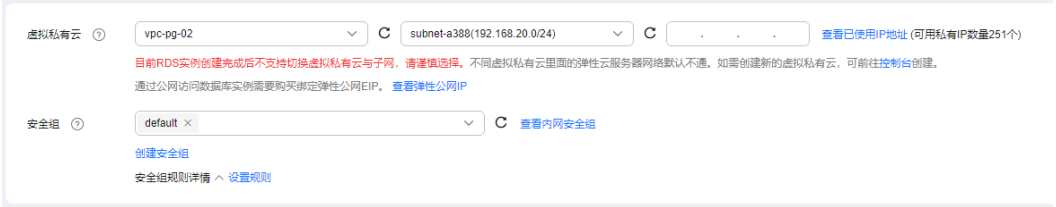


图 3-14 设置管理员密码

步骤3 进行规格确认。

- 如果需要重新选择实例规格，单击“上一步”，回到上个页面修改实例信息。
- 如果规格确认无误，单击“提交”，完成购买实例的申请。

----结束

3.1.6 配置跨区域网络互通

搭建异地容灾实例，首先需要完成跨区域网络的连通。当前提供**方式一：通过云连接配置跨区域VPC互通**和**方式二：通过虚拟专用网络配置跨区域VPC互通**两种方式实现跨区域网络连通。

在选择带宽大小时，建议根据事务日志生成速率监控指标进行选择，大于等于该指标最高值的10倍即可，因为网络带宽单位为Mbit/s，而事务日志生成速率监控指标的单位为MB/s。

例如事务日志生成速率监控指标最高值为10MB/s，则网络带宽建议选择100Mbit/s，以便于灾备节点有足够的带宽可以及时同步主节点的数据。

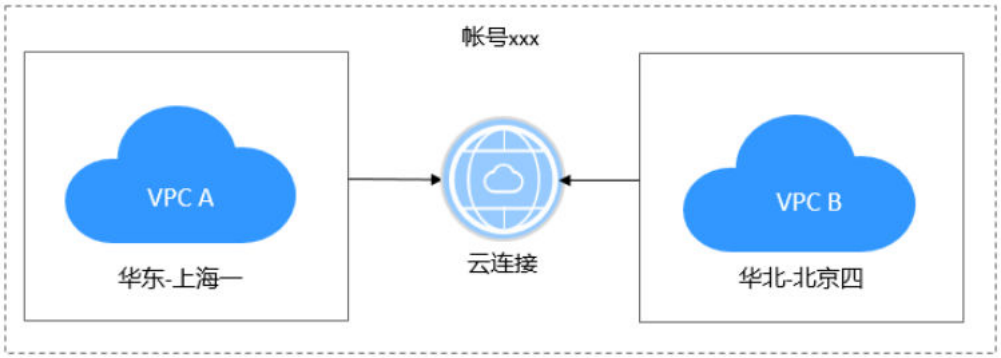
在网络打通后，需要配置主实例和容灾实例互相放通安全组，详见**配置安全组**。

方式一：通过云连接配置跨区域 VPC 互通

搭建异地容灾实例，首先需要完成跨区域网络的连通。

可以使用**云连接 CC**产品完成跨区域VPC网络连通。

图 3-15 跨区域同账号互通



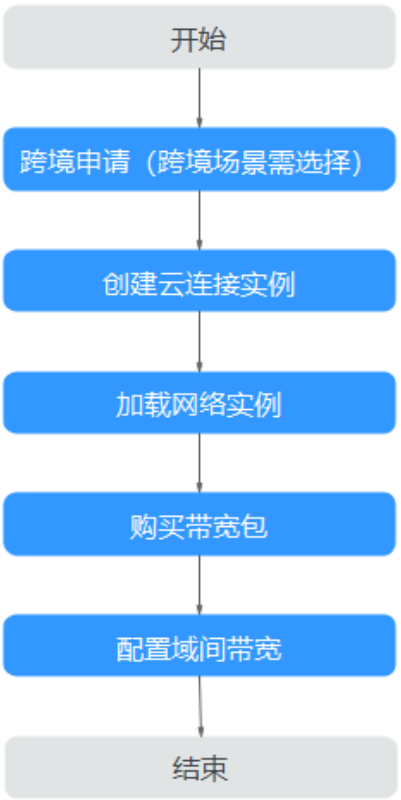
须知

配置前请确认搭建的主实例和灾备实例在云连接**已上线区域清单**列表上。

配置云连接两端需放通主实例和灾备实例所属VPC子网的网段，仅放通单个数据库IP会搭建失败。

跨区域VPC网络连通具体操作步骤可以按照**跨区域同账号VPC互通**进行配置。

图 3-16 云连接流程图



方式二：通过虚拟专用网络配置跨区域 VPC 互通

可以使用**虚拟专用网络 VPN**服务完成跨区域VPC网络连通。

须知

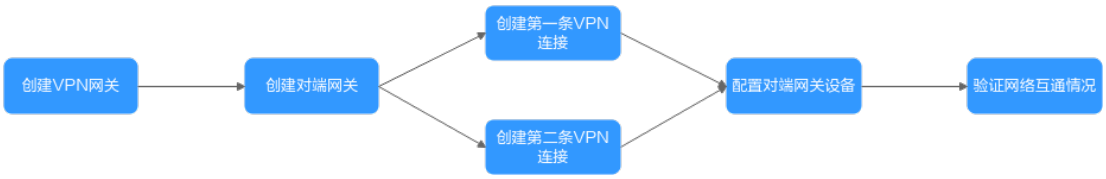
配置前请确认搭建的主实例和灾备实例在虚拟专用网络**功能支持区域**列表上。

当前在使用虚拟专用网络连通时，需要在配置完VPN服务后，联系VPN服务客服，进行网络配置调配，才能使用。

配置跨VPC两端需放通主实例和灾备实例所属VPC子网的网段，仅放通单个数据库IP会搭建失败。

虚拟专用网络的具体操作步骤可以参考**虚拟专用网络入门指引**进行配置。

图 3-17 操作流程



配置安全组

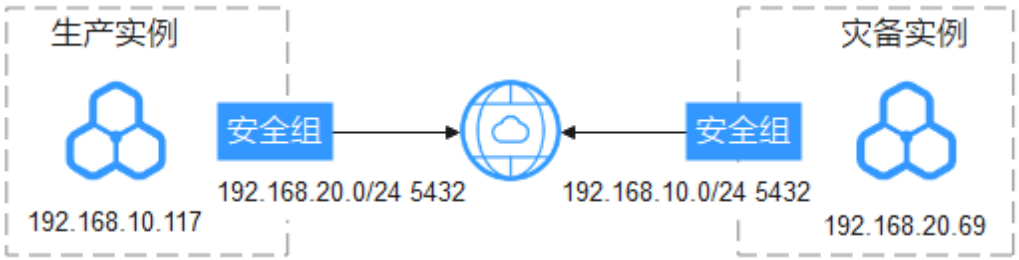
完成跨区域VPC互通后，还需要配置主实例和灾备实例的安全组，使得VPC网段间的端口互通。

假设存在**表3-2**所示的实例配置，其数据库端口都为默认值5432。则生产实例和灾备实例的的防火墙配置如**图3-18**所示。

表 3-2 实例网段

类别	VPC网段	IP地址
生产实例	192.168.10.0/24	192.168.10.117
灾备实例	192.168.20.0/24	192.168.20.69

图 3-18 防火墙配置



3.1.7 搭建容灾关系

操作场景

建立跨区域容灾关系后，当主实例所在区域发生突发性自然灾害等状况，主节点无法连接，可将异地灾备实例升为主实例，在应用端修改数据库连接地址后，即可快速恢复应用的业务访问。

注意事项

- 使用该功能前，必须要确保跨区域数据库实例之间的网络打通，可以使用**云连接CC**或**虚拟专用网络 VPN**产品完成跨区域VPC网络连通。
- 使用该功能前，确保主实例和灾备实例状态正常，主实例和灾备实例在不同区域上，且主实例为主备实例，灾备实例为单机实例。
- 灾备实例的CPU和内存规格以及磁盘容量要大于或等于主实例的规格以及磁盘容量。
- RDS for PostgreSQL 12及以上支持建立跨区域容灾关系。
- 修改主实例的端口或内网地址后需要重新搭建灾备关系。

操作步骤

步骤1 配置生产实例容灾能力，即将灾备实例的配置信息复制到生产实例上。

1. **登录管理控制台**。
2. 单击管理控制台左上角的，选择灾备实例所在的区域，例如“亚太-新加坡”。
3. 单击页面左上角的，选择“数据库>云数据库 RDS”，进入RDS信息页面。
4. 在“实例管理”页面，单击灾备实例的实例名称进入“概览”页面。
5. 单击“灾备配置信息”。
6. 在弹框中，单击“一键复制”。

图 3-19 复制灾备实例配置信息

7. 单击管理控制台左上角的，选择生产实例所在的区域，例如“中国-香港”。
8. 在“实例管理”页面，选择生产实例，单击“操作”列的“更多 > 查看容灾详情”，进入“容灾管理”页面。
9. 单击“搭建容灾”，在弹框中，将**步骤1.6**中复制的灾备配置信息粘贴至输入框中，单击“确定”，开始配置生产实例容灾能力。

图 3-20 粘贴灾备实例信息

10. 在生产实例的“容灾管理”页面查看搭建情况。当“搭建状态” 显示为“已搭建”，则表示配置生产实例容灾能力成功。确保此步骤搭建成功后再进行后续操作。

图 3-21 查看搭建容灾成功

步骤2 配置灾备实例容灾能力，即将生产实例的配置信息复制到灾备实例上。

1. 在“实例管理”页面，单击生产实例的实例名称进入“概览”页面。
2. 单击“灾备配置信息”。
3. 在弹框中，单击“一键复制”。
4. 单击管理控制台左上角的，选择灾备实例所在的区域，例如“亚太-新加坡”。
5. 在“实例管理”页面，选择灾备实例，单击“操作”列的“更多 > 查看容灾详情”，进入“容灾管理”页面。
6. 单击“搭建容灾”，在弹框中，将**步骤2.3**中复制的灾备配置信息粘贴至输入框中，单击“确定”，开始配置灾备实例容灾能力。
7. 在“容灾管理”页面查看搭建情况。当“搭建状态” 显示为“已搭建”，则表示配置灾备实例容灾能力成功，至此，容灾搭建成功。

8. 在“容灾管理”页面可以查看灾备复制状态、发送延迟大小、端到端延迟大小和回放延迟时间。

----结束

3.1.8 灾备升主

操作场景

当主实例所在区域发生突发性自然灾害等状况，主节点无法连接，可将异地灾备实例升为主实例，在应用端修改数据库连接地址后，即可快速恢复应用的业务访问。

注意事项

灾备升主后的新主实例和原主实例将会解除灾备关系。

操作步骤

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角的，选择灾备实例所在的区域，例如“亚太-新加坡”。

步骤3 单击页面左上角的，选择“数据库>云数据库 RDS”，进入RDS信息页面。

步骤4 单击灾备实例名称，进入实例的概览页面。

步骤5 在左侧导航栏，选择“容灾管理”。

步骤6 在容灾关系列表单击“操作”列的“灾备升主”。

步骤7 在弹框中，单击“确认”，开始下发灾备升主任务。

步骤8 可在“任务中心”中查看任务的执行结果，当任务状态为完成时，表示灾备升主任务成功。

步骤9 需用户在应用端修改数据库连接地址，手动将业务切换到新主实例。

----结束

3.1.9 解除灾备

操作场景

当不需要容灾关系时，可以将搭建好的容灾关系解除。

注意事项

当前只支持解除搭建成功的容灾关系，并且需要先解除灾备实例的容灾关系，再解除主实例的容灾关系，否则可能会引起异常告警。

操作步骤

步骤1 登录管理控制台。

步骤2 首先解除灾备实例的容灾关系。

1. 进入主实例的概览页面，单击“灾备配置信息”。
2. 在弹框中，单击“一键复制”。
3. 单击灾备实例名称，进入实例的概览页面。
4. 在左侧导航栏，选择“容灾管理”。
5. 在容灾关系列表单击“操作”列的“解除容灾关系”。
6. 将刚复制的灾备配置信息粘贴进弹框中。
7. 可在“容灾管理”中查看任务的执行结果，当列表被删除时，则执行成功。

步骤3 然后解除主实例的容灾关系，步骤参考**步骤2**，复制灾备实例的“灾备配置信息”，然后在主实例的“容灾管理”页面解除。

----结束

3.1.10 常见问题

- 问题1：配置灾备实例容灾能力时，任务执行失败。

  排查生产中心和灾备中心的安全组是否互相放通数据库VPC子网网段的端口。如果使用VPN连接，确认是否按照**方式二：通过虚拟专用网络配置跨区域VPC互通**的注意事项配置。

- 问题2：使用云连接配置VPC时，系统提示“当前VPC存在路由冲突，此VPC路由已存在”。

  参考**加载网络实例时出现系统异常怎么办**进行排查处理。

3.2 RDS for PostgreSQL 发布与订阅

逻辑定义

发布可以被定义在任何物理复制的主服务器上。定义有发布的节点被称为发布者。发布是从一个表或者一组表生成的改变的集合，也可以被描述为更改集合或者复制集合。每个发布都只存在于一个数据库中。

订阅是逻辑复制的下游端。订阅被定义在其中的节点被称为订阅者。一个订阅会定义到另一个数据库的连接以及它想要订阅的发布集合（一个或者多个）。逻辑订阅者的行为与一个普通的PostgreSQL实例（主库）无异，逻辑订阅者也可以创建自己的发布，拥有自己的订阅者。

使用权限

- 创建发布时，发布者必须有流复制权限。即replication权限。
- 创建发布时，使用all tables发布所有表时，需确保发布者是**提权起始及之后版本**的root用户。
- 创建/删除订阅时，需确保订阅者是**提权起始及之后版本**的root用户。
- 创建发布/订阅时，需确保发布端和订阅端实例在同一VPC下。

各个版本root用户提权情况参见**root用户权限说明**。

发布使用限制

- 发布目前只能包含表（即：索引，序列号，物化视图这些不会被发布），每个表可以添加到多个发布中。
- 一个publication允许有多个订阅者。
- 允许使用all tables发布所有表。
- 在同一个数据库中，可以创建多个publication，但是不能重名。已创建的publication可以通过查询pg_publication获取。
- 发布可以筛选所需的变更类型：包括insert、update、delete 和truncate的任意组合，类似触发器事件，默认所有变更都会被发布。

  例如：发布表t1的**update**和**delete**操作。

  ```
  CREATE PUBLICATION update_delete_only FOR TABLE t1
    WITH (publish = 'update, delete') ;
  ```

- 复制标识：当发布了表的**update**, **delete**时，表必须设置复制标识（Replica Identity），如果设置了nothing，则执行**update**, **delete**时会报错。

  表上的复制标识可以通过查阅pg_class.relreplident获取。

  这是一个字符类型的“枚举”，标识用于组装 “复制标识” 的列：d = default，f = 所有的列，i 使用特定的索引，n 没有复制标识。

  表上是否具有可用作复制标识的索引约束，可以通过以下查询获取：

  ```
  SELECT quote_ident(nspname) || '.' || quote_ident(relname) AS name, con.ri AS keys,
        CASE relreplident WHEN 'd' THEN 'default' WHEN 'n' THEN 'nothing' WHEN 'f' THEN
  'full' WHEN 'i' THEN 'index' END AS replica_identity
  FROM pg_class c JOIN pg_namespace n ON c.relnamespace = n.oid, LATERAL (SELECT
  array_agg(contype) AS ri FROM pg_constraint WHERE conrelid = c.oid) con
  WHERE relkind = 'r' AND nspname NOT IN ('pg_catalog', 'information_schema', 'monitor',
  'repack', 'pg_toast')
  ORDER BY 2,3;
  ```

- 复制标识配置

  表到复制标识可以通过**ALTER TABLE**进行修改。

  ```
  ALTER TABLE table_name REPLICA IDENTITY
  { DEFAULT | USING INDEX index_name | FULL | NOTHING };
  -- 具体有四种形式
  ALTER TABLE t_normal REPLICA IDENTITY DEFAULT;                    -- 使用主键，如果没有主键则为FULL
  ALTER TABLE t_normal REPLICA IDENTITY FULL;                       -- 使用整行作为标识
  ALTER TABLE t_normal REPLICA IDENTITY USING INDEX t_normal_v_key; -- 使用唯一索引
  ALTER TABLE t_normal REPLICA IDENTITY NOTHING;                    -- 不设置复制标识
  ```

- 复制标识在实际使用中的注意事项
  - 表上有主键，使用默认的default复制标识。
  - 表上没有主键，但是有非空唯一索引，显式配置index复制标识。
  - 表上既没有主键，也没有非空唯一索引，显式配置full复制标识（运行效率非常低，仅能作为兜底方案）。
  - 其他所有情况，都无法正常完成逻辑复制功能。输出的信息不足，可能会报错。
  - 特别需要注意：如果nothing复制标识的表纳入到逻辑复制中，对其进行删改会导致发布端报错。

订阅使用限制

- 为了确保使用Failover Slot，必须在发布端手工创建逻辑复制槽(Failover Slot)，并通过**create_slot = false**关联已有复制槽，如下：

  CREATE SUBSCRIPTION sub1 CONNECTION 'host=192.168.0.1 port=5432 user=user1 dbname=db1' PUBLICATION pub_name with (create_slot = false,slot_name = FailoverSlot_name);
- 逻辑复制不会复制DDL变更，因此发布集中的表必须已经存在于订阅端上。
- 同一个数据库中，可以创建多个subscription，这些subscription可以来自一个或多个发布者。
- 订阅者的同一张表，不能接受来自同一个源的多个发布。
- 在创建subscription或者alter subscription时，可以使用enable来启用该订阅，或者使用disable暂停该订阅。
- 如果要完全删除订阅，使用**DROP SUBSCRIPTION**，注意，删除订阅后，本地的表不会被删除，数据也不会清除，仅仅是不再接收该订阅的上游信息。

须知

如果订阅与复制槽相关联，就不能在事务块内部执行**DROP SUBSCRIPTION**。可以使用**ALTER SUBSCRIPTION**取消关联复制槽。

删除订阅可参考以下步骤：

a. 在订阅端查询订阅关联的的复制槽。

   select subname,subconninfo,subslotname from pg_subscription where subname = 'sub2';

   - subname为订阅者名称。
   - subconninfo为连接远程主机信息。
   - subslotname 为远程主机复制槽名称。

b. 在订阅端执行**ALTER SUBSCRIPTION**取消关联复制槽并删除。

   ALTER SUBSCRIPTION subname SET (slot_name = NONE);

   DROP SUBSCRIPTION subname;

c. 在发布端删除关联的复制槽。

   select pg_drop_replication_slot(' slot_name);

语法参考

- 发布

  CREATE PUBLICATION用于创建发布，**DROP PUBLICATION**用于移除发布，**ALTER PUBLICATION**用于修改发布。

  发布创建之后，可以通过**ALTER PUBLICATION**动态地向发布中添加或移除表，这些操作都是事务性的。
- 订阅

  CREATE SUBSCRIPTION用于创建订阅，**DROP SUBSCRIPTION**用于移除订阅，**ALTER SUBSCRIPTION**用于修改订阅。

订阅创建之后，可以通过**ALTER SUBSCRIPTION**随时**暂停**与**恢复**订阅。移除并重建订阅会导致**同步信息丢失**，这意味着相关数据需要重新进行同步。

具体使用说明请参考以下官方文档，以PostgreSQL 13版本为例：

- 创建发布：**https://www.postgresql.org/docs/13/sql-createpublication.html**
- 删除发布：**https://www.postgresql.org/docs/13/sql-droppublication.html**
- 修改发布：**https://www.postgresql.org/docs/13/sql-alterpublication.html**

3.3 RDS for PostgreSQL 自定义数据类型转换

简介

PostgreSQL数据类型有三种转换方式：隐式转换，赋值转换，显式转换。对应的转换类型在系统表“pg_cast”中分别对应：i（Implicit）、a（Assignment）、e（Explicit）。

- 隐式转换（Implicit）：同一类型间，低字节到高字节为隐式转换，比如int到bigint。
- 赋值转换（Assignment）：同一类型间，高字节到低字节为赋值转换，比如smallint到int。
- 显式转换（Explicit）：不同类型间，称为显示转换。

基本使用

1. 在进行数据类型转换前，可以通过如下命令查看RDS for PostgreSQL是否已经支持数据类型转换。

```
select * from pg_catalog.pg_cast ;
oid  | castsource | casttarget | castfunc | castcontext | castmethod
-------+------------+------------+----------+-------------+------------
 11277 |         20 |         21 |      714 | a           | f
 11278 |         20 |         23 |      480 | a           | f
 11279 |         20 |        700 |      652 | i           | f
 11280 |         20 |        701 |      482 | i           | f
.....
```

2. 通过如下命令查询**int4**是否支持转换**text**。

```
select * from pg_catalog.pg_cast where castsource = 'int4'::regtype and casttarget = 'bool'::regtype;
  oid  | castsource | casttarget | castfunc | castcontext | castmethod
-------+------------+------------+----------+-------------+------------
 11311 |         23 |         16 |     2557 | e           | f
(1 row)
```

此时查出结果是默认支持的，转换类型是隐式转换。

如果没有内置的转换函数，需要自定义转换函数来支持这种转换，具体参考**自定义类型转换**。

自定义类型转换

- 通过双冒号方式进行强制转换

```
select '10'::int,'2023-10-05'::date;
 int4 |    date
------+------------
   10 | 2023-10-05
(1 row)
```

- 通过类型转换函数**CAST**进行转换

```
select CAST('10' as int),CAST('2023-10-05' as date);
 int4 |    date
------+------------
   10 | 2023-10-05
(1 row)
```

- 自定义类型转换

  具体语法及使用可查看：**https://www.postgresql.org/docs/14/sql-createcast.html**

  须知

  由于新增自定义类型转换会影响RDS for PostgreSQL已有的执行计划，一般不建议自定义类型转换。

  - 时间与字符类型的转换

    CREATE CAST(varchar as date) WITH INOUT AS IMPLICIT;
  - boolean类型与数值类型转换

    create cast(boolean as numeric) with INOUT AS IMPLICIT;
  - 数值类型与字符类型转换

    create cast(varchar as numeric) with INOUT AS IMPLICIT;

  示例：将**text**转换为**date**

```
create or replace function public.text_to_date(text) returns date as
$$
  select to_date($1,'yyyy-mm-dd');
$$
language sql strict;

create cast (text as date) with function public.text_to_date(text) as implicit;

select text '2023-09-09' + 1;
  ?column?
------------
 2023-09-10
(1 row)
```

3.4 使用客户端驱动程序实现故障转移和读写分离

从PostgreSQL 10（libpq.so.5.10）开始，libpq驱动层开始支持故障转移和读写分离，JDBC驱动层则支持读写分离、故障转移和负载均衡。

PostgreSQL客户端连接程序向下兼容，对于RDS for PostgreSQL 9.5及9.6版本，使用新版本的libpq驱动程序也可以实现故障转移。

说明

本章节中故障转移指的是读业务的故障转移。

- libpq是PostgreSQL的C应用程序接口，包含一组库函数，允许客户端程序将查询请求发送给PostgreSQL后端服务器并接收这些查询的结果。
- JDBC是Java语言中用来规范客户端程序如何访问数据库的应用程序接口，在PostgreSQL中JDBC支持故障转移和负载均衡。

表 3-3 libpq 和 JDBC 驱动支持的功能

驱动	读写分离	负载均衡	故障转移
libpq驱动	√	×	√
JDBC驱动	√	√	√

libpq 实现故障转移和读写分离

通过libpq函数连接多个数据库，当出现故障时会自动切换到可用的数据库。

postgresql://[user[:password]@][netloc][:port][,...][/dbname][?param1=value1&...]

示例：连接1个RDS for PostgreSQL主实例数据库和对应的2个只读实例数据库，只要确保至少有一个数据库可用，读请求就不会失败。

postgres://
<instance_ip>:*<instance_port>*,*<instance_ip>*:*<instance_port>*,*<instance_ip>*:*<instance_port>*/*<database_name>*?**target_session_attrs=any**

表 3-4 参数说明

参数	说明	取值样例
<instance_ip>	数据库的主机IP。	如果通过内网连接，“instance_ip”是主机IP，即“概览”页面该实例的“内网地址”。 如果通过连接了公网的设备访问，“instance_ip”为该实例已绑定的“弹性公网IP”。
<instance_port>	数据库端口。	默认5432，当前端口，参考“概览”页面该实例的“数据库端口”。
<database_name>	数据库名，即需要连接的数据库名。	默认的管理数据库是postgres，可根据业务实际情况填写数据库名。

参数	说明	取值样例
target_session_attrs	允许连接到指定状态的数据库。	• any：默认值，表示允许连接到任意数据库，会连接到第一个允许连接的数据库，如果连接的数据库出现故障导致连接断开，会尝试连接其他数据库，从而实现故障转移。 • read-write：只会连接到支持读写的数据库，即从第一个数据库开始尝试连接，如果连接后发现不支持读写，则会断开连接，然后尝试连接第二个数据库，以此类推，直至连接到支持读写的数据库。 • read-only：只会连接只读数据库，即从第一个数据库开始尝试连接，如果连接后发现支持读写，则会断开连接，然后尝试连接第二个数据库，以此类推，直至连接到只读的数据库。RDS for PostgreSQL 13（libpq.so.5.13）及以下版本，不支持该取值。

更多libpq的使用方法和参数说明请参见**Connection Strings**。

您还可以在应用程序中结合pg_is_in_recovery()函数，判断连接的数据库是主实例数据库（结果为“f”表示主数据库）还是只读实例数据库，进而实现读写分离。

使用Python代码的示例如下（psycopg2使用的为libpq）：

```
// 认证用的用户名和密码直接写到代码中有很大的安全风险，建议在配置文件或者环境变量中存放(密码应密文存放，使用时解密)，确保安全。
// 本示例以用户名和密码保存在环境变量中为例，运行本示例前请先在本地环境中设置环境变量(环境变量名称请根据自身情况进行设置)EXAMPLE_USERNAME_ENV和EXAMPLE_PASSWORD_ENV。

import psycopg2
import os

username = os.getenv("EXAMPLE_USERNAME_ENV")
password = os.getenv("EXAMPLE_PASSWORD_ENV")
conn = psycopg2.connect(database=<database_name>,host=<instance_ip>, user=username,
password=password, port=<instance_port>, target_session_attrs="read-write")
cur = conn.cursor()
cur.execute("select pg_is_in_recovery()")
row = cur.fetchone()
print("recovery =", row[0])
```

JDBC 实现故障转移和读写分离

您可以在连接URL中定义多个数据库（主机和端口），并用逗号分隔，驱动程序将尝试按顺序连接到它们中的每一个，直到连接成功。如果没有成功，会返回连接异常报错。

jdbc:postgresql://node1,node2,node3/${database}?targetServerType=preferSecondary&loadBalanceHosts=true

示例：

jdbc:postgresql://*<instance_ip>*:*<instance_port>*,*<instance_ip>*:*<instance_port>*,*<instance_ip>*:*<instance_port>*/*<database_name>*?**targetServerType=preferSecondary&loadBalanceHosts=true**

JDBC连接实例java实现代码请参考：**通过JDBC连接RDS for PostgreSQL实例**。

表 3-5 参数说明

参数	说明	取值样例
targetServerType	允许连接到指定状态的数据库。	• any：任何数据库。 • primary：主数据库（可写可读）。JDBC 42.2.0以下版本请使用参数值“master”。 • secondary：从数据库（可读）。JDBC 42.2.0以下版本请使用参数值“slave”。 • preferSecondary：优先从数据库，如果没有从数据库才连接到主数据库。JDBC 42.2.0以下版本请使用参数值“preferSlave”。
loadBalanceHosts	尝试连接数据库的顺序。	• False：默认值，按URL中的定义顺序连接数据库。 • True：随机连接数据库。

说明

区别数据库主从的方式是通过查询数据库是否允许写入，允许写入数据的判断为主数据库，不允许写入数据的判断为从数据库。参考**libpq实现故障转移和读写分离**中通过pg_is_in_recovery()函数来判断，结果为“f”表示为主数据库。

为实现读写分离，需要在配置JDBC时设置2个数据源，首先设置targetServerType=primary，用于写操作。另一个可以根据以下情况进行设置：

- 有一个只读实例，为实现高可用设置targetServerType=preferSecondary，用于读操作。假设主实例IP为10.1.1.1，只读实例IP为10.1.1.2。

  jdbc:postgresql://10.1.1.2:5432,10.1.1.1:5432/${database}?targetServerType=preferSecondary

- 有两个以上只读实例，可设置targetServerType=any，用于读操作。假设只读实例IP分别为10.1.1.2、10.1.1.3。

  jdbc:postgresql://10.1.1.2:5432,10.1.1.3:5432/${database}?targetServerType=any&loadBalanceHosts=true

3.5 PoWA 插件使用最佳实践

3.5.1 插件介绍

PoWA是一套开源的用于对RDS for PostgreSQL数据库进行性能监控的系统。它由PoWA-archivist、PoWA-collector、PoWA-web三个部件组成工作系统，并通过安装于RDS for PostgreSQL数据库中的其他插件获取性能数据。重要组成如下所示：

- PoWA-archivist：作为PostgreSQL的一个插件，用于收集其他插件获取到的性能数据。
- PoWA-collector：是通过部署于远程服务器上的专用于存储库收集目标PostgreSQL数据库性能指标的守护进程。

- PoWA-web：通过Web图形用户界面展示PoWA-collector收集到的性能指标。
- 其他插件：性能指标数据的实际来源，安装于目标PostgreSQL数据库实例上。
- PoWA：整个系统的总称。

安全风险提醒

PoWA在进行部署配置中，会存在以下几个安全风险点：

- （远程模式时）在powa-repository中配置采集性能指标实例信息时，需要输入目标实例的IP、root用户账号、连接密码，并且可以通过powa_servers表查询到相关信息，其中连接密码以明文形式呈现，存在安全风险。
- 在PoWA-collector配置文件中，powa-repository的连接信息中无连接密码配置，表示powa-repository对于PoWA-collector的连接配置项必须为trust，存在安全风险。
- 在PoWA-web配置文件中，可选配置username、password对应powa-repository（远程模式）或者数据库实例（本地模式）的root用户及连接密码，且以明文形式存储，存在安全风险。

在使用PoWA插件时，请悉知以上安全风险。可以参考**PoWA官方手册**进行安全加固。

其他扩展插件

除了pg_stat_statements、btree_gist、powa为必须的插件，PoWA还支持以下几个插件作为性能指标采集的扩展：

- pg_qualstats
- pg_stat_kcache
- pg_wait_sampling
- pg_track_settings
- hypopg

每个插件都可以扩展不同的对应的性能指标。当前RDS for PostgreSQL支持的插件，请参见**支持的插件列表**。

3.5.2 支持的性能指标

3.5.2.1 数据库级性能指标

General Overview

图 3-22 General Overview

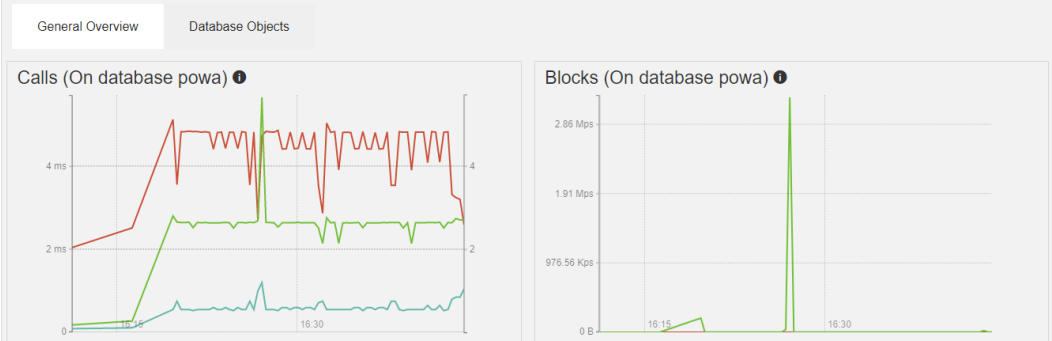


表 3-6 Calls 字段解释

字段	说明
Queries per sec	每秒执行查询的次数。
Runtime per sec	每秒内执行查询的总耗时。
Avg runtime	查询的平均耗时。

表 3-7 Blocks 字段解释

字段	说明
Total shared buffers hit	命中共享缓冲区的数据量。
Total shared buffers miss	未命中共享缓冲区的数据量。

Database Objects

图 3-23 Database Objects

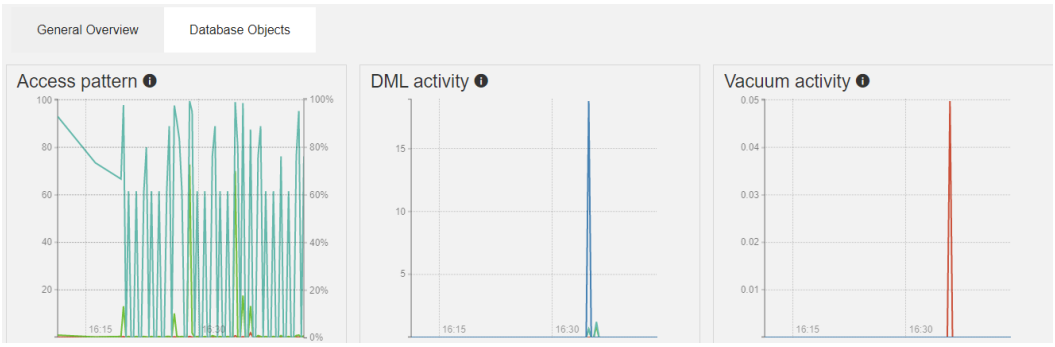


表 3-8 Access pattern 字段解释

字段	说明
Index scans ratio	索引扫描/序列扫描的比率。
Index scans	每秒索引扫描次数。
Sequential scans	每秒顺序扫描次数。

表 3-9 DML activity 字段解释

字段	说明
Tuples inserted	每秒插入的行数。
Tuples updated	每秒更新的行数。

字段	说明
Tuples HOT updated	每秒更新(HOT)的行数。
Tuples deleted	每秒删除的行数。

表 3-10 Vacuum activity 字段解释

字段	说明
# Vacuum	每秒手动清理的次数。
# Autovacuum	每秒自动清理的次数。
# Analyze	每秒手动分析的次数。
# Autoanalyze	每秒自动分析的次数。

Details for all databases

图 3-24 Details for all databases

表 3-11 Details for all databases 字段解释

字段	注释
Query	执行的SQL。
(Execution) #	执行该SQL次数。
(Execution) Time	执行该SQL总时间。
(Execution) Avg time	执行该SQL平均时间。
(I/O Time) Read	读I/O等待时间。
(I/O Time) Write	写I/O等待时间。
(Blocks) Read	磁盘读页面数。

字段	注释
(Blocks) Hit	共享缓冲区命中页面数。
(Blocks) Dirtied	脏页面数。
(Blocks) Written	磁盘写页面数。
(Temp blocks) Read	磁盘读临时页面数。
(Temp blocks) Write	磁盘写临时页面数。

3.5.2.2 实例级性能指标

General Overview

图 3-25 General Overview 性能指标

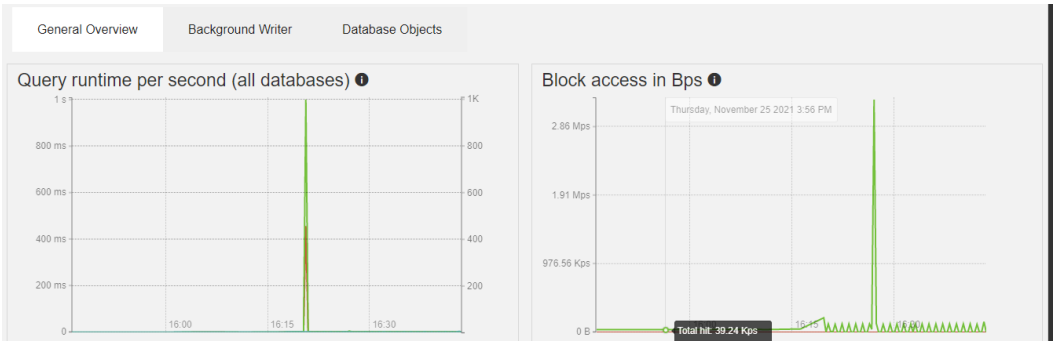


表 3-12 Query runtime per second (all databases)字段解释

字段	说明
Queries per sec	每秒执行查询的次数。
Runtime per sec	每秒执行的查询的总持续时间。
Avg runtime	平均查询时长。

表 3-13 Block access in Bps 字段解释

字段	说明
Total hit	在共享缓冲区中找到的数据量。
Total read	在操作系统缓存中找到或从磁盘读取的数据量。

Background Writer

图 3-26 Background Writer 性能指标

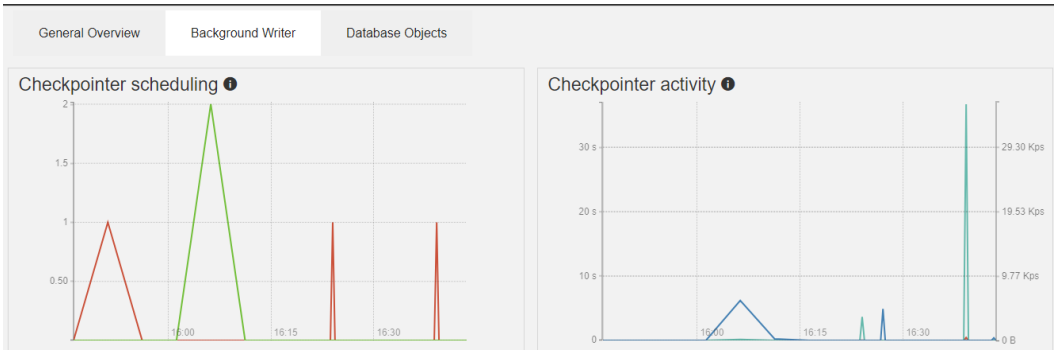


表 3-14 Checkpointer scheduling 字段解释

字段	说明
of requested checkpoints	已执行的请求检查点数。
of scheduled checkpoints	已执行的预定检查点数。

表 3-15 Checkpointer activity 字段解释

字段	说明
Buffers alloc	分配的缓冲区数。
Sync time	文件同步到磁盘的检查点处理部分所花费的总时间（单位：毫秒）。
Write time	在将文件写入磁盘的检查点处理部分中花费的总时间（单位：毫秒）。

表 3-16 Background writer 字段解释

字段	说明
Maxwritten clean	后台编写器因写入过多缓冲区而停止清理扫描的次数。
Buffers clean	后台写入器写入的缓冲区数。

表 3-17 Backends 字段解释

字段	说明
Buffers backend fsync	后端必须执行自己的 fsync 调用的次数。

字段	说明
Buffers backend	后端直接写入的缓冲区数。

Database Objects

图 3-27 Database Objects 性能指标

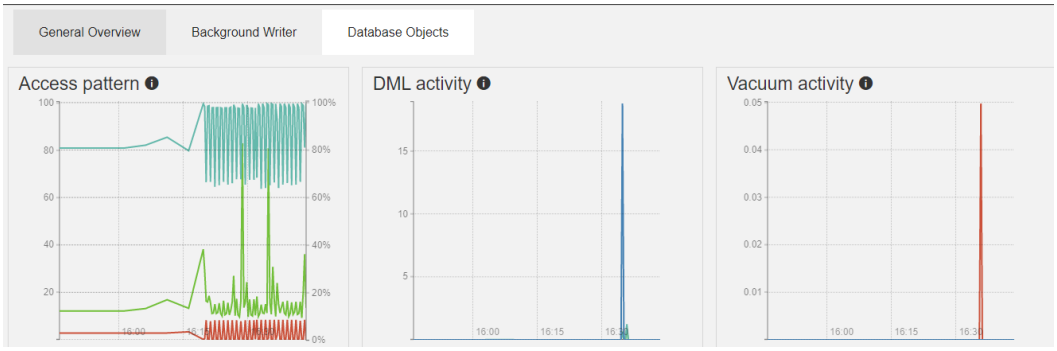


表 3-18 Access pattern 字段解释

字段	说明
Index scans ratio	索引扫描/序列扫描的比率。
Index scans	每秒索引扫描次数。
Sequential scans	每秒顺序扫描次数。

表 3-19 DML activity 字段解释

字段	说明
Tuples inserted	每秒插入的行数。
Tuples updated	每秒更新的行数。
Tuples HOT updated	每秒更新（HOT）。
Tuples deleted	每秒删除的行数。

表 3-20 Vacuum activity 字段解释

字段	说明
# Vacuum	每秒手动清理的次数。
# Autovacuum	每秒自动清理的次数。

字段	说明
# Analyze	每秒手动分析的次数。
# Autoanalyze	每秒自动分析的次数。

Details for all databases

图 3-28 Details for all databases 性能指标

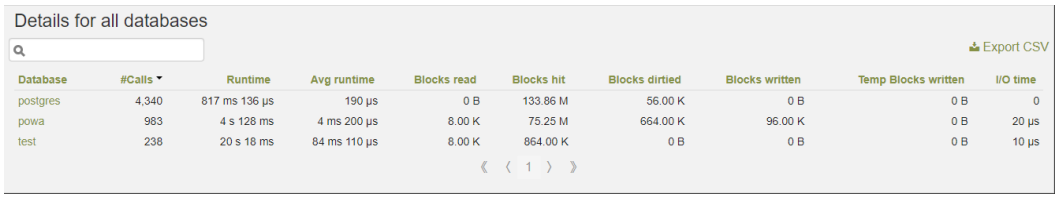


表 3-21

字段	注释
Database	数据库名称。
#Calls	执行SQL总数。
Runtime	执行SQL总耗时。
Avg runtime	执行SQL平均耗时。
Blocks read	磁盘读取的页面数。
Blocks hit	共享缓冲区命中的页面数。
Blocks dirtied	脏页数。
Blocks written	磁盘写页面数。
Temp Blocks written	磁盘写临时页面数。
I/O time	I/O等待时间。

3.5.3 部署 PoWA

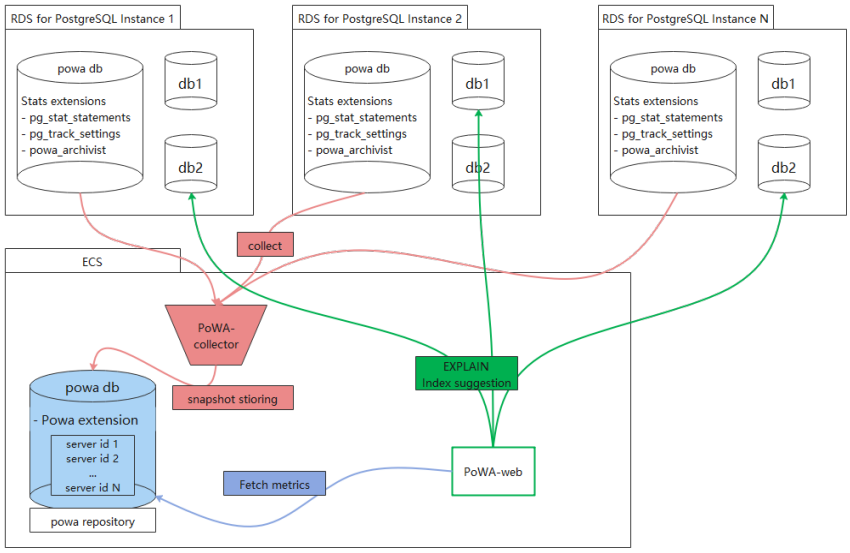
3.5.3.1 云上 PostgreSQL 实例部署 PoWA

华为云上进行远程模式部署PoWA，需要一台ECS，并在ECS上安装PoWA-archivist、PoWA-collector、PoWA-web。本章节主要介绍PoWA-archivist、PoWA-collector、PoWA-web的安装过程。

架构图

远程模式部署PoWA的架构如下图所示：

图 3-29 远程模式架构图



准备工作

- 已创建RDS for PostgreSQL 12.6实例。
- 已创建ECS并绑定弹性公网IP，本次演示所创建的ECS系统镜像为：CentOS 8.2 64bit。

Python3 的安装部署

安装PoWA-collecotor、PoWA-web依赖Python3环境，且使用pip3安装可以减少很多依赖环境安装的工作量。当前ECS已默认安装了 Python 3.6.8版本，由于版本偏低，安装最新版本的PoWA失败，建议安装最新的Python版本，详情请参见**安装Python 3.9.9**。

安装 PoWA-archivist

1. 通过wget命令获取PoWA-archivist源码：
   ```
   wget https://github.com/powa-team/powa-archivist/archive/refs/tags/REL_4_1_2.tar.gz
   ```
2. 将下载好的REL_4_1_2.tar.gz进行解压。
3. 进入解压后的目录，执行命令完成安装。
   ```
   make && make install
   ```

安装 PoWA-collector、PoWA-web

1. 切换到RDS for PostgreSQL数据库用户下，本次演示使用的是postgres。
   ```
   su - postgres
   ```
2. psycopg2 是 PoWA-collector、powa-web安装必不可少的依赖环境。
   ```
   pip install psycopg2
   pip install powa-collector
   pip install powa-web
   ```

安装完成后，查看路径树如下所示，表示PoWA-collector、PoWA-web均已安装完成。

```
/home/postgres/.local/bin
├── powa-collector.py
├── powa-web
└── __pycache__
```

创建 powa 插件

步骤1 使用root用户登录RDS for PostgreSQL实例的powa数据库。（若不存在，请先自行创建powa数据库）

步骤2 在powa数据库中创建powa插件。

```
select control_extension('create', 'pg_stat_statements');
select control_extension('create', 'btree_gist');
select control_extension('create', 'powa');
```

----结束

常见问题

Q：在执行**pip install psycopg2**时可能会遇到报错python setup.py build_ext --pg-config /path/to/pg_config build。

A：配置RDS for PostgreSQL的bin、lib路径到环境变量中，重新执行 pip install psycopg2 即可完成安装。

安装 Python 3.9.9

1. 环境准备。

   请按照以下顺序执行，否则安装Python3.9.9可能会有部分失败（SSL组件依赖失败），导致后续无法安装PoWA-collector、PoWA-web。

   ```
   yum install readline* -y
   yum install zlib* -y
   yum install gcc-c++ -y
   yum install sqlite* -y
   yum install openssl-* -y
   yum install libffi* -y
   ```

2. 安装python 3.9.9。

   a. 使用root用户执行下列命令。

   ```
   mkdir env
   cd env
   wget https://www.python.org/ftp/python/3.9.9/Python-3.9.9.tgz
   tar -xzvf Python-3.9.9.tgz
   cd Python-3.9.9
   ./configure --prefix=/usr/local/python3.9.9
   make && make install
   ```

   b. 创建软链接。

   ```
   ln -s /usr/local/python3.9.9/bin/python3.9 /usr/bin/python
   ln -s /usr/local/python3.9.9/bin/pip3.9 /usr/bin/pip
   ```

3. 验证安装是否成功。

   a. 验证安装，重点验证SSL功能。

   ```
   [root@ecs-ad4d Python-3.9.9]# python
   Python 3.9.9 (main, Nov 25 2021, 12:36:32)
   [GCC 8.4.1 20200928 (Red Hat 8.4.1-1)] on linux
   Type "help", "copyright", "credits" or "license" for more information.
   import ssl
   import urllib.request
   context = ssl._create_unverified_context()
   urllib.request.urlopen('https://www.example.com/',context=context).read()
   ```

   b. 如果有返回，说明安装成功。执行以下命令退出。

   ```
   quit()
   ```

3.5.3.2 自建 PostgreSQL 实例部署 PoWA

本章节主要介绍ECS自建PostgreSQL数据库部署PoWA的过程。

准备工作

已有自建PostgreSQL实例：

- 版本：PostgreSQL 12.6
- 管理员账号：postgres
- PostgreSQL专用存储数据库：powa-repository
- data路径：/home/postgres/data

部署 PoWA

步骤1 修改配置文件 /home/postgres/data/postgresql.conf，添加 pg_stat_statements 至参数 shared_preload_libraries，如下图所示：

```
shared_preload_libraries = 'pg_stat_statements'         # (change requires restart)
```

步骤2 执行命令重启数据库。

```
pg_ctl restart -D /home/postgres/data/
```

步骤3 使用postgres登录数据库，并创建database: powa，以及安装相关插件。

须知

创建的database必须命名为powa，否则PoWA运行过程中会报错，部分功能失效。

```
[postgres@ecs-ad4d ~]$ psql -U postgres -d postgres
psql (12.6)
Type "help" for help.
postgres=# create database powa;
CREATE DATABASE
postgres=# \c powa
You are now connected to database "powa" as user "postgres".
powa=# create extension pg_stat_statements ;
CREATE EXTENSION
powa=# create extension btree_gist ;
CREATE EXTENSION
powa=# create extension powa;
CREATE EXTENSION
```

步骤4 配置需要采集性能指标的实例信息。

1. 执行SQL，添加目标实例信息。

```
powa=# select powa_register_server(
    hostname => '192.168.0.1',
    alias => 'myInstance',
    port => 5432,
    username => 'user1',
    password => '**********',
    frequency => 300);
     powa_register_server
    ----------------------
     t
    (1 row)
```

2. 通过查看“powa_servers”表来获取当前采集指标的实例信息。

```
powa=# select * from powa_servers;
id | hostname | alias | port | username |  password  | dbname | frequency | powa_coalesce | retention |
allow_ui_connection |version
----+---------------+------------+------+----------+------------+--------+-----------+---------------+-----------
+-----------------
0 |           | <local>|  0 |          |            |        |        -1 |   100         | 00:00:00  | t           |
1 | 192.168.0.1 | myInstance | user1 | 5432     | ********** | powa   |       300 |           100 | 1 day       |
t           |
(2 rows)
```

须知

在录入目标实例信息、查询目标实例都会涉及到目标实例的IP、root用户账户、明文密码等重要隐私信息，可能会面临信安全风险。

请谨慎评估该插件带来的安全风险后决定是否使用该插件。

----结束

PoWA-collector 配置

启动PoWA-collector：

```
cd /home/postgres/.local/bin
./powa-collector.py &
```

PoWA-collector启动时，将按以下顺序搜索配置文件作为其配置：

1. /etc/powa-collector.conf
2. ~/.config/powa-collector.conf
3. ~/.powa-collector.conf
4. ./powa-collector.conf

配置文件中需要包含以下选项：

- repository.dsn : URL，用于通知 powa-collector 如何连接专用存储数据库（ powa-repository ）。
- debug : Boolean类型，用于指定是否在调试模式下启动 powa-collector。

本次演示中将配置写入文件./powa-collector.conf

```
{
   "repository": {
   "dsn": "postgresql://postgres@localhost:5432/powa"
   },
   "debug": true
}
```

PoWA-collector 的配置中并没有密码的配置，所以powa-repository数据库的pg_hba.conf中需要配置对应的连接策略为trust免密连接。

PoWA-web 配置

启动PoWA-web：

```
cd /home/postgres/.local/bin
./powa-web &
```

PoWA-web启动时，将按以下顺序搜索配置文件作为其配置：

1. /etc/powa-web.conf
2. ~/.config/powa-web.conf
3. ~/.powa-web.conf
4. ./powa-web.conf

本次实例中需要将配置内容写入文件./powa-web.conf中。

```
# cd /home/postgres/.local/bin
# vim ./powa-web.conf
# 写入配置内容，并保存
servers={
    'main': {
      'host': 'localhost',
      'port': '5432',
      'database': 'powa',
      'username': 'postgres',
      'query': {'client_encoding': 'utf8'}
    }
}
cookie_secret="SECRET_STRING"
```

本章节中powa-repository数据库pg_hab.conf中配置为trust，免密连接，因此未配置password。

3.5.4 在 PoWA 上查看指标详情

PoWA部署完成并成功启动PoWA-collector、PoWA-web后，可以通过浏览器登录PoWA，查看监控实例的指标详情。

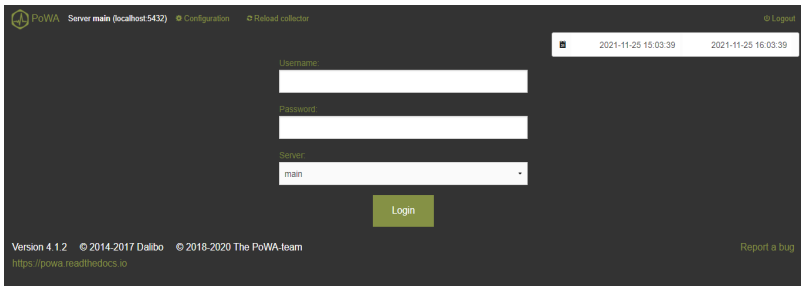
访问 PoWA

步骤1 使用浏览器访问PoWA。

说明

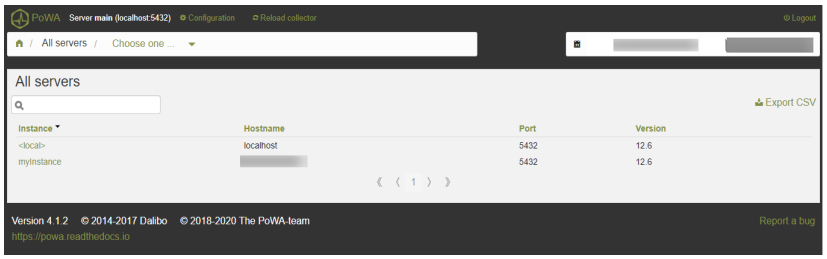
- powa-web.conf中未配置port选项，使用默认值8888
- 浏览器访问链接： http://*演示使用的ECS IP地址*:8888/

图 3-30 访问 PoWA



步骤2 输入用户名和密码，单击“Login”。

图 3-31 PoWA 首页



该PoWA中采集了两个PostgreSQL实例的信息：

- <local>：ECS自建PostgreSQL，作为powa-repository角色。
- myinstance：云数据库 RDS for PostgreSQL实例，作为性能数据采集目标。（ myinstance为在powa-repository中注册实例别名(alias字段) ）。

步骤3 单击对应的实例，即可查看实例具体的性能指标。

----结束

查看指标详情

PoWA可以采集、显示的性能指标非常丰富，下面的步骤以查看慢SQL指标为例。

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角的，选择区域。

步骤3 单击页面左上角的，选择“数据库 > 云数据库 RDS”，进入RDS信息页面。

步骤4 在“实例管理”页面，选择目标实例，单击操作列的“登录”，进入数据管理服务实例登录界面。

您也可以在“实例管理”页面，单击目标实例名称，在页面右上角，单击“登录”，进入数据管理服务实例登录界面。

步骤5 正确输入数据库用户名和密码，单击“登录”，即可进入您的数据库并进行管理。

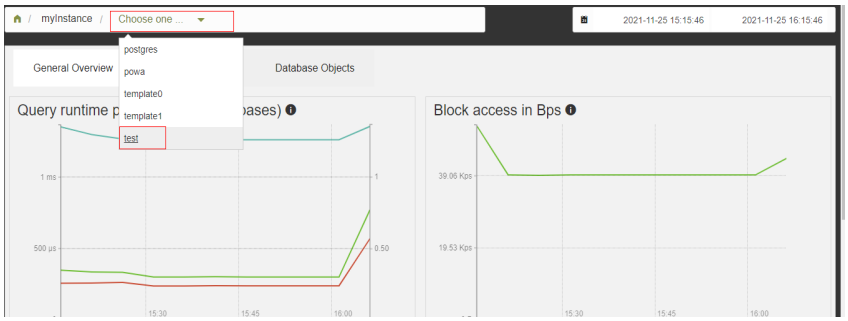
步骤6 在首页数据库列表栏单击“新建数据库”。

步骤7 在弹窗中填写数据库名称“test”、字符集等信息。

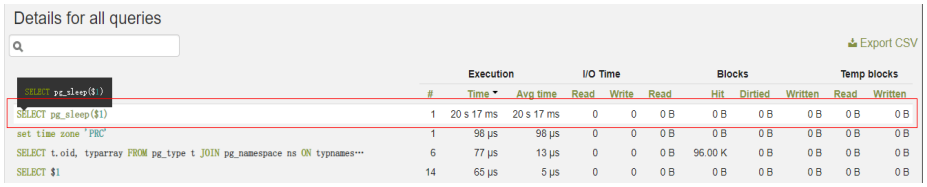
步骤8 单击“SQL查询”，在test数据库上执行慢SQL。

步骤9 等待大概5分钟后，在PoWA首页选中目标实例，选择test数据库，如下图所示：

图 3-32 PoWA 首页



在 Details for all queries中可以看到SELECT pg_sleep($1)语句，对应执行时间20s。



----结束

安装扩展插件并采集性能指标

下面步骤以pg_track_settings插件为例。

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角的，选择区域。

步骤3 单击页面左上角的，选择“数据库 > 云数据库 RDS”，进入RDS信息页面。

步骤4 在“实例管理”页面，选择目标实例，单击操作列的“登录”，进入数据管理服务实例登录界面。

您也可以在“实例管理”页面，单击目标实例名称，在页面右上角，单击“登录”，进入数据管理服务实例登录界面。

步骤5 正确输入数据库用户名和密码，单击“登录”，即可进入您的数据库并进行管理。

步骤6 选择powa数据库，执行SQL命令创建pg_track_settings插件。

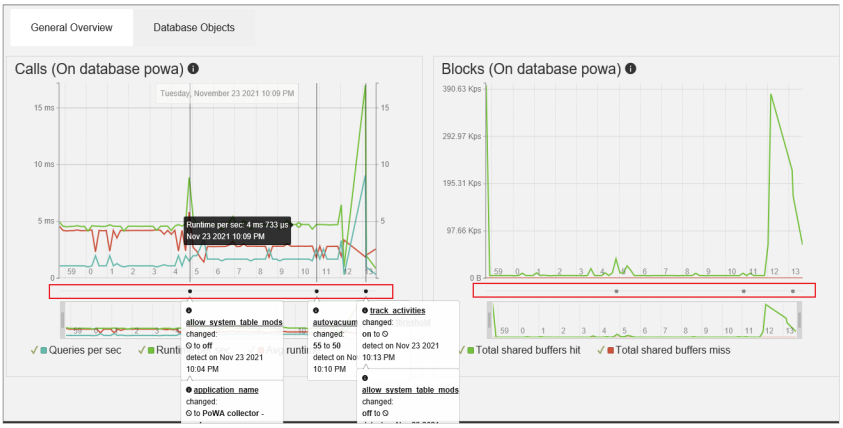
```
select control_extension('create', 'pg_track_settings');
```

步骤7 ECS上自建PostgreSQL(powa-repository)，安装pg_track_settings插件，并激活pg_track_settings插件采集性能指标。

```
# pg_track_settings
cd /home/postgres/env
wget https://github.com/rjuju/pg_track_settings/archive/refs/tags/2.0.1.tar.gz
mv 2.0.1.tar.gz pg_track_settings.2.0.1.tar.gz
tar -xzvf pg_track_settings.2.0.1.tar.gz
cd pg_track_settings-2.0.1
make && make install
# powa-repository
psql -d powa
powa=# create extension pg_track_settings ;
CREATE EXTENSION
# 激活目标实例 pg_track_settings 采集功功能
dbpowa=# select powa_activate_extension(1, 'pg_track_settings');
powa_activate_extension
-------------------------
t
(1 row)
```

步骤8 pg_track_settings插件扩展完成，进行验证。

在目标实例上修改参数“autovacuum_analyze_threshold”，原始默认值为50，修改后为55，等待大概5分钟，在PoWA页面上就可以看到对应参数修改的记录了，如下图所示：



上图中3个说明框中记录内容如下：

- 记录了pg_track_settings插件激活的时间点及当时数据库参数值。
- 记录了“autovacuum_analyze_threshold”参数被修改的时间以及原始值和修改后的值。
- 记录了pg_track_settings插件被取消的时间点及当时数据库参数值。

----结束

3.6 pg_dump 使用最佳实践

简介

pg_dump是PostgreSQL原生的备份工具。pg_dump生成的备份文件可以是一个SQL脚本文件，也可以是一个归档文件。详细信息请查看**pg_dump官方说明**。

- SQL脚本文件：纯文本格式的文件，其中包含将数据库重建到备份时状态的SQL命令。
- 归档格式的备份文件：必须与pg_restore一起使用来重建数据库，这种格式允许pg_restore选择恢复哪些数据。

注意事项

pg_dump适合单个库、schema级、表级导出，只会导出表及数据、函数等，数据库和用户需要提前在要恢复的库创建。

- --format=custom：备份为二进制格式，二进制格式的备份只能使用pg_restore来还原，并且可以指定还原的表。
- --format=plain：备份为文本，文本格式的备份还原，直接使用用户连接到对应的数据库执行备份文本即可。

限制条件

在使用pg_dump和pg_restore进行备份和恢复时，确保源数据库和目标库的版本一致，以避免出现兼容性问题，如果版本不一致可能会导致数据丢失或无法正确还原数据。

准备测试数据

```
# 创建数据库
create database dump_database;

# 登录dump_database数据库
\c dump_database

# 创建表1并插入数据
create table dump_table(id int primary key, content char(50));
insert into dump_table values(1,'aa');
insert into dump_table values(2,'bb');

# 创建表2并插入数据
create table dump_table2(id int primary key, content char(50));
insert into dump_table2 values(1,'aaaa');
insert into dump_table2 values(2,'bbbb');
```

使用 pg_dump 将数据库导出至 SQL 文件

语法

```
pg_dump --username=<DB_USER> --host=<DB_IPADDRESS> --port=<DB_PORT> --format=plain --
file=<BACKUP_FILE><DB_NAME>
```

- DB_USER为数据库用户。
- DB_IPADDRESS为数据库地址。
- DB_PORT为数据库端口。
- BACKUP_FILE为要导出的文件名称。
- DB_NAME为要导出的数据库名称。
- --format为导出的文件格式，plain为输出纯文本SQL脚本文件（默认）。其他选项详见**pg_dump官方说明**。

示例

- 导出数据库至SQL文件（INSERT语句）。
  ```
  $ pg_dump --username=root --host=192.168.61.143 --port=5432 --format=plain --inserts --
  file=backup.sql dump_database
  Password for user root:
  ```
- 导出数据库中所有表结构至SQL文件。
  ```
  $ pg_dump --username=root --host=192.168.61.143 --port=5432 --format=plain --schema-only --
  file=backup.sql dump_database
  Password for user root:
  ```
- 导出数据库中所有表数据至SQL文件。
  ```
  $ pg_dump --username=root --host=192.168.61.143 --port=5432 --format=plain --data-only --
  file=backup.sql dump_database
  Password for user root:
  ```

命令执行完会生成“backup.sql”文件，如下：

```
[rds@localhost ~]$ ll backup.sql
-rw-r----- 1 rds rds 5657 May 24 09:21 backup.sql
```

使用 pg_dump 将数据库中的表导出至 SQL 文件

语法

```
pg_dump --username=<DB_USER> --host=<DB_ADDRESS> --port=<DB_PORT> --format=plain --
file=<BACKUP_FILE> <DB_NAME> --table=<TABLE_NAME>
```

- DB_USER为数据库用户。
- DB_ADDRESS为数据库地址。
- DB_PORT为数据库端口。
- BACKUP_FILE为要导出的文件名称。
- DB_NAME为要迁移的数据库名称。
- TABLE_NAME为要迁移的数据库中指定表名称。
- --format为导出的文件格式，plain为输出纯文本SQL脚本文件（默认）。其他选项详见**pg_dump官方说明**。

示例

- 导出数据库中指定的单表至SQL文件。
```
 $ pg_dump --username=root --host=192.168.61.143 --port=5432 --format=plain --file=backup.sql dump_database --table=dump_table
 Password for user root
```
- 导出数据库中指定的多表至SQL文件。
```
 $ pg_dump --username=root --host=192.168.61.143 --port=5432 --format=plain --file=backup.sql dump_database --table=dump_table --table=dump_table2
 Password for user root:
```
- 导出数据库中以ts_开头的所有表至SQL文件。
```
 $ pg_dump --username=root --host=192.168.61.143 --port=5432 --format=plain --file=backup.sql dump_database --table=ts_*
 Password for user root:
```
- 导出数据库中除ts_开头之外的所有表至SQL文件。
```
 $ pg_dump --username=root --host=192.168.61.143 --port=5432 --format=plain --file=backup.sql dump_database -T=ts_*
 Password for user root:
```

命令执行完会生成“backup.sql”文件，如下：

```
[rds@localhost ~]$ ll backup.sql
-rw-r----- 1 rds rds 5657 May 24 09:21 backup.sql
```

使用 pg_dump 导出特定 schema 下的数据

语法

```
pg_dump --username=<DB_USER> --host=<DB_IPADDRESS> --port=<DB_PORT> --format=plain --schema=<SCHEMA> <DB_NAME> --table=<BACKUP_FILE>
```

- DB_USER为数据库用户。
- DB_IPADDRESS为数据库地址。
- DB_PORT为数据库端口。
- BACKUP_FILE为要导出的文件名称。
- DB_NAME为要导出的数据库名称。
- SCHEMA为要导出的schema名称。
- --format为导出的文件格式，plain为输出纯文本SQL脚本文件（默认）。其他选项详见**pg_dump官方说明**。

示例

- 导出指定库中public schema的所有数据。
```
pg_dump --username=root --host=192.168.61.143 --port=5432 --format=plain --schema=public dump_database  > backup.sql
```

- 导出指定库中除public schema以外的所有数据，结果以自定义压缩格式导出。
  ```
  pg_dump --username=root --host=192.168.61.143 --port=5432 --format=custom -b -v -N public
  dump_database > all_sch_except_pub.backup
  ```

还原数据

使用纯文本SQL脚本文件导出的数据，还原时直接使用psql命令即可，比如：

```
# 还原特定数据库
psql --username=root --host=192.168.61.143 --port=5432  backup_database  < backup.sql

# 还原特定表
psql --username=root --host=192.168.61.143 --port=5432  backup_database --
table=dump_table  < backup.sql

# 还原特定schema
psql --username=root --host=192.168.61.143 --port=5432  backup_database --schema=public  <
backup.sql
```

说明

在恢复之前在目标库中创建数据库backup_database。

使用其他格式导出的数据进行还原时，需要使用pg_restore。**pg_restore**用于恢复由pg_dump转储的任何非纯文本格式中的PostgreSQL数据库。

```
pg_restore --username=root --host=192.168.61.143 --port=5432 --dbname=backup_database --
format=custom all_sch_except_pub.backup --verbose
```

常见问题

1. 如果在使用pg_dump导出时，报错用户权限不足。

   解决方法：

   检查是否使用的root用户导出，如果不是root用户则会报权限不足；如果使用root用户导出，仍然提示没有权限，请检查数据库版本，root用户执行pg_dump命令需要内核版本为支持root提权的版本，支持root提权版本情况见**root用户权限说明**。

2. 将备份的文件导入到RDS for PostgreSQL目标数据库时发现control_extension等几个函数报错。

   解决方法：

   由于目标库中自带这些函数，因此该报错可以忽略。

3.7 PgBouncer 使用最佳实践

PgBouncer 介绍

PgBouncer是为PostgreSQL提供的轻量级连接池工具，作用如下：

- 能够缓存和PostgreSQL的连接，当有连接请求进来的时候，直接分配空闲进程，而不需要PostgreSQL fork出新进程来建立连接，以节省创建新进程，创建连接的资源消耗。
- 能够有效提高连接的利用率，避免过多的无效连接，导致数据库消耗资源过大，CPU占用过高。
- 对客户端连接进行限制，预防过多或恶意的连接请求。

轻量级体现在：

- 使用libevent进行socket通信，通信效率高。
- C语言编写，效率高，每个连接仅消耗2KB内存。

PgBouncer目前支持三种连接池模型：

- session会话级连接。只有与当客户端的会话结束时，PgBouncer才会收回已分配的连接。
- transaction事务级连接。当事务完成后，PgBouncer会回收已分配的连接。也就是说客户端只是在事务中才能独占此连接，非事务请求没有独享的连接。
- statement语句级连接。任何数据库请求完成后，PgBouncer都会回收连接。此种模式下，客户端不能使用事务，否则会造成数据的不一致。

PgBouncer默认选项是session，建议修改为transaction。

安装配置

在云上部署PgBouncer连接池，需要先**购买弹性云服务器**。建议选择与后端RDS实例相同VPC、相同子网创建，降低网络通信时延。购买成功后登录ECS进行环境搭建。

1. 由于PgBouncer是基于libevent开发，需要安装libevent-devel openssl-devel两个依赖包。命令如下：
```
yum install -y libevent-devel
yum install -y openssl-devel
```
2. 依赖包安装后，在PgBouncer官网下载源码，以普通用户身份进行编译、安装。
```
su - pgbouncer
tar -zxvf pgbouncer-1.19.0.tar.gz
cd  pgbouncer-1.19.0
./configure --prefix=/usr/local
make
make install
```
3. 创建如下目录，用于保存PgBouncer的生成文件（日志、进程标识等）。
```
mkdir -p /etc/pgbouncer/
mkdir -p /var/log/pgbouncer/
mkdir -p /var/run/pgbouncer/
```
4. 启动PgBouncer前，需要构建配置文件“pgbouncer.ini”。
```
[databases]
* = host=127.0.0.1 port=5432
[pgbouncer]
logfile = /var/log/pgbouncer/pgbouncer.log
pidfile = /var/run/pgbouncer/pgbouncer.pid
listen_addr = *
listen_port = 6432
auth_type = md5
auth_file = /etc/pgbouncer/userlist.txt
admin_users = postgres
stats_users = stats, postgres
pool_mode = transaction
server_reset_query = DISCARD ALL
max_client_conn = 100
default_pool_size = 20
;; resolve: unsupported startup parameter: extra_float_digits
;;ignore_startup_parameters = extra_float_digits
```
配置文件中各参数含义可参考**PgBouncer官方文档**。

启动 pgbouncer

PgBouncer不能以root身份启动，需要基于普通用户身份进行启动。

```
pgbouncer -d /etc/pgbouncer/pgbouncer.ini
```

启动后，可通过**netstat -tunlp | grep pgbouncer**查看连接池的监听端口，而后进行连接：

```
psql -U root -d postgres -h 127.0.0.1 -p 6432
Password for user root:
psql (12.13)
Type "help" for help.
postgres=> \l
                                  List of databases
   Name    |   Owner   | Encoding |   Collate   |    Ctype    |    Access privileges
-----------+-----------+----------+-------------+-------------+-------------------------
 postgres  | pgbouncer | UTF8     | en_US.UTF-8 | en_US.UTF-8 |
 template0 | pgbouncer | UTF8     | en_US.UTF-8 | en_US.UTF-8 | =c/pgbouncer
           |           |          |             |             | pgbouncer=CTc/pgbouncer
 template1 | pgbouncer | UTF8     | en_US.UTF-8 | en_US.UTF-8 | =c/pgbouncer
```

停止 PgBouncer

可以直接通过Kill命令停止。

```
kill `cat /var/run/pgbouncer/pgbouncer.pid`
cat /var/run/pgbouncer/pgbouncer.pid | xargs kill -9
```

PgBouncer 管理

PgBouncer对外提供了一个虚拟数据库pgbouncer，之所以称为虚拟数据库，是因为它可以提供像PostgreSQL那样的数据库操作界面，但是这个数据库却并不是真实存在的，而是PgBouncer虚拟出来的一个命令行界面。登录虚拟数据库：

```
psql -p 6432 -d pgbouncer
```

如果修改了一些配置参数，可以不用重启PgBouncer而是**reload**使其生效。

```
pgbouncer=# reload;
RELOAD
```

登录后可以通过**show help**查看命令帮助，通过**show clients**查看客户端连接信息，通过**show pools**查看连接池信息。

实现读写分离示例

PgBouncer并不支持自动解析读写请求，并进行读写分离路由，需要业务侧对读写操作进行区分。

1. 首先，修改配置文件“pgbouncer.ini”配置的数据库信息，添加主库、只读库连接配置。本例中参数设置如下：

   ```
   [databases]
   ;; * = host=127.0.0.1 port=5432
   #配置只读库的连接信息
   mydb_read：host=10.7.131.69 port=5432 dbname=postgres user=root password=***
   # 配置主库的连接信息
   mydb_write:  host=10.8.115.171 port=5432 dbname=postgres user=root password=***
   [pgbouncer]
   logfile = /var/log/pgbouncer/pgbouncer.log
   pidfile = /var/run/pgbouncer/pgbouncer.pid
   listen_addr = *
   listen_port = 6432
   auth_type = md5
   auth_file = /etc/pgbouncer/userlist.txt
   admin_users = postgres
   stats_users = stats, postgres
   pool_mode = transaction
   ```

```
server_reset_query = DISCARD ALL
max_client_conn = 100
default_pool_size = 20
;; resolve: unsupported startup parameter: extra_float_digits
;;ignore_startup_parameters = extra_float_digits
```

2. 验证是否能连接主库和只读数据库。通过psql成功连接只读、主库，可支持业务读写分离。

```
psql -U root -d mydb_write -h 127.0.0.1 -p 6432
Password for user root:
psql (14.6)
mydb_write=> SELECT pg_is_in_recovery();
 pg_is_in_recovery
----------------------
 f
(1 row)
psql -U root -d mydb_read -h 127.0.0.1 -p 6432
Password for user root:
psql (14.6)
mydb_read=> SELECT pg_is_in_recovery();
pg_is_in_recovery
----------------------
 t
(1 row)
```

3.8 RDS for PostgreSQL 安全最佳实践

PostgreSQL数据库在可靠性、稳定性、数据一致性等获得了业内极高的声誉，已成为许多企业的首选开源关系数据库，业界简称PG。RDS for PostgreSQL是一种基于云计算平台的即开即用、稳定可靠、弹性伸缩、便捷管理的在线云数据库服务。

为加强RDS for PostgreSQL数据库安全性，本文将从以下几个维度给出建议，您可以根据业务需要在本指导的基础上进行安全配置。

- **配置数据库的最大连接数**
- **配置客户端认证超时时间**
- **配置SSL连接和加密算法**
- **配置密码加密功能**
- **配置服务器拒绝带反斜杠转义的引号**
- **定期检查并删除业务不再使用的角色**
- **建议回收public模式的所有权限**
- **设置合理的用户角色密码有效期**
- **配置日志级别记录发生错误的SQL语句**
- **确保数据库账号的最低权限**
- **开启备份功能**
- **开启数据库审计功能**
- **避免绑定EIP直接通过公网访问RDS for PostgreSQL**
- **数据库版本更新到最新版本**
- **配置账号认证失败延迟时间**

配置数据库的最大连接数

max_connections 决定了数据库的最大并发连接数。增加这个参数值可能引起RDS for PostgreSQL请求更多的System V共享内存或者信号量，会导致超出操作系统默认配置

允许的值。请根据业务的复杂度，合理配置max_connections，具体可参考**实例使用规范**。

配置客户端认证超时时间

authentication_timeout控制完成客户端认证的时间上限，单位是秒。该参数可以防止客户端长时间占用连接通道，默认是60s。如果在指定的时间内没有完成认证，连接将被强制关闭。该超时时间的配置是为了增强PostgreSQL的安全性。

配置 SSL 连接和加密算法

尽可能利用SSL进行TCP/IP连接，使用SSL加密通信可确保客户端和服务器之间的所有通信都经过加密，防止数据被泄露和篡改，确保数据的完整性。在设置SSL加密时，服务端需要配置安全的TLS协议和加密算法，推荐使用TLSv1.2协议，加密算法推荐使用EECDH+ECDSA+AESGCM:EECDH+aRSA+AESGCM:EDH+aRSA+AESGCM:EDH+aDSS+AESGCM:!aNULL:!eNULL:!LOW:!3DES:!MD5:!EXP:!SRP:!RC4，具体请参考**SSL连接**。

可通过修改参数“ssl_min_protocol_version”配置TLS协议，修改参数“ssl_ciphers”配置加密算法。

配置密码加密功能

密码必须要加密。使用**CREATE USER**或者**ALTER ROLE**修改密码时候，默认使用加密的方式，推荐使用scram-sha-256，可通过修改参数“password_encryption”进行配置。

MD5选项仅供与低版本兼容场景使用，新建数据库实例默认使用scram-sha-256。

须知

参数“password_encryption”修改后需要重置密码后才能生效。

配置服务器拒绝带反斜杠转义的引号

参数“backslash_quote”控制字符串里面引号是否可以被\'代替。推荐使用SQL标准方法，表示一个引号是写两遍 ('')，如果客户端代码不能正确的转义，可能发生SQL注入攻击。建议配置参数“backslash_quote”值为“safe_encoding”，拒绝带反斜杠转义的引号的查询，可以避免SQL注入的风险。

定期检查并删除业务不再使用的角色

对于每个查询出来的角色，检查是否必须存在，任何未知的角色都需要被审视，确保每个角色都是正常使用的，否则删除这些角色。可通过如下命令进行查询：

SELECT rolname FROM pg_roles;

建议回收 public 模式的所有权限

public模式是默认的模式，所有用户都可以访问其中的对象，包括表、函数、视图等。如果public模式中的对象被授予了权限，那么所有用户都可以访问这些对象，这可能会导致安全漏洞。root用户可通过如下命令回收权限：

revoke all on schema public from public;

设置合理的用户角色密码有效期

当创建角色时候，使用**VALID UNTIL**关键字设置过多长时间后角色的密码不再有效。如果这个关键字被忽略，密码会长期有效。建议定期更改密码，例如每三个月更改一次密码。可通过如下命令进行设置：

CREATE ROLE name WITH PASSWORD *'password'* **VALID UNTIL 'timestamp';**

检查是否设置密码有效期：

SELECT rolname,rolvaliduntil FROM pg_roles WHERE rolsuper = false AND rolvaliduntil IS NULL;

配置日志级别记录发生错误的 SQL 语句

参数“log_min_error_statement”控制哪些引起错误的SQL语句记录到服务器日志中。对于大于等于当前配置等级的SQL语句消息，会记录到日志里。有效的值包括debug5, debug4, debug3, debug2, debug1, info, notice, warning, error, log, fatal, panic。“log_min_error_statement”至少配置为“error”，具体可参考**日志配置管理**。

确保数据库账号的最低权限

RDS for PostgreSQL支持“基于角色”的方法授予账号对数据和命令的访问权限。建议管理员结合业务需要，遵从最低授权原则，创建合适的**数据库账号**，对账号进行授权。如果发现存在不符合该角色的账号权限，请结合业务需要，对账号权限进行更新或者**删除**。由于PostgreSQL存在一些**内置账号**，用于给数据库实例提供完善的后台运维管理服务，禁止用户使用和删除。

开启备份功能

创建云数据库RDS实例时，系统默认开启自动备份策略，默认自动备份保留7天，可根据业务需要调整备份保留时长。RDS for PostgreSQL实例支持**自动备份**和**手动备份**，您可以定期对数据库进行备份，当数据库故障或数据损坏时，可以**通过备份文件恢复数据库**，从而保证数据可靠性，详情请参见**数据备份**。

开启数据库审计功能

通过将PostgreSQL审计扩展（pgAudit）与RDS for PostgreSQL数据库实例一起使用，可以捕获审计员通常需要或满足法规要求的详细记录。例如，您可以设置pgAudit扩展来跟踪对特定数据库和表所做的更改、记录进行更改的用户以及许多其他详细信息。pgAudit默认不开启，根据业务需要开启插件。具体配置可参考**使用pgAudit插件**。

避免绑定 EIP 直接通过公网访问 RDS for PostgreSQL

避免RDS for PostgreSQL部署在公网或者DMZ里，应该将RDS for PostgreSQL部署在华为云内部网络，使用路由器或者防火墙技术把RDS for PostgreSQL保护起来，避免直接绑定EIP方式从公网访问RDS for PostgreSQL。通过这种方式防止未授权的访问及DDos攻击等。建议解绑弹性公网IP，如果您的业务必须绑定EIP，请务必通过设置**安全组规则**限制访问数据库的源IP。

数据库版本更新到最新版本

PostgreSQL社区当前9.5/9.6/10版本已经EOL，社区已不再维护，云上9.5/9.6版本已经发布**EOS公告**。使用较老的版本可能存在安全风险，运行最新版本的软件可以避免受

到某些攻击。如果业务需要，可通过**升级内核小版本**或者**使用转储与还原升级大版本**。

配置账号认证失败延迟时间

PostgreSQL数据库默认内置了auth_delay插件，auth_delay会使服务器在返回认证失败之前短暂停止，使得暴力破解数据库密码更难。可通过**修改RDS for PostgreSQL实例参数**设置auth_delay.milliseconds参数（该参数为返回认证失败之前等待的毫秒数）延迟账号登录认证失败的等待时间，缺省值是0。

4 RDS for SQL Server

4.1 恢复备份文件到 RDS for SQL Server 实例的版本限制

关系型数据库支持使用已有的自动和手动备份恢复实例数据，可恢复到备份被创建时的状态。

最佳实践

- 您可以将本地实例上的数据库通过全量备份生成备份文件，并通过OBS服务与DRS服务，将该备份文件直接还原到RDS for SQL Server实例上。
- 数据库版本支持从低版本恢复到高版本，用户从本地备份出来的备份文件的版本必须小于等于要还原的目标实例的版本。

  说明

  例如：您本地是2012标准版的实例，备份文件就只能还原到2014，2016标准版或企业版，不能还原到2008的所有版本，和2014、2016的Web版上。
- 云数据库RDS控制台提供多种恢复方式，具体请参见**将数据库实例恢复到指定时间点**和**恢复备份**。

4.2 使用导入导出功能将 ECS 上的 SQL Server 数据库迁移到 RDS for SQL Server

适用场景

- 用户在ECS上创建SQL Server数据库。
- 当ECS上SQL Server实例的版本高于RDS for SQL Server实例的版本时，无法通过DRS进行迁移。
- 已成功安装SSMS客户端。

操作步骤

步骤1 创建一个ECS虚拟机。

说明

虚拟机跟对应的RDS应在同一个Region、VPC下。

步骤2 在ECS上安装SQL Server 2008、SQL Server 2012、SQL Server 2014版本。

说明

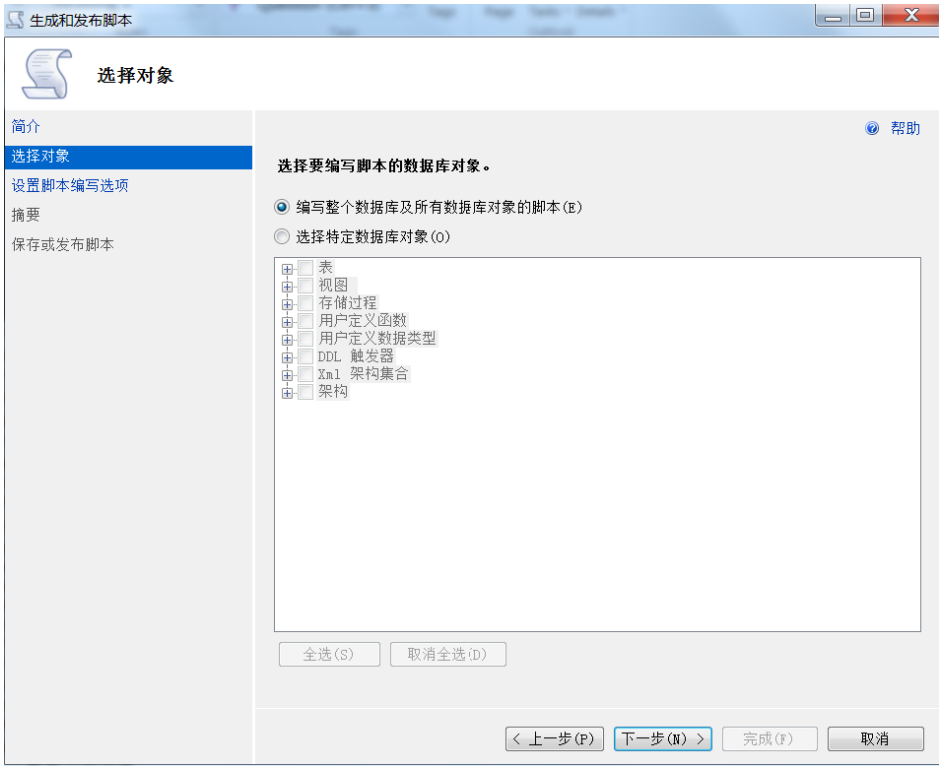
在ECS上安装的SQL Server版本，至少是标准版，最好跟需要还原的目标实例版本保持一致。

步骤3 将本地“.bak”文件上传至ECS服务器端，并通过该ECS上的SQL Server服务器进行本地还原。

步骤4 通过SQL Server自带的脚本生成工具，生成ECS上的数据库结构脚本。

1. 选中需要生成schema脚本的数据库，单击鼠标右键选择“任务 > 生成脚本”。
2. 在导航页中根据提示单击“下一步”，在“选择对象”页面，确定要导出的对象，可选择全部，也可以选择独立对象模块导出。如图4-1所示。

图 4-1 选择要导出的对象

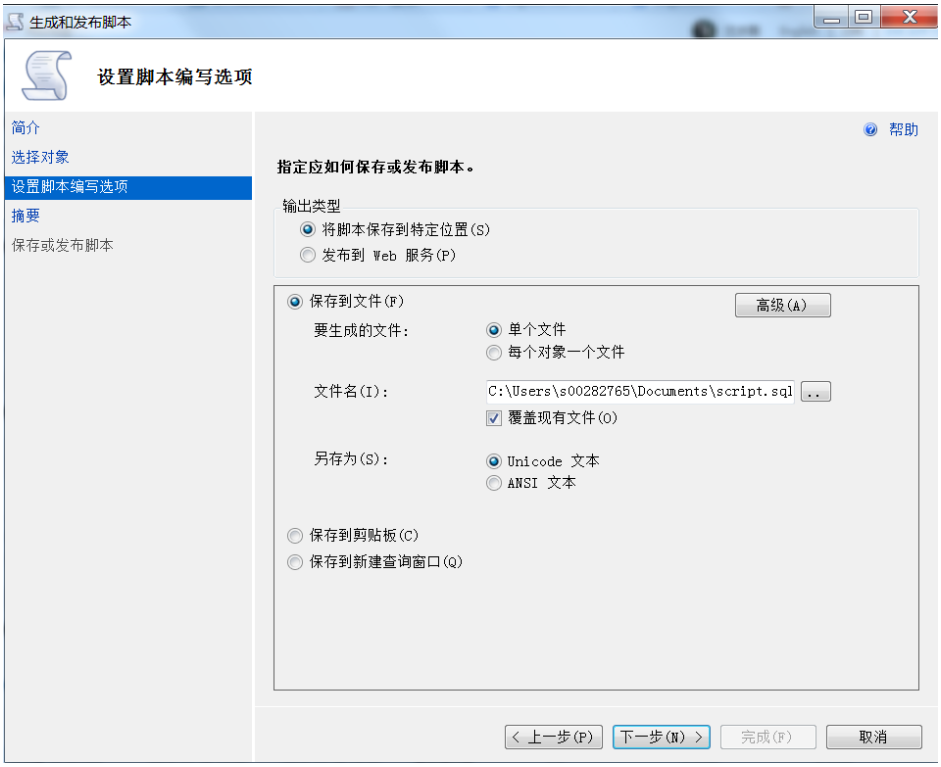


3. 单击“下一步”，在“设置脚本编写选项”页面，选择将要导出文件的保存位置。

说明

建议保存到本机，并生成一个SQL脚本方便执行。

图 4-2 选择导出文件的保存位置



4. 单击图4-2中的“高级”按钮，进入“高级脚本编写选项”页面，根据实际需要选择具体脚本生成规则和相关细节，单击“确定”。例如：触发器，索引，唯一键，主键，服务器版本等重要选项。

图 4-3 高级脚本编写选项

说明

脚本Drop和Create是编写脚本数据类型的重要选项。

5. 单击“下一步”完成脚本生成。

步骤5 通过SSMS客户端连接到目标RDS实例上，打开生成的脚本SQL文件。

说明

首先创建一个空的数据库，再通过该脚本在该数据库上创建相关结构。

步骤6 完成以上步骤后通过SQL Server自带的导入导出功能完成数据迁移。

1. 选择要导入的数据库，单击鼠标右键选择“任务 > 导入数据”。
2. 根据页面导航，单击“下一步”。
3. 在“选择数据源”页面，选择要从中复制的源，单击“下一步”。
4. 在“选择目标”页面，指定要将数据复制到何处，单击“下一步”。
   - **目标**：选择SQL Server Native Client（该选项根据您的目标类型进行选择）。
   - **服务器名称**：输入目标实例所在的IP和端口号。
   - **身份验证**：选择使用SQL Server身份验证，并在下方输入rdsuser账号和密码。
   - **数据库**：选择要导入数据的目标数据库。
5. 选择复制源数据库中现有表或视图的全部数据，单击“下一步”。
6. 在“选择源表和源视图”页面，勾选需要导入的表或视图，也可全选要导入的所有对象，再单击“编辑映射”，根据实际需要进行选择，至少选中启用标识插入。
7. 根据页面导航，单击“下一步”。
8. 选择立即执行，单击“下一步”。
9. 根据导航单击“完成”，开始数据导入并查看进度，一般为4000行/秒。

----结束

4.3 修改 RDS for SQL Server 实例的参数

每一个数据库实例都有自己唯一的参数组，您可根据业务需求对您所创建的参数组里边的参数进行调整。

每个实例的参数都是唯一的，且修改后不会对其他实例产生影响。

操作步骤

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角的，选择区域。

步骤3 单击页面左上角的，选择“数据库 > 云数据库 RDS”，进入RDS信息页面。

步骤4 在“实例管理”页面，选择指定的实例，单击实例名称。

步骤5 在“参数修改”页签，修改相应参数。

说明

- 系统默认参数组中的所有参数组不可修改。
  - 每个SQL Server版本都有对应的唯一默认参数组模板。
  - 选择对应版本的模板，单击“更多 > 应用”，可将该默认参数组模板上的参数应用到当前实例对应的参数上。
- 您可修改您所创建的自定义参数组中部分参数的值。
  - 您可以在“参数模板管理”的“自定义”页签下根据一个默认参数组模板创建自定义参数组。
  - 修改完成后保存修改，可将该自定义参数组应用到对应版本的多个实例上。

相关参数设置如表4-1所示，可提高实例性能。

表 4-1 相关参数

参数	说明	适用场景
max degree of parallelism	每个执行语句的CPU最大并行度，参数值默认为0。当您在使用实例时，SQL Server会通过查询引擎自动地给每一个请求分配CPU执行计划，以通过并行执行的方式有效提升实例的执行性能。	• 当用户的本地实例主要用于查询获取结果，参数值可设置为0。 • 当用户的本地实例主要用于写入，更新，删除等操作，参数值可设置为1。
max server memory (mb)	用于控制实例上SQL Server数据库服务占用整个服务器的最大内存的上限。	RDS for SQL Server已经根据您的实例进行了适当配置，该参数值可保持默认值。 如果需要修改，有以下限制条件： • 不低于2GB。 • 不高于实例最大内存的95%。
user connections	用于控制实例上用户发起的最大连接数。 参数值默认为1000，可根据实际情况进行调整。	• 设置为0，该实例连接数将不受限制。 • 不能设置1-10之间的值。

- 单击“保存”，在弹出框中单击“确定”，保存修改。
- 单击“取消”，放弃本次设置。
- 单击“预览”，可对比参数修改前和修改后的值。

参数修改完成后，您可单击“参数修改历史”查看参数的修改详情。

----结束

4.4 RDS SQL Server 支持 DMV 动态管理视图

RDS for SQL Server支持DMV动态管理视图，方便用户快速查询实例上性能消耗最高的10条SQL语句。

操作场景

- 数据库执行效率较低。
- 某些时段的CPU，IO较高。

操作步骤

步骤1 登录SQL SERVER客户端，通过rdsuser账号连接目标实例，在管理面中执行以下SQL语句。

```
declare @DatabaseName nvarchar(100)
set @DatabaseName = 'Wisdom_TT_ODS'

select top 100
DB_NAME(st.dbid) as DBName, OBJECT_NAME(st.objectid,st.dbid) as ObjectName,
substring(st.text,(qs.statement_start_offset/2)+1,((case qs.statement_end_offset when -1 then
datalength(st.text) else qs.statement_end_offset end - qs.statement_start_offset)/2) + 1) as
Statement,
st.text as Query,
qp.query_plan,
plan_generation_num,
creation_time,
last_execution_time,
execution_count,
total_worker_time,
min_worker_time,
max_worker_time,
total_logical_reads,
min_logical_reads,
max_logical_reads,
total_elapsed_time,
min_elapsed_time,
max_elapsed_time,
total_rows,
min_rows,
max_rows,
total_worker_time/execution_count as avg_worker_time,                    --平均CPU耗时
total_logical_reads/execution_count as avg_logical_reads,                --平均逻辑读
total_elapsed_time/execution_count as avg_elapsed_time,                  --平均总耗时
total_rows/execution_count as avg_rows,                                  --平均处理数据行
sql_handle,
plan_handle,
query_hash,
query_plan_hash
from sys.dm_exec_query_stats qs
cross apply sys.dm_exec_sql_text(plan_handle) st
cross apply sys.dm_exec_query_plan(plan_handle) qp
where st.dbid=DB_ID(@DatabaseName)
and text not like '%sys.%'and text not like '%[[]sys]%'
order by avg_worker_time desc
```

步骤2 查看结果中对应数据库的SQL执行记录及资源消耗情况。

----结束

4.5 使用导入导出功能将本地 SQL Server 数据库迁移到 RDS for SQL Server

适用场景

- 用户在本地实例上创建SQL Server数据库。
- 本地SQL Server实例的版本高于RDS for SQL Server实例的版本时，无法通过DRS进行迁移。
- 不想进行数据库粒度的同步，仅针对个别表对象进行同步。

操作步骤

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角的，选择区域。

步骤3 单击页面左上角的，选择“数据库 > 云数据库 RDS”，进入RDS信息页面。

步骤4 在“实例管理”页面，选择目标实例，单击实例名称，进入实例的“概览”页签。

步骤5 在左侧导航栏，选择“连接管理”。

步骤6 在“连接信息”模块“公网地址”处，单击“绑定”。

步骤7 在弹出框选择对应的弹性IP。

步骤8 在本地安装SQL Server客户端管理工具，通过弹性IP进行连接。

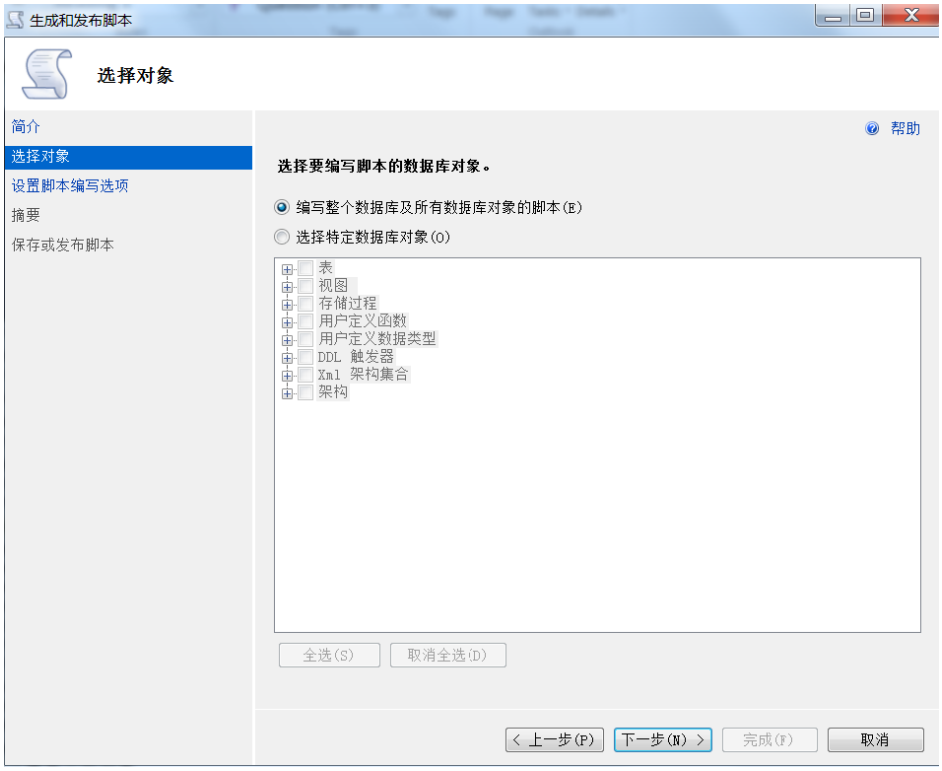
说明

单击“此处”，下载官网客户端。

步骤9 通过SQL Server自带的脚本生成工具，生成ECS上的数据库结构脚本。

1. 选中需要生成schema脚本的数据库，单击鼠标右键选择“任务 > 生成脚本”。
2. 在导航页中根据提示单击“下一步”，在“选择对象”页面，确定要导出的对象，可选择全部，也可以选择独立对象模块导出。如图4-4所示。

图 4-4 选择要导出的对象

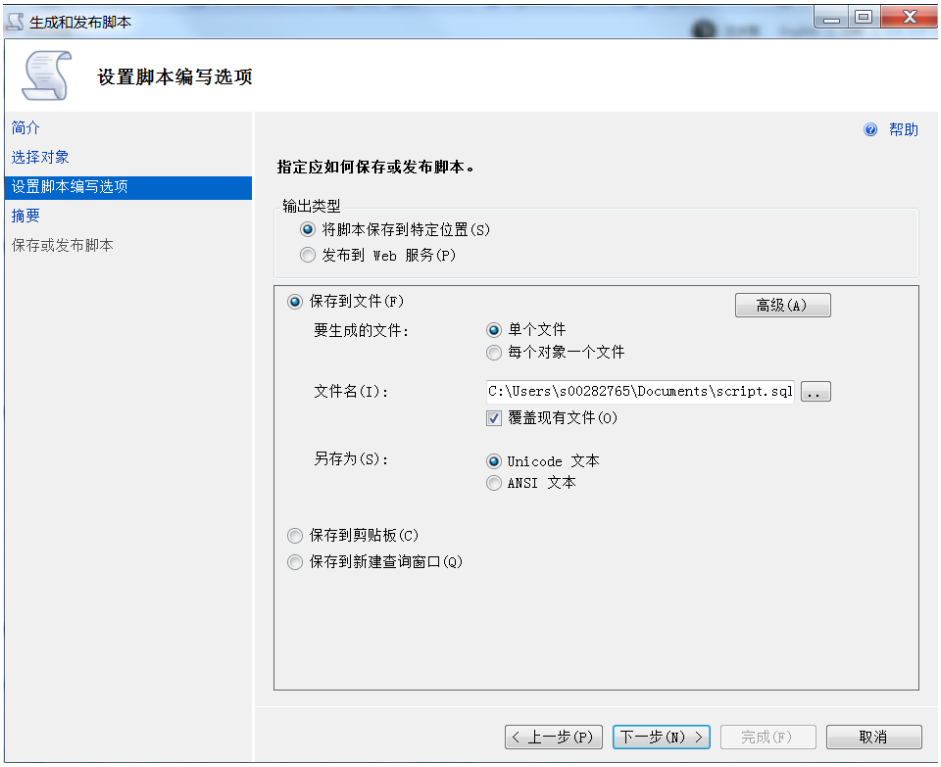


3. 单击“下一步”，在“设置脚本编写选项”页面，选择将要导出文件的保存位置。

说明

建议保存到本机，并生成一个SQL脚本方便执行。

图 4-5 选择导出文件的保存位置



4. 单击图4-5中的“高级”按钮，进入“高级脚本编写选项”页面，根据实际需要选择具体脚本生成规则和相关细节，单击“确定”。例如：触发器，索引，唯一键，主键，服务器版本等重要选项。

图 4-6 高级脚本编写选项

说明

脚本Drop和Create是编写脚本数据类型的重要选项。

5. 单击“下一步”完成脚本生成。

步骤10 通过SSMS客户端连接到目标RDS实例上，打开生成的脚本SQL文件。

说明

首先创建一个空的数据库，再通过该脚本在该数据库上创建相关结构。

步骤11 完成以上步骤后通过SQL Server自带的导入导出功能完成数据迁移。

1. 选择要导入的数据库，单击鼠标右键选择“任务 > 导入数据”。
2. 根据页面导航，单击“下一步”。
3. 在“选择数据源”页面，选择要从中复制的源，单击“下一步”。
4. 在“选择目标”页面，指定要将数据复制到何处，单击“下一步”。
   - **目标**：选择SQL Server Native Client（该选项根据您的目标类型进行选择）。
   - **服务器名称**：输入目标实例所在的IP和端口号。
   - **身份验证**：选择使用SQL Server身份验证，并在下方输入rdsuser账号和密码。
   - **数据库**：选择要导入数据的目标数据库。
5. 选择复制源数据库中现有表或视图的全部数据，单击“下一步”。
6. 在“选择源表和源视图”页面，勾选需要导入的表或视图，也可全选要导入的所有对象，再单击“编辑映射”，根据实际需要进行选择，至少选中启用标识插入。
7. 根据页面导航，单击“下一步”。
8. 选择立即执行，单击“下一步”。
9. 根据导航单击“完成”，开始数据导入并查看进度，一般为4000行/秒。

----结束

4.6 在 rdsuser 主账号下创建子账号

适用场景

创建子账号并添加用户数据库权限、创建只读账号、为子账号授权。其中rdsuser账号支持的权限如**rdsuser权限**所示。

前提条件

已完成用户数据库的创建，创建方法请参考**新建数据库**。

操作步骤

步骤1 通过DAS登录实例。

1. **登录管理控制台**。
2. 单击管理控制台左上角的，选择区域。
3. 单击页面左上角的，选择“数据库 > 云数据库 RDS”，进入RDS信息页面。
4. 在目标实例所在行，单击“操作”列的“登录”。
5. 在“实例登录”页面，使用**rdsuser**用户信息登录。

表 4-2 登录实例

参数	参数说明
登录用户名	请输入**rdsuser**。
密码	请输入**rdsuser**的密码。 **说明** 您可以选择“记住密码”，方便您下次直接登录。
定时采集	请根据实际需求选择实例是否需要使用“定时采集”功能。开启“定时采集”后： – 允许DAS保存实例中的仅库名、表名、字段名等结构定义数据，不包含表中的实际数据。 – 元数据采集默认每天凌晨采集一次。
SQL执行记录	请根据实际需求选择实例是否需要使用“SQL执行记录”功能。开启“SQL执行记录”功能后，方便您查看SQL执行历史记录，并可再次执行，无需重复输入。

6. 单击“登录”。

步骤2 创建子账号。

1. 在DAS控制台主菜单中，单击“账号管理 > 登录名”。
2. 在“登录名”页面，单击“新建登录名”。
3. 在“新建登录名”页面，配置登录信息。

表 4-3 登录信息

参数	参数说明
登录名	请自定义新的登录名名称。
验证类型	固定为“Microsoft SQL Server Authentication”。
密码	请按照以下规则自定义为新登录名设置密码。 – 至少包含大写字母、小写字母、数字和特殊字符中的三种，其中特殊字符包含~!@#$^*-_=+?% – 长度为8~128个字符。 – 不能包含登录名。 – 不能与弱密码相同。
确认密码	请再次输入密码。 **说明** 为提升安全性，建议您选择“强制实施密码策略”。
默认数据库	请在下拉框中选择新建登录名默认登录的数据库名称。
默认语言	请在下拉框中选择新建登录名使用的语言。

4. 单击“保存”。

5. 单击“返回登录名管理列表”。
6. 在“登录名”列表中，确认并查看新登录名信息。

步骤3 为子账号（即新建登录名）赋权。

说明

- 表4-4为您介绍添加单个权限（常用）的操作方法。例如您需要为授予读写权限，您可以在“编辑数据库角色”页面，同时选择“db_datareader”和“db_datawriter”。
- rdsuser支持的权限请参考**rdsuser权限**。

表 4-4 为子账号赋予不同权限的操作

授权类型	操作步骤
数据库操作权限	1. 单击新建登录名所在行“操作”列的“编辑”。 2. 在目标编辑登录名页面，单击“用户映射”标签。 3. 在“映射到此登录名的用户”列表中，单击用户数据库和新建登录名同时存在所在行的“编辑”。 4. 在“编辑数据库角色”页面，选择“db_owner”，并单击“确定”。 5. 单击“保存”。
服务器角色权限	1. 单击新建登录名所在行“操作”列的“编辑”。 2. 在目标编辑登录名页面，单击“服务器角色”标签。 3. 在“服务器角色”列表中，选择需要的服务器角色名称。 4. 单击“保存”。
安全对象权限	1. 单击新建登录名所在行“操作”列的“编辑”。 2. 在目标编辑登录名页面，单击“安全对象”标签。 3. 在“安全对象”列表中，选择需要的服务器权限名称。 4. 单击“保存”。
只读权限	1. 单击新建登录名所在行“操作”列的“编辑”。 2. 在目标编辑登录名页面，单击“用户映射”标签。 3. 在“映射到此登录名的用户”列表中，单击用户数据库和新建登录名同时存在所在行的“编辑”。 4. 在“编辑数据库角色”页面，选择“db_datareader”，并单击“确定”。 5. 单击“保存”。

授权类型	操作步骤
写权限	1. 单击新建登录名所在行“操作”列的“编辑”。 2. 在目标编辑登录名页面，单击“用户映射”标签。 3. 在“映射到此登录名的用户”列表中，单击用户数据库和新建登录名同时存在所在行的“编辑”。 4. 在“编辑数据库角色”页面，选择“db_datawriter”，并单击“确定”。 5. 单击“保存”。

----结束

rdsuser 权限

表 4-5 rdsuser 权限

名称	权限分类	权限
实例级权限	实例级角色权限	[processadmin]
		[setupadmin]
	实例级对象权限	ALTER ANY CONNECTION
		ALTER ANY LOGIN
		ALTER ANY SERVER ROLE
		ALTER SERVER STATE
		ALTER TRACE
		CONNECT ANY DATABASE
		CONTROL SERVER
		CONNECT SQL
		CREATE ANY DATABASE
		SELECT ALL USER SECURABLES
		VIEW ANY DEFINITION
		VIEW ANY DATABASE
		VIEW SERVER STATE
	数据库权限	master：public
		Msdb:Public SQLAgentUserRole
		Model:Public

名称	权限分类	权限
		Rdsadmin:Public
		OtherDB:Db_Owner

4.7 创建 tempdb 临时数据文件

操作场景

tempdb是系统数据库，是一个全局资源，可供连接到SQL Server实例或SQL数据库的所有用户使用 。它是一个临时数据库，无法永久保存数据，作用是给实例中的各种请求处理中间数据，分为主数据文件（.mdf）、次要数据文件（.ndf）和日志文件（.ldf）。当服务重启的时候，tempdb会被重新创建。

tempdb数据库如果在设计上存在缺陷，会存在性能上的问题。尤其是tempdb数据库在一些高并发的场景，如果应用频繁地创建和销毁临时表，会导致实例卡顿从而影响业务。

微软官方建议将临时数据库的文件拆分成多个，一般与逻辑CPU个数相同，超过8个则使用8个数据文件，解决闩锁争用问题每次额外加4个文件。

更多介绍请参见**tempdb数据库官方文档**。

使用限制

- 云数据库 RDS for SQL Server的2008、2012、2014实例默认是1个临时数据文件，2016实例默认4个临时数据文件，2017实例默认8个临时数据文件。
- 云数据库 RDS for SQL Server所有版本只有一个日志文件。

应用场景

您需要根据实例实际规格和具体场景确定tempdb文件的创建个数。下面将以32U的SQL Server 2014EE实例为例创建8个临时数据文件。

前提条件

- 访问**Microsoft网站**，获取SQL Server Management Studio的安装包。双击安装包，按照向导完成安装。
- 在关系型数据库服务创建一个32U的SQL Server 2014EE实例，请参见**创建SQL Server实例**。

操作步骤

步骤1 启动SQL Server Management Studio客户端。

步骤2 选择“连接 > 数据库引擎”，在“连接到服务器”弹出框中填选登录信息。

图 4-7 连接到服务器

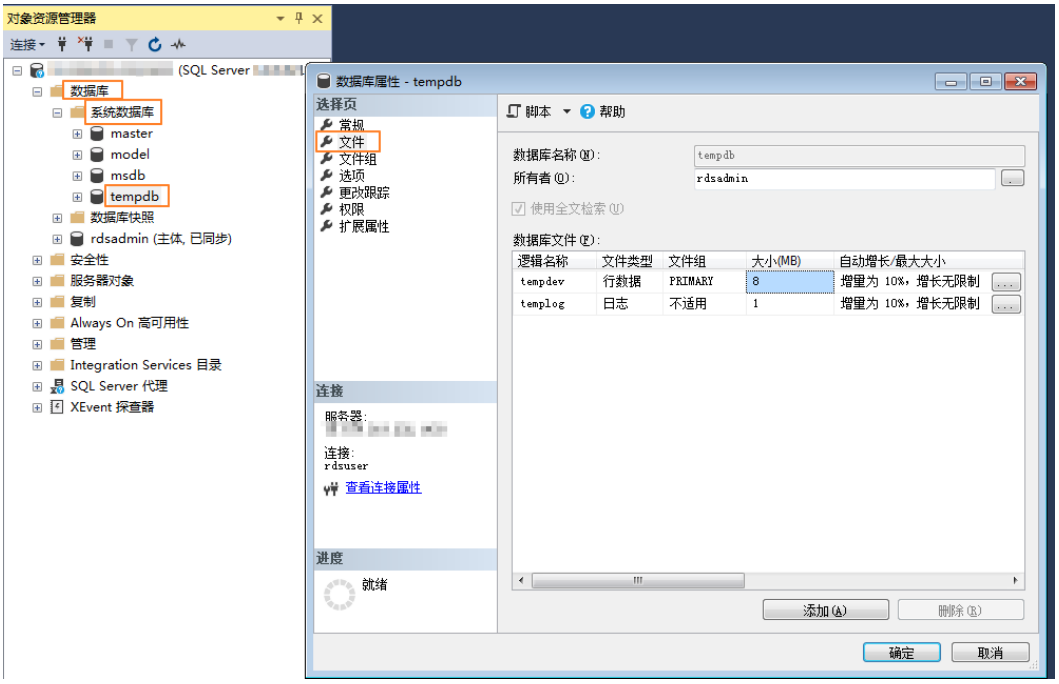
表 4-6 参数说明

参数	说明
服务器名称	目标实例的主机IP和数据库端口（IP和数据库端口之间请使用英文半角逗号）。例如：x.x.x.x,8080 ● 主机IP为已绑定的弹性公网IP地址。 ● 端口为“连接管理”页签中的“数据库端口”。
身份验证	认证方式，选择“SQL Server身份验证”。
登录名	待访问的数据库账号，默认管理员账号为rdsuser。
密码	待访问的数据库账号对应的密码。

步骤3 查看当前tempdb信息。

- 选择“数据库 > 系统数据库 > 临时数据库”，右键单击“属性”，在弹出框中选择“文件”，查看当前tempdb信息。

图 4-8 查看当前 tempdb 信息



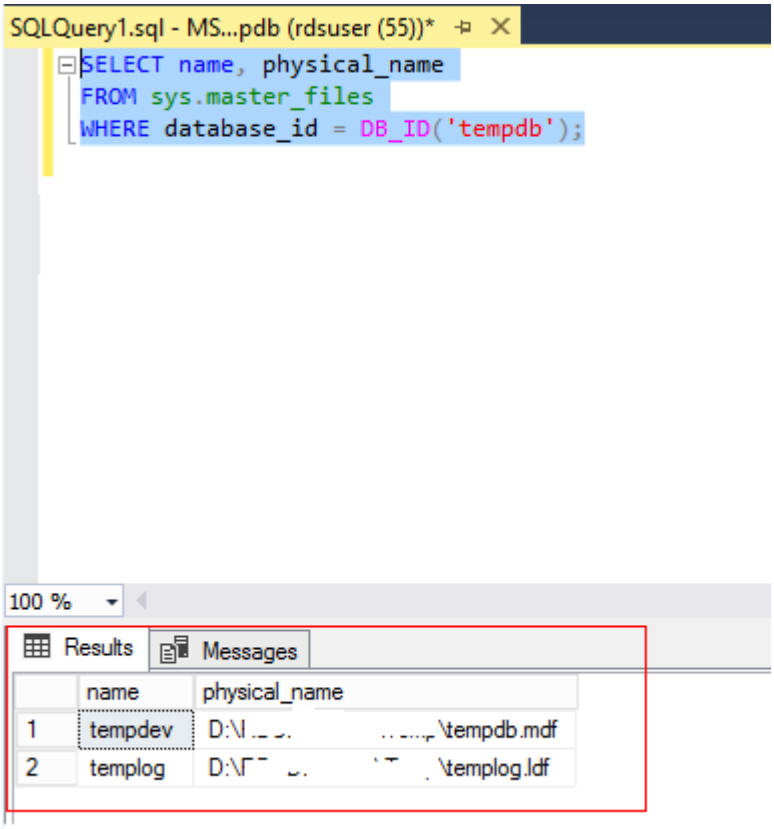
- 通过SQL语句查询。

  ```
  SELECT name AS FileName,
  size*1.0/128 AS FileSizeInMB,
  CASE max_size
  WHEN 0 THEN 'Autogrowth is off.'
  WHEN -1 THEN 'Autogrowth is on.'
  ELSE 'Log file grows to a maximum size of 2 TB.'
  END,
  growth AS 'GrowthValue',
  'GrowthIncrement' =
  CASE
  WHEN growth = 0 THEN 'Size is fixed.'
  WHEN growth > 0 AND is_percent_growth = 0
  THEN 'Growth value is in 8-KB pages.'
  ELSE 'Growth value is a percentage.'
  END
  FROM tempdb.sys.database_files;
  GO
  ```

步骤4 使用如下语句查看当前实例的tempdb的逻辑文件名称。

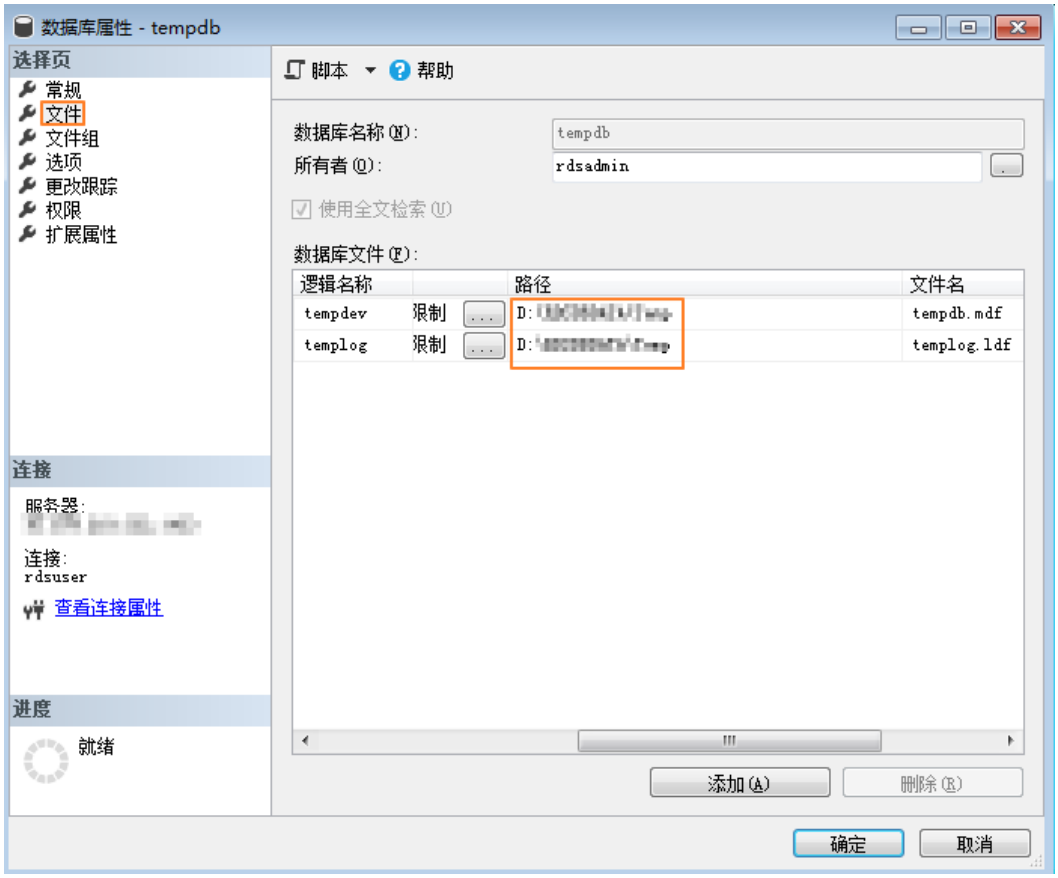
```
SELECT name, physical_name
FROM sys.master_files
WHERE database_id = DB_ID('tempdb');
```

图 4-9 查看 tempdb



步骤5 在步骤3的“文件”页签下查看tempdb在磁盘上的当前位置。

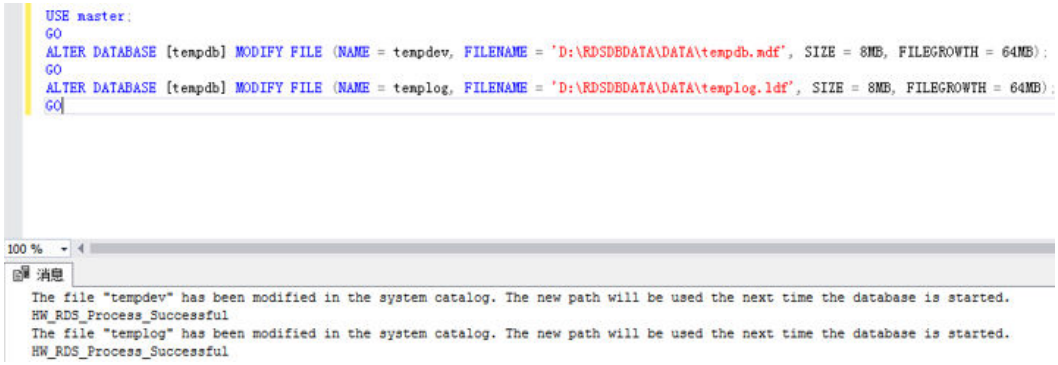
图 4-10 查看当前位置



步骤6 使用如下语句将tempdb文件迁移到D盘RDSDBDATA文件夹的DATA目录下，根据实际需要指定初始大小和增长速度。

```
USE master;
GO
ALTER DATABASE [tempdb] MODIFY FILE (NAME = tempdev, FILENAME = 'D:\RDSDBDATA\DATA\tempdb.mdf', SIZE = 8MB, FILEGROWTH = 64MB);
GO
ALTER DATABASE [tempdb] MODIFY FILE (NAME = templog, FILENAME = 'D:\RDSDBDATA\DATA\templog.ldf', SIZE = 8MB, FILEGROWTH = 64MB);
GO
```

图 4-11 迁移文件



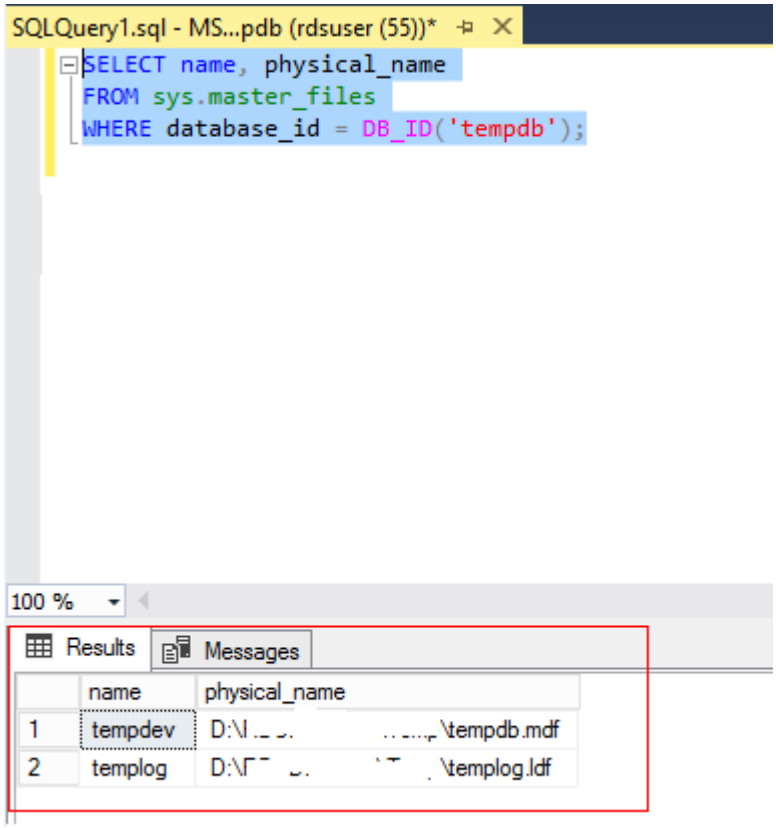
步骤7 在“实例管理”页面，选择指定的主实例，单击“更多 > 重启实例”。

您也可以在“实例管理”页面，单击目标实例名称，在页面右上角，单击“重启实例”。

步骤8 使用如下SQL语句查询文件是否迁移成功。

```
SELECT name, physical_name
FROM sys.master_files
WHERE database_id = DB_ID('tempdb');
```

图 4-12 查看 tempdb



步骤9 根据实际需要配置文件名、初始大小、增长速度等信息，通过如下SQL语句或界面增加tempdb的文件数。

- 通过如下SQL语句增加tempdb的文件数。

  -- 根据CPU的数量增加tempdb文件数、初始大小和增长速度分别为8MB和64MB

  USE [master]

  GO

  ALTER DATABASE [tempdb] ADD FILE (NAME = N'temp2', FILENAME = N'D:\RDSDBDATA\DATA\tempdb2.ndf', SIZE = 8MB, FILEGROWTH = 64MB)

  GO

  ALTER DATABASE [tempdb] ADD FILE (NAME = N'temp3', FILENAME = N'D:\RDSDBDATA\DATA\tempdb3.ndf', SIZE = 8MB, FILEGROWTH = 64MB)

  GO

  ALTER DATABASE [tempdb] ADD FILE (NAME = N'temp4', FILENAME = N'D:\RDSDBDATA\DATA\tempdb4.ndf', SIZE = 8MB, FILEGROWTH = 64MB)

  GO

  ALTER DATABASE [tempdb] ADD FILE (NAME = N'temp5', FILENAME = N'D:\RDSDBDATA\DATA\tempdb5.ndf', SIZE = 8MB, FILEGROWTH = 64MB)

  GO

  ALTER DATABASE [tempdb] ADD FILE (NAME = N'temp6', FILENAME = N'D:\RDSDBDATA\DATA\tempdb6.ndf', SIZE = 8MB, FILEGROWTH = 64MB)

  GO

  ALTER DATABASE [tempdb] ADD FILE (NAME = N'temp7', FILENAME = N'D:\RDSDBDATA\DATA\tempdb7.ndf', SIZE = 8MB, FILEGROWTH = 64MB)

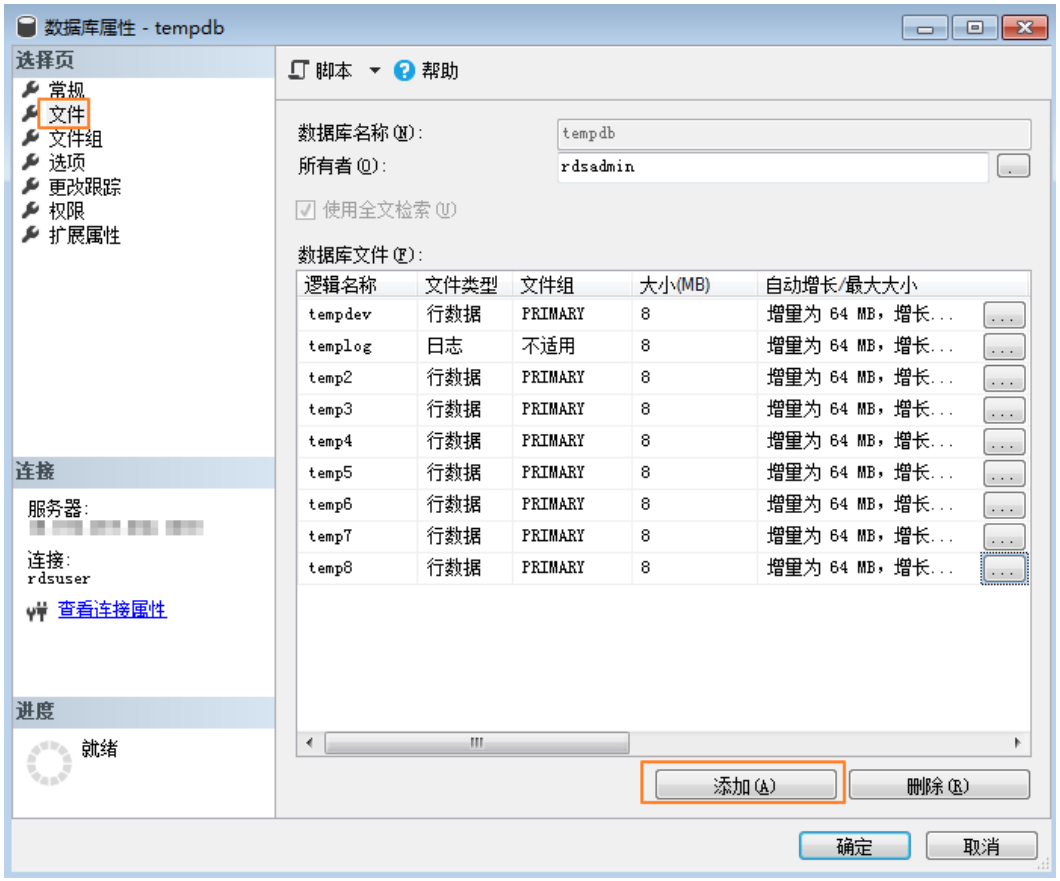
  GO

  ALTER DATABASE [tempdb] ADD FILE (NAME = N'temp8', FILENAME = N'D:\RDSDBDATA\DATA\tempdb8.ndf', SIZE = 8MB, FILEGROWTH = 64MB)

  GO

- 在**步骤3**的“文件”页签，单击“添加”，增加tempdb的文件数。

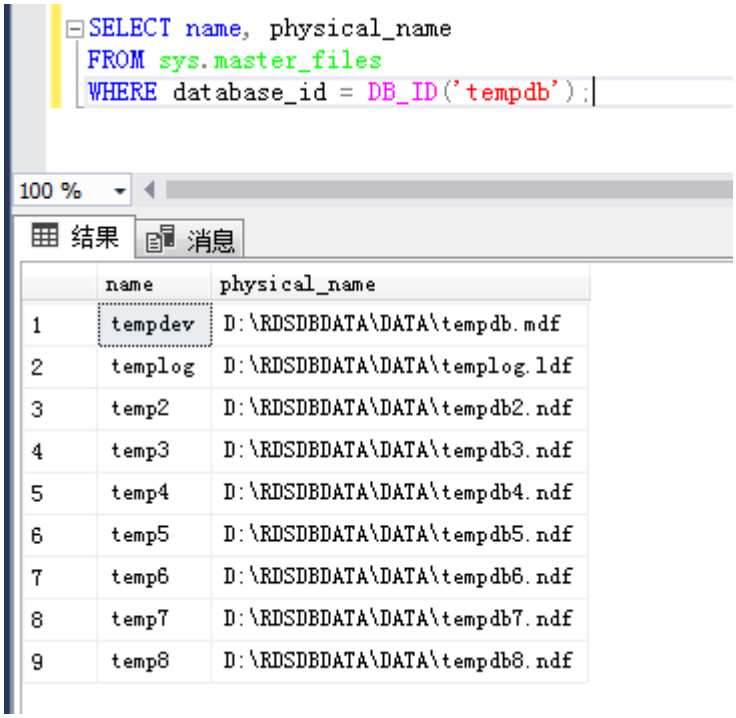
图 4-13 添加 tempdb 文件



步骤10 配置完成后，请参考**步骤7**再次重启实例。

步骤11 重复**步骤8**，验证文件是否增加成功。

图 4-14 查看 tempdb 信息



	name	physical_name
1	tempdev	D:\RDSDBDATA\DATA\tempdb.mdf
2	templog	D:\RDSDBDATA\DATA\templog.ldf
3	temp2	D:\RDSDBDATA\DATA\tempdb2.ndf
4	temp3	D:\RDSDBDATA\DATA\tempdb3.ndf
5	temp4	D:\RDSDBDATA\DATA\tempdb4.ndf
6	temp5	D:\RDSDBDATA\DATA\tempdb5.ndf
7	temp6	D:\RDSDBDATA\DATA\tempdb6.ndf
8	temp7	D:\RDSDBDATA\DATA\tempdb7.ndf
9	temp8	D:\RDSDBDATA\DATA\tempdb8.ndf

----结束

4.8 Microsoft SQL Server 发布与订阅

Microsoft SQL Server提供的发布与订阅功能，利用复制技术来实现数据同步，可以通过其提供的发布与订阅功能实现数据的读写分离和线下线上数据同步。

本章节提供使用SQL Server Management Studio（SSMS）配置发布与订阅的方法。RDS for SQL Server支持在界面创建发布和订阅，详见**创建发布**。

准备工作

环境说明：

1. 本地环境：windows系统，Microsoft SQL Server 2014 SE标准版。
2. 线上环境：
   - 华为云 Microsoft SQL Server 2014 SE 单机实例 2u16g规格 1个，绑定弹性公网EIP。
   - 华为云 Microsoft SQL Server 2014 SE 主备实例 4u8g规格 1个，绑定弹性公网EIP。

环境搭建

- 发布服务器（Publisher）：数据写入源头，维护源数据，决定将特定数据分发到分发服务器（Distributor），此处即为本地环境构建的服务器。
  a. 使用SQL Server Management Studio（SSMS）配置发布服务器，以sa身份登录本地数据库。单击右键“复制”，选择“配置分发”，可以将自己作为分发服务器，也可以选择配置其他服务器作为分发服务器，单击“下一步”。

须知

- sa为管理员账号。
- 登录的账户必须具有**sysadmin**权限，否则无法配置发布和订阅。

b. 指定快照文件夹的根位置并记录，单击“下一步”。

说明

发布需要配置相关的代理权限，以供代理账户有权限操作该文件夹，否则会导致发布失败。

c. 选择分发数据库和日志文件的名称及位置，单击“下一步”。

d. 使服务器能够成为发布服务器后使用此分发服务器，单击“下一步”。

e. 单击“完成”，执行此配置操作。

- 配置代理账户控制文件。

a. 根据快照文件夹目录地址，需要将***agent代理账户***加入到该文件的控制属性。未加入该账户到文件控制会出现拒绝访问路径的报错信息：

b. 打开本地SQLSERVER配置管理器，找到对应代理，右键单击选择“属性”，复制“account name”。

c. 返回设置的快照文件夹的目录，右键单击文件夹选择“属性”，在弹出框中选择“安全 > 编辑 > 添加”，选择位置为本地，名称为代理账户名称，单击“确定”，勾选所有权限设置即可。

- 分发服务器（Distributor）：数据分发源，负责具体执行发送到哪个订阅服务器。将分发和发送服务器都指定为本地服务器，即发送和分发为同一服务器。因而无需再做多余设置。更多设置信息可参考官方文档**分发服务器**。
- 订阅服务器（Subscriber）：数据接收服务器，数据读取的源头，接收端，用于接收分发服务器发送的指定数据。订阅分为推送订阅和请求订阅。
  - **推送订阅**：发布服务器将更改传播到订阅服务器，而无需订阅服务器发出请求，数据将连续同步或按照经常重复执行的计划同步。
  - **请求订阅**：订阅服务器主动请求订阅，数据通常按需或按计划同步，而非连续同步。华为云实例不支持请求订阅，因而需要此处设置为推送订阅，仅需在发送服务器端设置即可实现订阅。

在订阅前需要确保服务器间网络互通，可以在本地服务器上访问云上实例。

配置本地端订阅之前，需要将云上信息配置在本地。

a. 为订阅服务器在本地服务器上设置别名。由于订阅服务**不支持IP访问**，因此需要将RDS实例的公网IP映射为别名。别名不可随意取名，需先登录RDS实例后，执行以下SQL语句。

```
select  @@SERVERNAME
```

b. 得到别名名称，打开本地sqlserver配置管理器选择“native client”，右键单击“Aliases”，选择“new Aliases”。

c. 填写相关信息，单击“确认”。

表 4-7 参数说明

参数	说明
Alias Name	a中设置的别名。

参数	说明
Port No	对应实例的端口号。
Server	绑定的公网IP。

d. 配置本地host。在**C:\Windows\System32\drivers\etc**中，打开host文件并添加一条映射：
Server地址 MSSQL-177FFD84\MSSQL2014STD

发布

步骤1 创建发布。

展开服务器下的“复制”节点，右键单击“本地发布”，选择“新建发布”。

步骤2 选择事务发布。

步骤3 选择以表作为发布对象。

步骤4 添加筛选对象，进行个性化的发布。

步骤5 事务发布会先创建一个快照以复制表当前的状态。也可以设置快照代理用以执行计划。

步骤6 设置代理安全性，这里需要设置登录账号为本地sa账号。

步骤7 设置发布名称，单击“完成”。

步骤8 创建完成后可以通过**复制监视器**来查看是否创建发布成功。

----结束

订阅

步骤1 选择对应设置的发布，单击右键选择“新建订阅”。

步骤2 创建订阅的发布，单击“下一步”。

步骤3 选择推送订阅，单击“下一步”。

步骤4 选择“添加订阅服务器”，支持SQL Server引擎和非SQL Server作为订阅服务器，将创建并根据上述步骤配置的华为云实例作为一个订阅服务器。

步骤5 选择一个数据库作为订阅对象。

步骤6 配置与订阅服务器的连接。

步骤7 使用一个长期有效的数据库账号，保障订阅长期有效，这里的账号设置可以为登录华为云实例的数据库账号，单击“确定”。

步骤8 创建订阅成功。

步骤9 将鼠标移动到发布配置上可以看到对应的订阅信息。

----结束

4.9 RDS for SQL Server 添加 c#CLR 程序集的使用方法

SQL Server提供程序集，可以更加便捷的操作数据库数据。

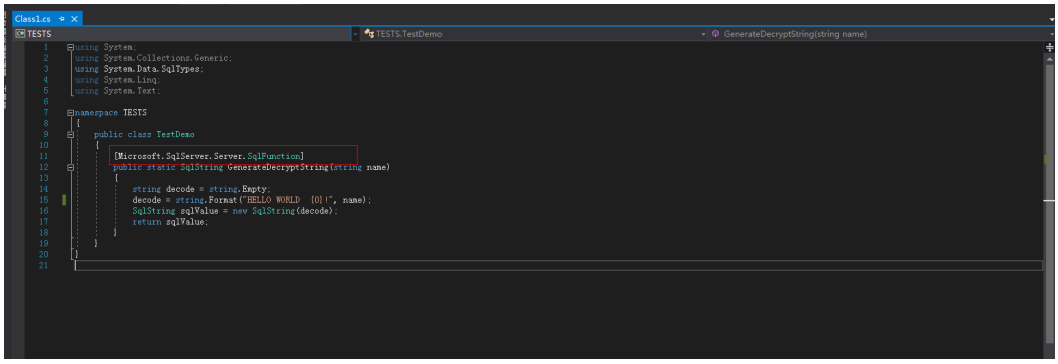
说明

当您将数据库实例恢复到新实例或已有实例，“clr enabled”参数默认不开启，需要重新开启，才可以正常使用CLR集成功能。启用CLR集成功能请参考**开启CLR集成功能**。

操作步骤

步骤1 创建c#函数，编译出一个SQL Server的dll。

图 4-15 c#函数代码



须知

创建函数详细说明请参见**官方文档**。

步骤2 使用**SSMS**等工具连接数据库。

图 4-16 连接数据库

步骤3 选择需要创建程序集的数据库，添加对应的程序集。

说明

- 只能创建safe模式（权限集显示为安全），不能创建其他模式。
- **dll**文件会以十六进制的形式存入。如图4-18所示。

图 4-17 新建程序集

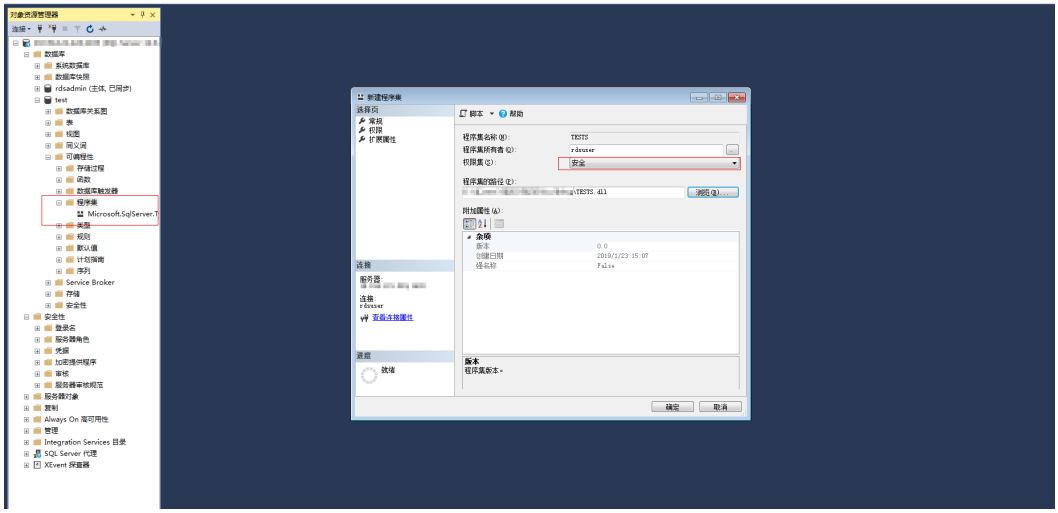


图 4-18 dll 文件

步骤4 执行程序，如图4-19所示表示执行成功。程序集中新增一个TESTS程序集，如图4-20所示。

图 4-19 执行结果

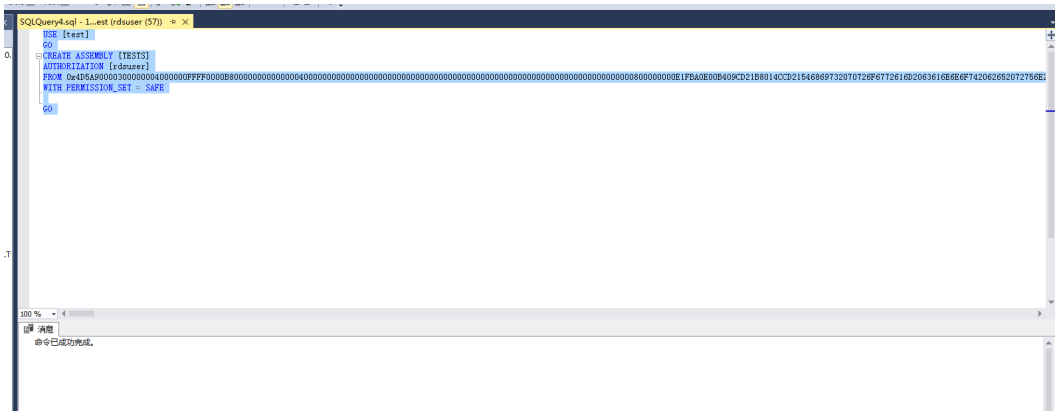
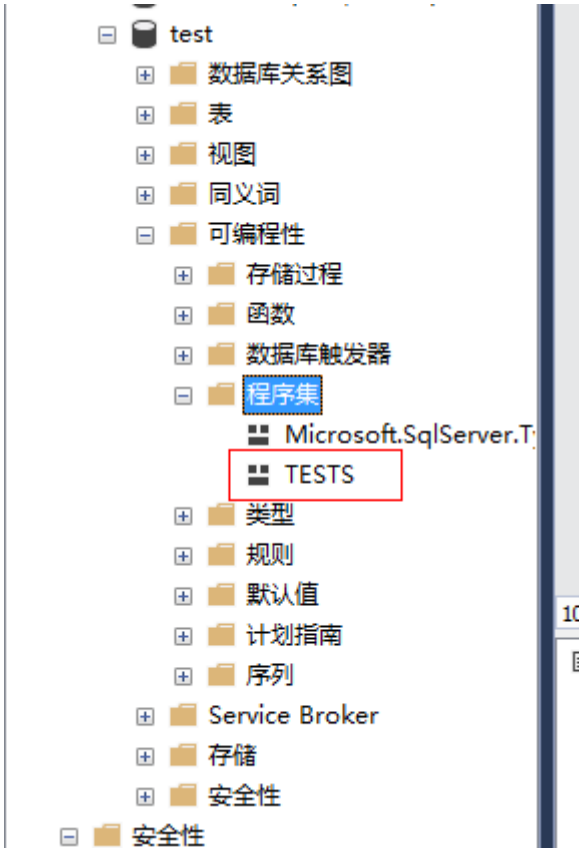


图 4-20 TESTS 程序集



----结束

4.10 RDS for SQL Server 添加链接服务器

SQL Server数据库实例2创建链接服务器访问另外一个SQL Server数据库实例1。

步骤1 开启两个实例的分布式事务，请参考**开启分布式事务**，并且互相加入对端的host信息。线下服务器或ECS服务器请参考**远程服务器上的名称解析**。

说明

SQL Server数据库实例2和SQL Server数据库实例1已经在相同VPC内。如果ECS与RDS不在相同VPC或者RDS与线下实例建立分布式请通过EIP进行连接，请参考**绑定弹性公网IP**为RDS实例绑定EIP。

步骤2 在SQL Server实例1中使用rdsuser创建数据库dbtest1。

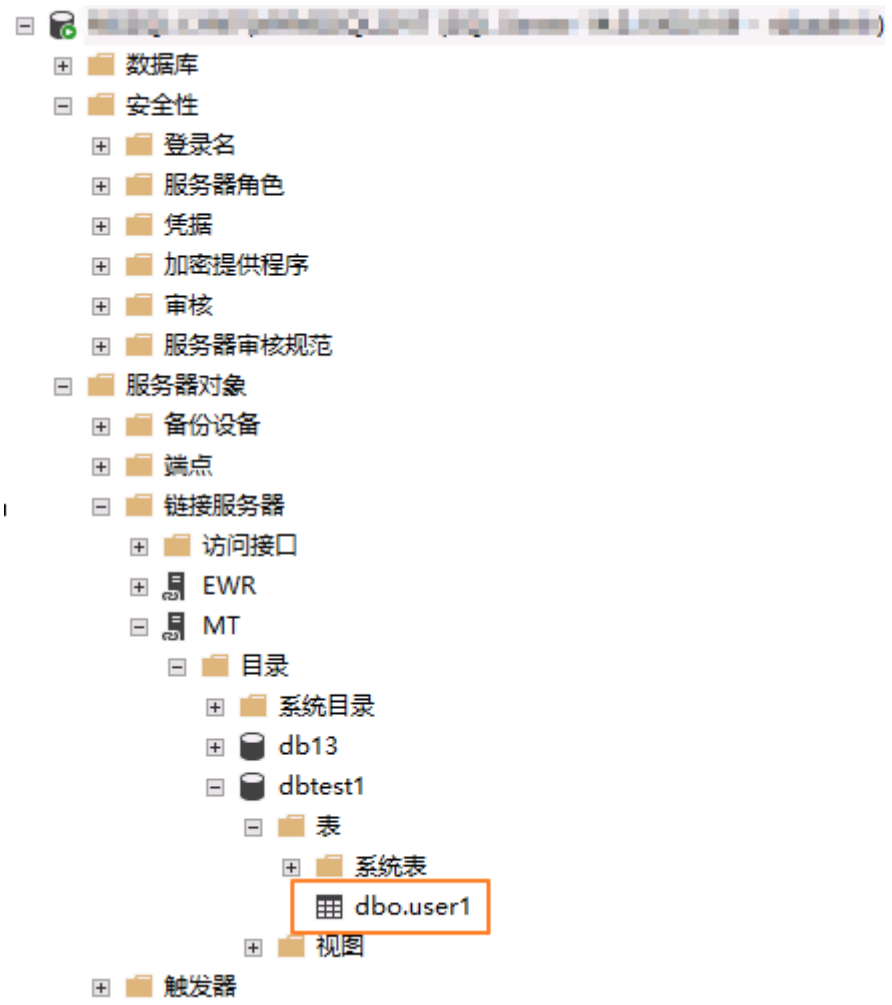
步骤3 在SQL Server实例2中使用rdsuser运行如下sql创建链接服务器。

```
USE [master]
GO
EXEC master.dbo.sp_addlinkedserver @server = N'TEST_SERVERNAME', @srvproduct=N'SQLServer',
@provider=N'SQLOLEDB', @datasrc=N'192.168.***.***,1433'
EXEC master.dbo.sp_addlinkedsrvlogin @rmtsrvname = N'TEST_SERVERNAME', @locallogin = NULL ,
@useself = N'false', @rmtuser = N'rdsuser', @rmtpassword = N'********'
GO
```

表 4-8 参数说明

参数	说明
@server	链接服务器名称。
@srvproduct	数据源的产品名称。使用默认值SQL Server。
@provider	使用该默认值。
@datasrc	要访问的实例IP和端口。
@rmtsrvname	链接服务器名称。
@locallogin	本地服务器上的登录名。默认值NULL即可。
@useself	是否通过模拟本地登录名或登录名和密码连接到链接服务器。此处填false，表示通过登录名和密码连接到链接服务器。
@rmtuser	用户名（rdsuser）。
@rmtpassword	用户密码。

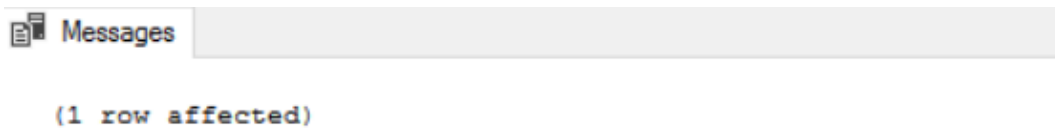
步骤4 建立dblink之后，在链接服务器中就可以看到SQL Server实例1中建立的库。



步骤5 使用如下SQL查看是否插入成功，结果如图4-21所示。

```
begin tran
set xact_abort on
INSERT INTO [LYNTEST].[dbtest1].[dbo].[user1]
([id],[lname],[rname])
VALUES('19','w’,'x')
GO
commit tran
```

图 4-21 插入结果



----结束

4.11 RDS for SQL Server 如何将线下 SSRS 报表服务部署上云

您可以借助报表服务制作各种各样的报表，无论是简单的还是复杂的报表，同时系统提供订阅功能方便用户对报表进行订阅。本文主要介绍RDS使用SSRS（Reporting Services）报表服务。

操作背景

微软的Microsoft SQL Server产品中包含SQL Server数据库引擎、Reporting Services（SSRS）、Analysis Services（SSAS）等服务端组件。其中SQL Server数据库引擎作为一个标准的关系型数据库组件，在华为云上以RDS for SQL Server数据库产品的形式提供了标准的PaaS（Platform-as-a-Service）服务。但其他如SSRS等组件在华为云上并未以PaaS服务的形式提供。如果要在华为云上使用SSRS服务，需要单独创建Windows系统的ECS实例，并安装配置SSRS服务组件。

原微软SQL Server产品组件包中的SQL Server Reporting Services已经在SQL Server 2017中独立出来，成为一个独立的组件服务，用户可通过微软官网直接下载，并安装到华为云的ECS Windows系统上，同时将RDS for SQL Server服务作为该SSRS报表服务的后端数据库，完美的做到将SSRS报表服务迁移上云。

前提条件

- 已成功**创建RDS for SQL Server实例**。
- 已成功创建Windows系统的ECS实例（ECS实例与RDS实例必须处于同一VPC、安全组、子网内）。

操作步骤

步骤1 在ECS实例上**下载Reporting Services**并按照向导完成安装。

步骤2 安装完成后单击“配置报表服务器”。

步骤3 在Report Server Configuration Manager软件中，确认报表服务器名称并单击“连接”。

步骤4 在左侧导航栏根据您的业务情况设置“服务账户”和“WEB服务URL”。

说明

详细设置请参见**官方文档**。

步骤5 配置报表服务器。

1. 在左侧导航栏选择“数据库”，单击“更改数据库”，在ECS实例上创建新的报表服务器数据库。
2. 在“更改数据库”弹框中，选择“创建新的报表服务器数据库”，单击“下一步”。

   如果有本地报表数据库，可以通过**DRS备份迁移服务**，将本地报表数据库的全备文件先迁移到目标RDS for SQL Server实例上。

3. 完善远程RDS for SQL Server实例连接信息。服务器名称请填写RDS for SQL Server的地址，格式为**ip,port**，ip和port之间用逗号分隔，账号请填写“rdsuser"。单击“测试连接”，测试连接通过后单击“下一步”。
4. 输入报表服务器数据库名称并选择脚本使用的语言，单击“下一步”。
5. 设置账户连接报表服务器rdsuser用户的凭据，单击“下一步”。
6. 确认新创建的报表服务器信息，单击“下一步”。
7. 等待报表服务器数据库配置完成后，单击“完成”。

说明

更多详细设置说明请参见**官方文档**。

步骤6 在左侧导航栏选择“WEB门户URL”，单击“应用”，等待应用完成后单击“URL”登录报表服务器的WEB管理页面。

步骤7 在右上角选择“新建 > 数据源”。

步骤8 设置新建数据源的各项参数，如下表所示。

表 4-9 新建数据源的各项参数说明

类别	参数	说明
属性	名称	新建数据源的名称。不能包含以下任何字符：/ @ $ & * + = < > : ' , ? | \
	说明	数据源的描述，便于进行业务区分。
	隐藏此项	勾选后会隐藏此数据源。
	启用此数据源	勾选后会启用此数据源。
连接	类型	数据源类型。选择Microsoft SQL Server。
	连接字符串	RDS for SQL Server实例的域名和数据库名。 格式：Data Source=<RDS for SQL Server实例内网IP地址，RDS for SQL Server实例端口>; Initial Catalog=<数据库名>
登录	登录数据源	选择“使用以下凭据”。
	凭据类型	选择“数据库用户名和密码”。
	用户名	RDS for SQL Server实例的数据库账号。
	密码	RDS for SQL Server实例的数据库账号对应的密码。

步骤9 单击“测试连接”，测试连接成功后单击“创建”。

步骤10 数据源创建完成后您可以使用Report Builder、Visutal Studio等软件设计报表。

详情请参见**Report Builder in SQL Server**。

----结束

4.12 RDS for SQL Server 收缩数据库

操作场景

云数据库 RDS for SQL Server提供使用存储过程收缩指定数据库的数据文件和日志文件的大小，以释放磁盘部分空间。

前提条件

成功连接RDS for SQL Server实例。通过SQL Server客户端连接目标实例，具体操作请参见**通过公网连接SQL Server实例**。

功能限制

- 数据库文件大小超过50MB，才可以使用该功能。如果要收缩的数据库文件大小不超过50MB，对该文件的收缩将不起作用。并且会显示相关提示。如下图所示：

  ```
  Cannot shrink file '2' in database 'master' to 6400 pages as it only contains 2
  ```

- 基于行版本控制的隔离级别下运行的事务可能会阻止收缩操作。若要解决此问题，请执行下列操作之一：
  a. 终止阻止收缩操作的事务。
  b. 终止收缩操作。 如果收缩操作终止，所有已完成的工作都会保留。
  c. 不执行任何操作，并允许收缩操作等到阻塞事务完成。

最佳实践

在计划收缩数据库文件时，请考虑以下信息：

- 在执行会产生大量未用空间的操作（如重启）后，执行收缩操作最有效。
- 大多数数据库都需要一些可用空间，以供常规日常操作使用。如果反复收缩数据库，并且它的大小再次增长，那么常规操作可能需要收缩空间。在这种情况下，反复收缩数据库是一种无意义的操作。
- 收缩操作不保留数据库中索引的碎片状态，通常还会在一定程度上增加碎片。此类碎片是不要反复收缩数据库的另一个原因。

操作步骤

步骤1 执行以下命令，进行数据库收缩。

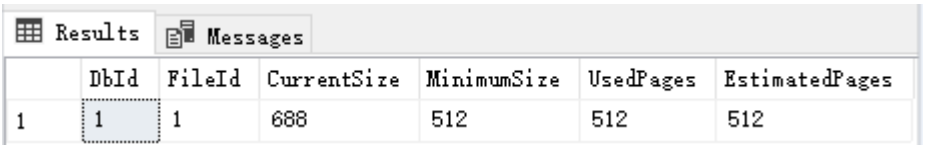
EXEC [master].[dbo].[rds_shrink_database] @DBName='*myDbName***';**

表 4-10 参数说明

参数	说明
myDbName	收缩指定数据库的数据库名称。如果未指定，默认收缩所有数据库。

执行结果集如下图所示，每个结果对应指定数据库（或所有数据库）的每个文件的相关信息。

图 4-22 结果集



	DbId	FileId	CurrentSize	MinimumSize	UsedPages	EstimatedPages
1	1	1	688	512	512	512

表 4-11 结果集参数说明

列名称	说明
DbId	当前收缩文件的数据库标识号。
FileId	当前收缩文件的文件标识号。
CurrentSize	文件当前占用的8KB页数。
MinimumSize	文件最低可以占用的8KB页数。此数字对应于文件的大小下限或最初创建大小。
UsedPages	文件当前使用的8KB页数。
EstimatedPages	数据库引擎估计文件能够收缩到的8KB页数。

步骤2 执行成功后，系统会显示执行进度，并最终进行如下提示：

```
HW_RDS_Process_Successful: Shrink Database Done.
```

----结束

故障排除

如果在执行数据库收缩后文件大小未改变，请执行以下SQL，验证文件是否有足够的可用空间：

```
SELECT name, size/128.0 - CAST(FILEPROPERTY(name, 'SpaceUsed') AS int)/
128.0 AS AvailableSpaceInMB FROM sys.database_files;
```

示例

1. 执行以下命令，对dbtest2数据库进行收缩。

   ```
   EXEC [master].[dbo].[rds_shrink_database] @DBName = 'dbtest2';
   ```

   执行结果如下图所示：

图 4-23 执行结果

```
[Shrink Start] Date and time: 2020-03-19 15:51:07

Start to shrink files in database [dbtest2], current file id is 1...
DBCC execution completed. If DBCC printed error messages, contact your system administrator.
Shrink file (id: 1) in database [dbtest2] done!

Start to shrink files in database [dbtest2], current file id is 2...
DBCC execution completed. If DBCC printed error messages, contact your system administrator.
Shrink file (id: 2) in database [dbtest2] done!

[Shrink End] Date and time: 2020-03-19 15:51:08

HW_RDS_Process_Successful : Shrink Database done.
```

2. 执行以下命令，对所有数据库进行收缩。

   EXEC [master].[dbo].[rds_shrink_database];

4.13 使用 DAS 在 RDS for SQL Server 主备实例上分别创建和配置 Agent Job 和 Dblink

操作背景

数据管理服务（Data Admin Service，简称DAS），用来登录和操作云上数据库的Web服务，提供数据库开发、运维、智能诊断一站式云上数据库管理平台，方便用户使用和运维华为云数据库。DAS目前支持SQL Server主库和备库切换操作，从而为云数据库 RDS for SQL Server实例的主库和备库同步操作提供了便捷。

登录 DAS

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角的 ，选择区域。

步骤3 单击页面左上角的 ，选择“数据库 > 云数据库 RDS”，进入RDS信息页面。

步骤4 在“实例管理”页面，选择目标实例，单击操作列的“登录”，进入数据管理服务数据库登录界面。

您也可以在“实例管理”页面，单击目标实例名称，在页面右上角，单击“登录”，进入数据管理服务数据库登录界面。

步骤5 正确输入数据库用户名和密码，单击“登录”，即可进入您的数据库并进行管理。

----结束

创建 JOB 同步备库

步骤1 在主节点创建job。

在DAS管理页面，操作栏单击“SQL查询”，在msdb库下，执行创建job命令。

说明

如果在主机通过其他方式已经有job创建不执行此步骤。

```
USE [msdb]
GO
DECLARE @jobId BINARY(16)
EXEC  msdb.dbo.sp_add_job @job_name=N'hwtest',
                @enabled=1,
                @notify_level_eventlog=0,
                @notify_level_email=2,
                @notify_level_page=2,
                @delete_level=0,
                @category_name=N'[Uncategorized (Local)]',
                @owner_login_name=N'rdsuser', @job_id = @jobId OUTPUT
select @jobId
GO
EXEC msdb.dbo.sp_add_jobserver @job_name=N'hwtest', @server_name = N'*******'
GO
USE [msdb]
GO
EXEC msdb.dbo.sp_add_jobstep @job_name=N'hwtest', @step_name=N'select orders',
                @step_id=1,
                @cmdexec_success_code=0,
                @on_success_action=1,
                @on_fail_action=2,
                @retry_attempts=0,
                @retry_interval=0,
                @os_run_priority=0, @subsystem=N'TSQL',
                @command=N'select * from orders;',
                @database_name=N'test',
                @flags=0
GO
USE [msdb]
GO
EXEC msdb.dbo.sp_update_job @job_name=N'hwtest',
                @enabled=1,
                @start_step_id=1,
                @notify_level_eventlog=0,
                @notify_level_email=2,
                @notify_level_page=2,
                @delete_level=0,
                @description=N'',
                @category_name=N'[Uncategorized (Local)]',
                @owner_login_name=N'zf1',
                @notify_email_operator_name=N'',
                @notify_page_operator_name=N''
GO
```

使用如下SQL查询job是否被创建。

use [msdb]

select * from msdb.dbo.sysjobs where name ='hwtest';

步骤2 切换到备库。

说明

目前云数据库 RDS for SQL Server实例暂不支持主备库job同步，因此需要在备库同步执行job创建，同步job。在**在主节点创建job**中，我们处于主库，单击主库旁的“切换SQL执行点”，即可切换到备库。

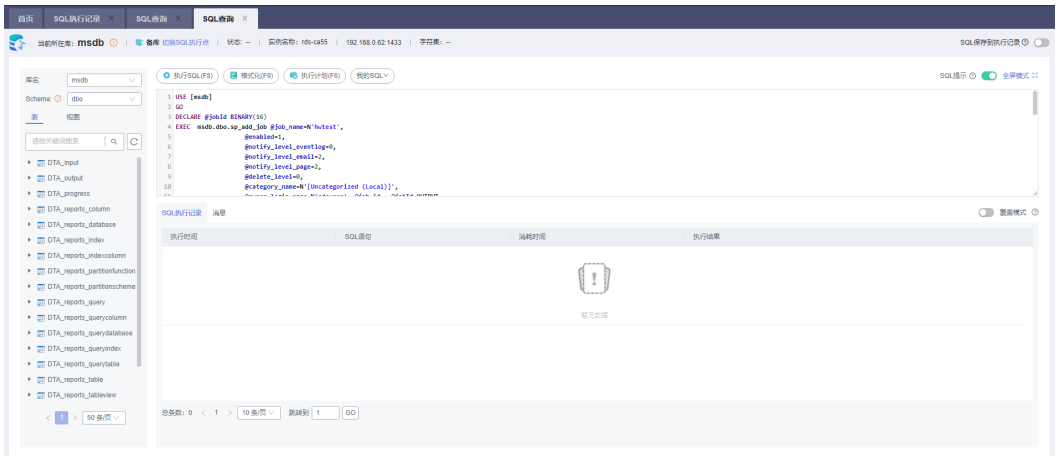
步骤3 使用**在主节点创建job**的语句在备库上创建job。

通过SQL Server Management Studio（简称：SSMS）工具导出之前创建的job到编辑窗，并复制到DAS的SQL查询窗口，执行sql即可。

若创建失败，建议先进行delete job操作后，再重新执行创建job。

图 4-24 导出 job

图 4-25 在 DAS 管理界面备库界面执行创建 job



使用如下SQL删除job命令。

USE [msdb]

GO

EXEC msdb.dbo.sp_delete_job @job_name=N'hwtest',
@delete_unused_schedule=1

GO

----结束

创建 DBLink 同步备库

通过DAS服务可以创建链接服务器，实现实例间的数据同步。

说明

请参考**RDS for SQL Server添加链接服务器**章节检查分布式事务MSDTC是否配置。

步骤1 参考如下代码在主库创建DBlink。

```
USE [master]

GO

EXEC master.dbo.sp_addlinkedserver @server = N'TEST',
@srvproduct=N'mytest', @provider=N'SQLOLEDB', @datasrc=N'abcd'

EXEC master.dbo.sp_addlinkedsrvlogin @rmtsrvname = N'TEST', @locallogin =
NULL , @useself = N'False', @rmtuser = N'rdsuser', @rmtpassword = N'********'

GO
```

创建成功后，可以连接到对应的实例或者其他数据库查看数据验证，如执行数据库查询：

```
SELECT name FROM [TEST].master.sys.databases ;

GO
```

图 4-26 数据库查询

步骤2 在备库创建DBLink。

在DAS管理界面，主库旁单击“切换SQL执行点”，同样执行创建DBLink的SQL。

说明

如果当前实例与对接的数据库不是同一VPC，或者使用公网EIP开启分布式事务，则备库上暂时无法执行查询语句，仅此步骤用于同步DBLink配置，若实例进行主备倒换后，则可以正常使用DBLink。

----结束

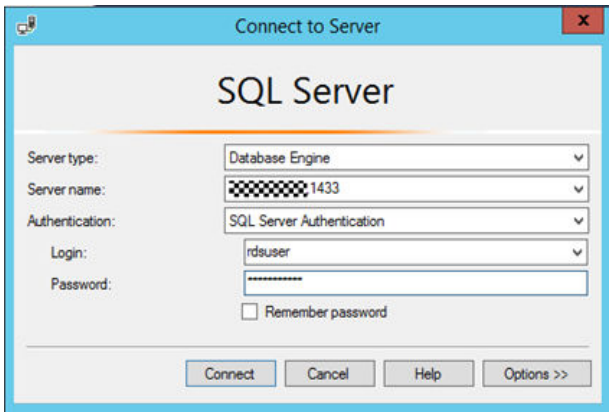
4.14 创建实例定期维护 job

操作场景

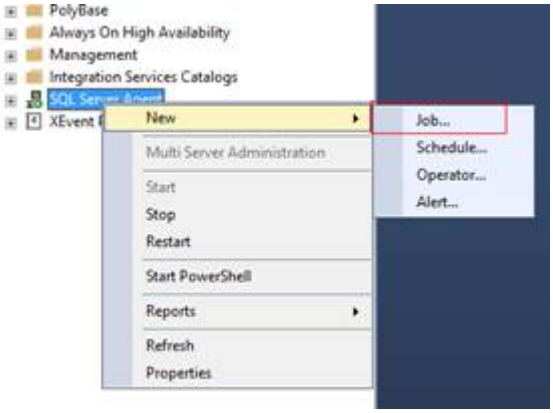
实例运行一段时间后，由于索引碎片增加，统计信息未及时更新等会导致系统性能有所下降。建议创建定期执行的SQL agent job，定期执行索引重建、统计信息更新、数据库收缩操作。

重建索引 job

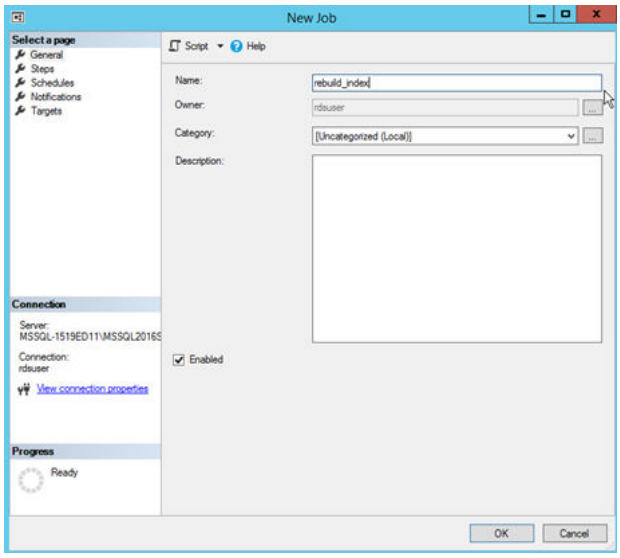
步骤1 启动SQL Server Managerment Studio客户端，使用rdsuser用户登录。



步骤2 选择“SQL Server Agent”，右键单击“New > Job”，新建SQL agent job。

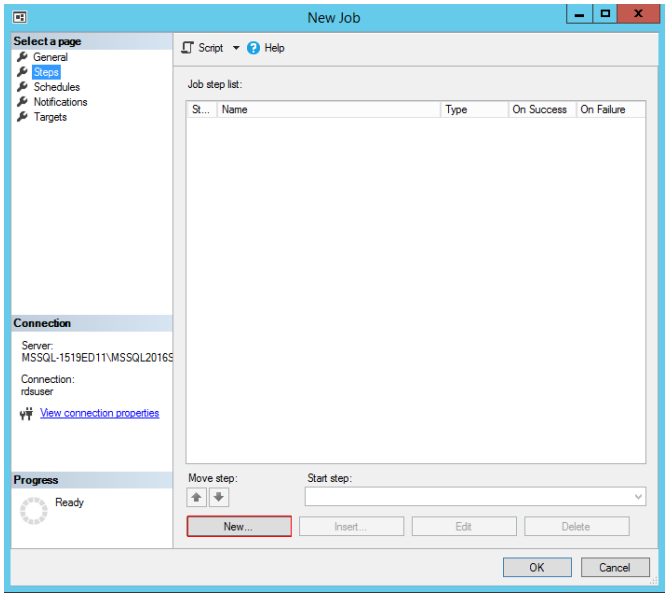


步骤3 输入名字以及描述信息，单击“OK”。



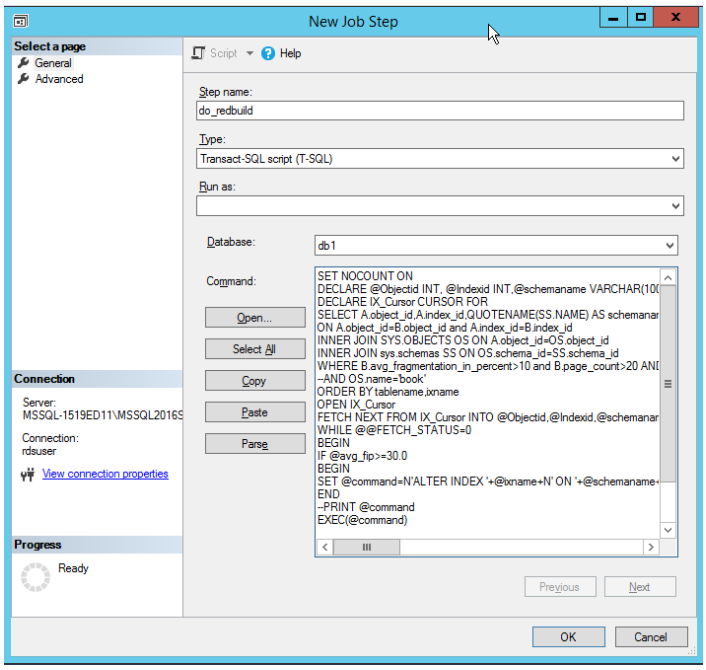
步骤4 选择“Steps”，单击“New”，添加执行步骤。

图 4-27 添加执行步骤



步骤5 输入步骤名称，类型及Command，完成后单击“OK”。Command中填写需要定时执行的SQL，当索引碎片达到一定程度，例如30%，可以进行重建。

图 4-28 步骤信息



执行以下SQL，对指定的dbname中的所有表检查索引碎片超过30%后进行重建。

```
use [dbname]
SET NOCOUNT ON
DECLARE @Objectid INT, @Indexid INT,@schemaname VARCHAR(100),@tablename
VARCHAR(300),@ixname VARCHAR(500),@avg_fip float,@command VARCHAR(4000)
DECLARE IX_Cursor CURSOR FOR
SELECT A.object_id,A.index_id,QUOTENAME(SS.name) AS
schemaname,QUOTENAME(OBJECT_NAME(B.object_id,B.database_id))as
tablename ,QUOTENAME(A.name) AS ixname,B.avg_fragmentation_in_percent AS avg_fip FROM
sys.indexes A inner join sys.dm_db_index_physical_stats(DB_ID(),NULL,NULL,NULL,'LIMITED') AS B
ON A.object_id=B.object_id and A.index_id=B.index_id
INNER JOIN sys.objects OS ON A.object_id=OS.object_id
INNER JOIN sys.schemas SS ON OS.schema_id=SS.schema_id
WHERE B.avg_fragmentation_in_percent>10 and B.page_count>20 AND A.index_id>0 AND A.is_disabled<>1
--AND OS.name='book'
ORDER BY tablename,ixname
OPEN IX_Cursor
FETCH NEXT FROM IX_Cursor INTO @Objectid,@Indexid,@schemaname,@tablename,@ixname,@avg_fip
WHILE @@FETCH_STATUS=0
BEGIN
IF @avg_fip>=30.0
BEGIN
SET @command=N'ALTER INDEX '+@ixname+N' ON '+@schemaname+N'.'+ @tablename+N' REBUILD ';
END
--PRINT @command
EXEC(@command)
FETCH NEXT FROM IX_Cursor INTO @Objectid,@Indexid,@schemaname,@tablename,@ixname,@avg_fip
END
CLOSE IX_Cursor
DEALLOCATE IX_Cursor
```

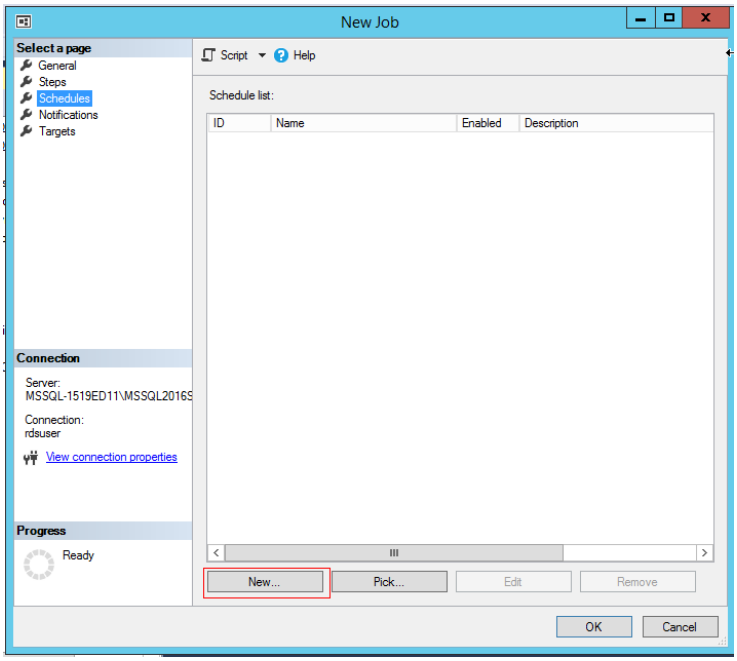
说明

上述重建的SQL只需要修改第一行（Use [dbname]），修改为指定的数据库即可。

如果需要对所有库执行，请修改SQL，添加多所有库的循环执行，此处不做详细示例。

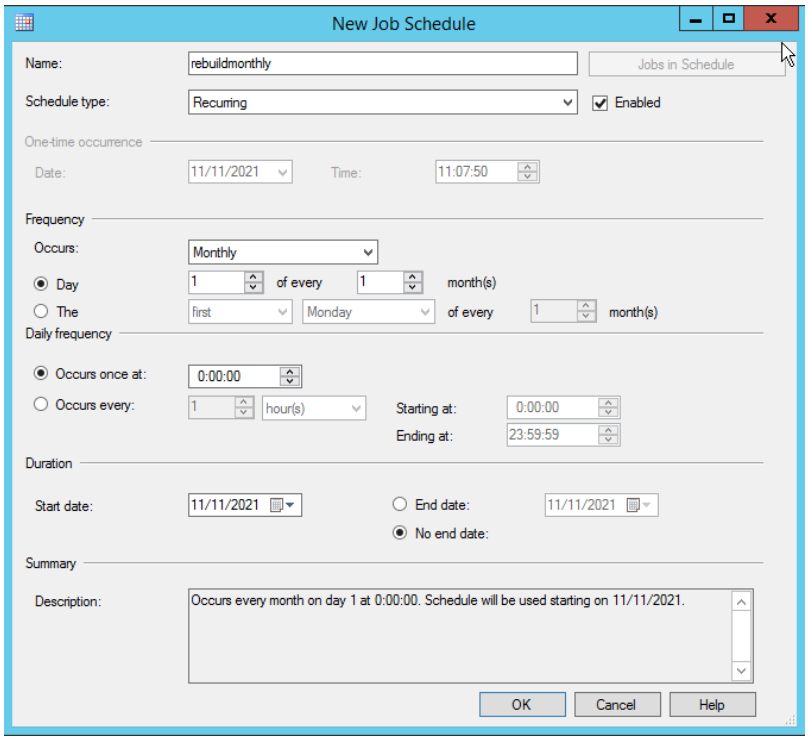
步骤6 选择“Schedules”，单击“New”，添加定时执行计划。

图 4-29 添加定时执行计划



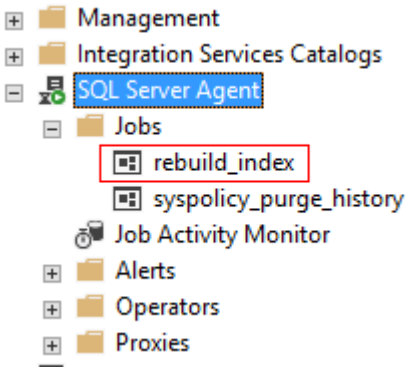
步骤7 添加每个月执行一次的定时计划，触发时间、定时周期可以修改，完成后单击“OK”。

图 4-30 定时执行计划



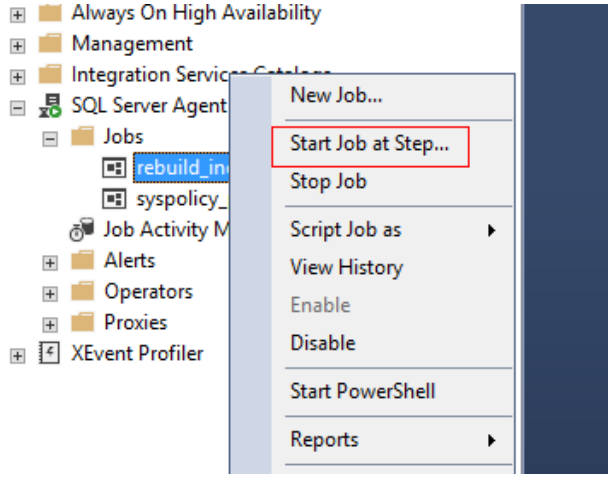
步骤8 上述步骤执行完成后，job建立完毕。

图 4-31 job

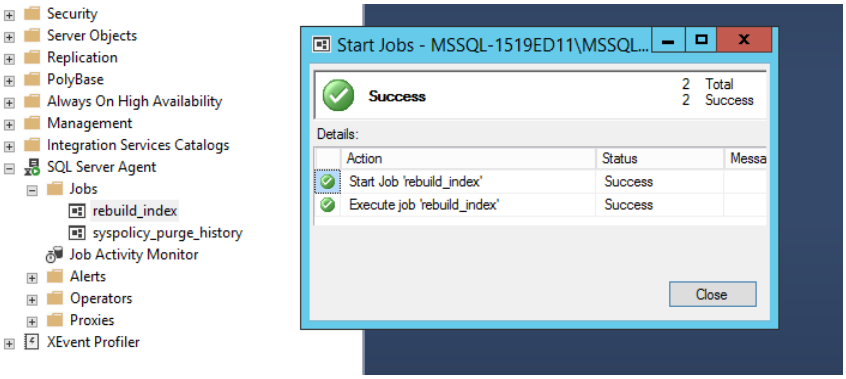


步骤9 选择job，右键单击“Start Job at Step”，手动运行job，检查job是否能正常运行。

图 4-32 运行 job



步骤10 运行正常，定时重建db1数据库的索引的维护job创建完毕。



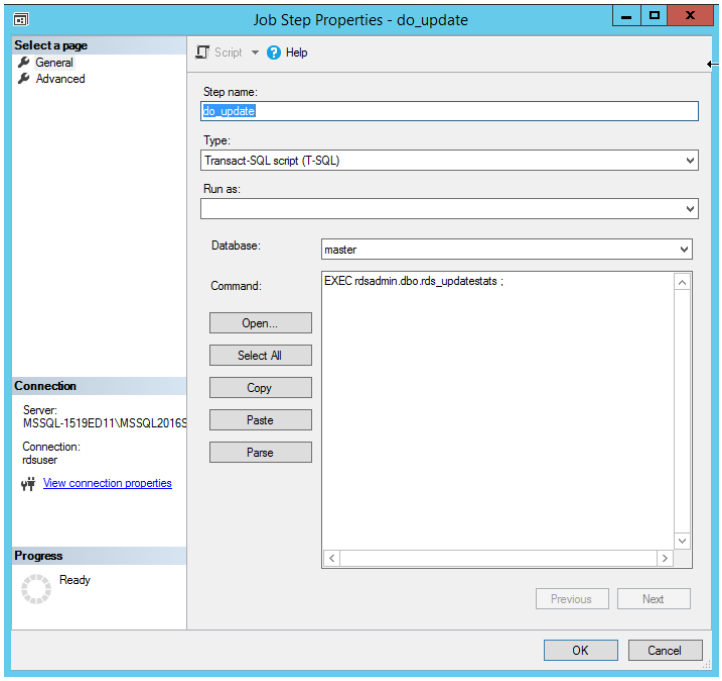
----结束

更新统计信息

步骤1 重复执行重建索引job中的**步骤1**~**步骤4**。

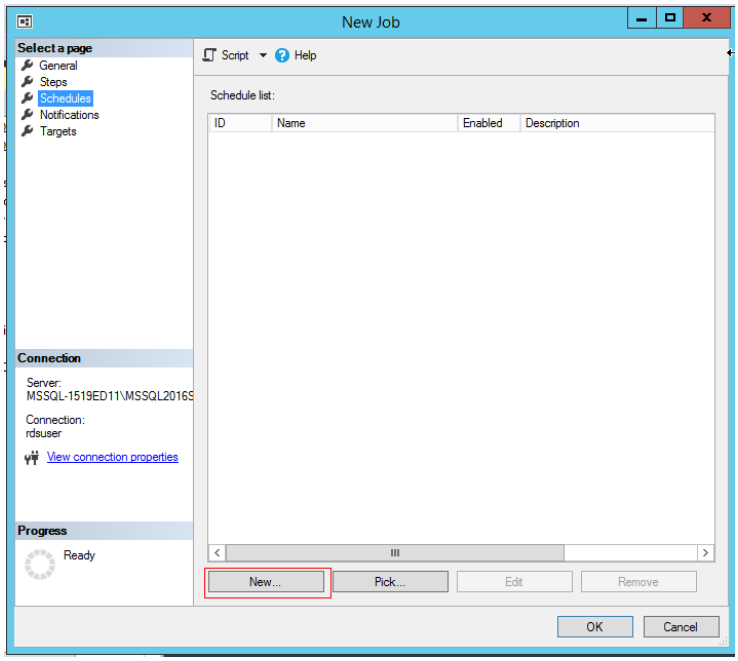
步骤2 输入步骤名称，类型及Command，完成后单击“OK”。Command中填写更新统计信息的存储过程，存储过程的详细内容请参考**更新数据库的统计信息**。

图 4-33 更新统计信息



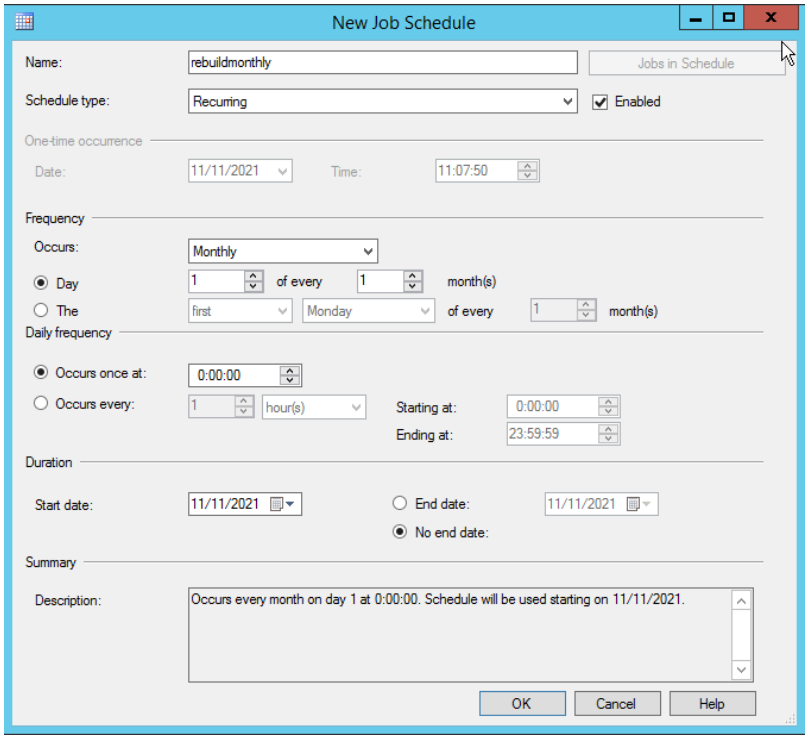
步骤3 选择“Schedules”，单击“New”，添加定时执行计划。

图 4-34 添加定时执行计划



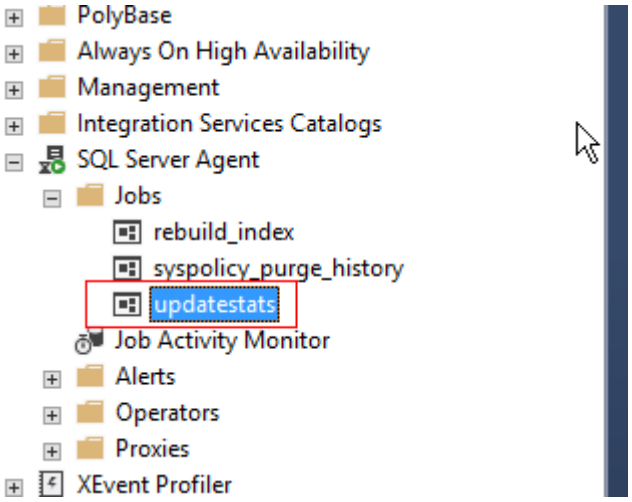
步骤4 添加每个月执行一次的定时计划，触发时间、定时周期可以修改，完成后单击“OK”。

图 4-35 定时执行计划



步骤5 上述步骤执行完成后，job建立完毕。

图 4-36 更新统计信息 job



步骤6 选择job，右键单击“Start Job at Step”，手动运行job，检查job是否能正常运行。

----结束

定时收缩数据库

步骤1 重复执行重建索引job中的**步骤1**~**步骤4**。

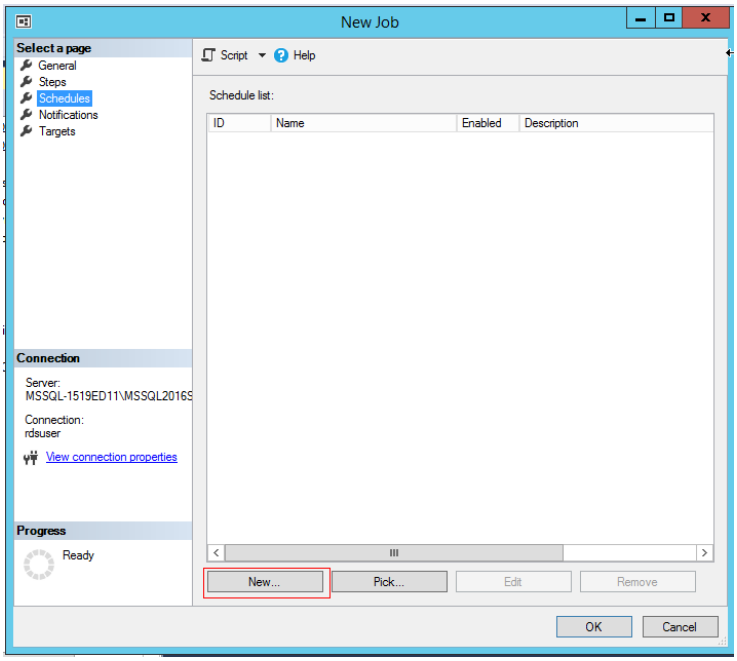
步骤2 输入步骤名称，类型及Command，完成后单击“OK”。Command中填写收缩数据库的SQL命令。

```
EXEC [master].[dbo].[rds_shrink_database_log] @dbname='myDbName';
```

其中@dbname参数填写数据库的名字。

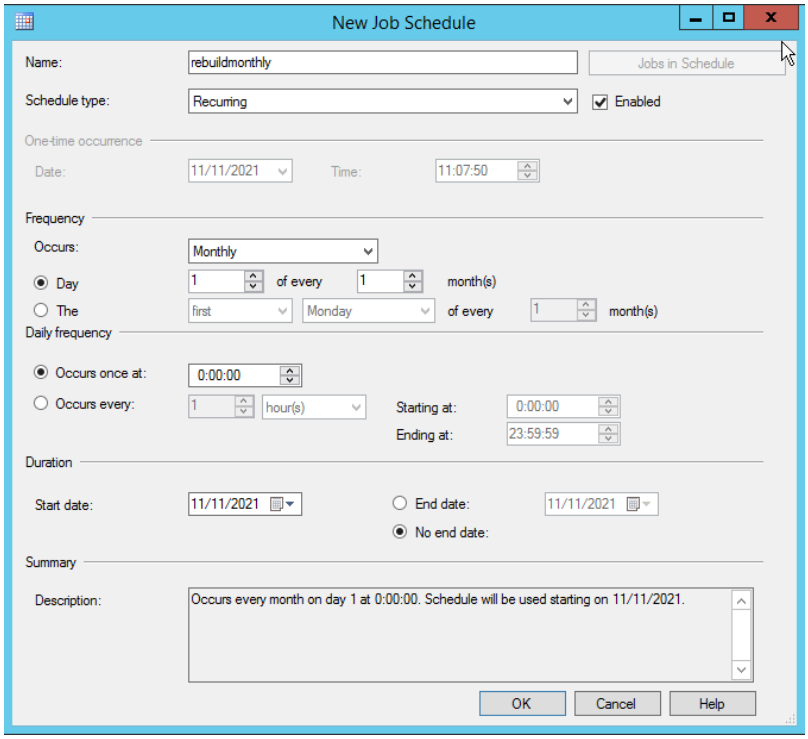
步骤3 选择“Schedules”，单击“New”，添加定时执行计划。

图 4-37 添加定时执行计划



步骤4 添加每个月执行一次的定时计划，触发时间、定时周期可以修改，完成后单击“OK”。

图 4-38 定时执行计划



步骤5 添加完成后，右键单击“Start Job at Step”，手动运行job，检查job是否能正常运行。

----结束

4.15 使用扩展事件

目前已开放扩展事件的权限，用户使用rdsuser可以对其他用户进行扩展事件授权、对扩展事件进行管理等。

更多内容，请参见**扩展事件官方指导**。

约束限制

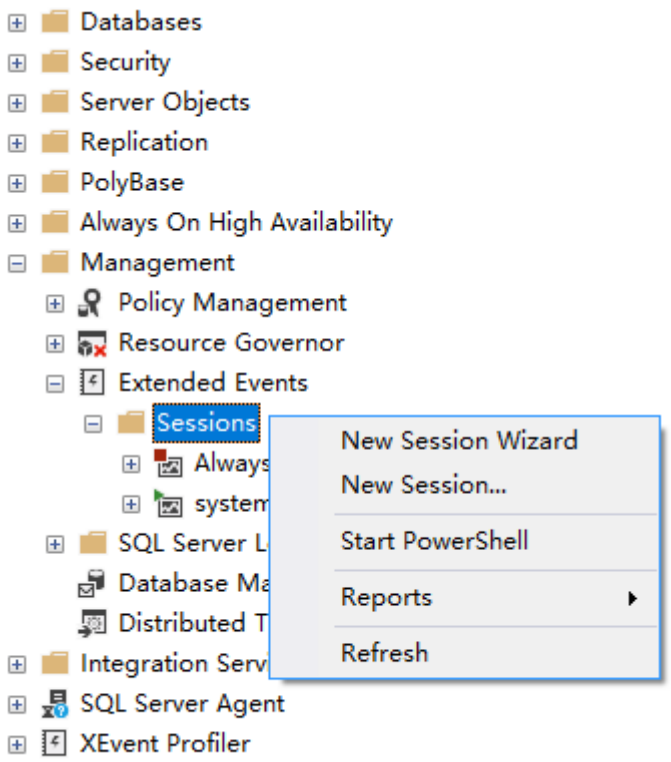
- 由于SQL Server 2008版本不支持扩展事件的功能，因此RDS for SQL Server 2008的各类版本均不支持扩展事件。
- Target暂未开放etw_classic_sync_target类型。
- 创建/更新扩展事件时，涉及到的路径目前只支持使用“D:\RDSDBDATA\Log\error”路径，文件名称可自由定义。

创建扩展事件

步骤1 启动SQL Server Managerment Studio客户端，使用rdsuser用户登录。

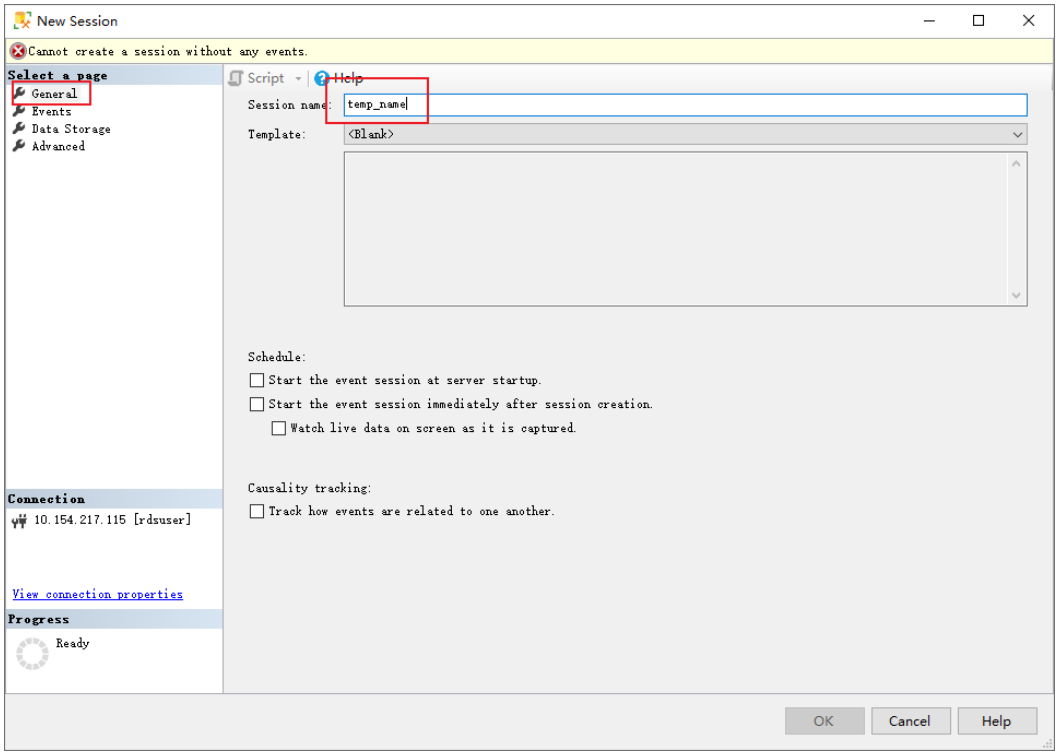
步骤2 在“Management > Sessions”路径下选择“New Session”新建扩展事件。

图 4-39 新建事件



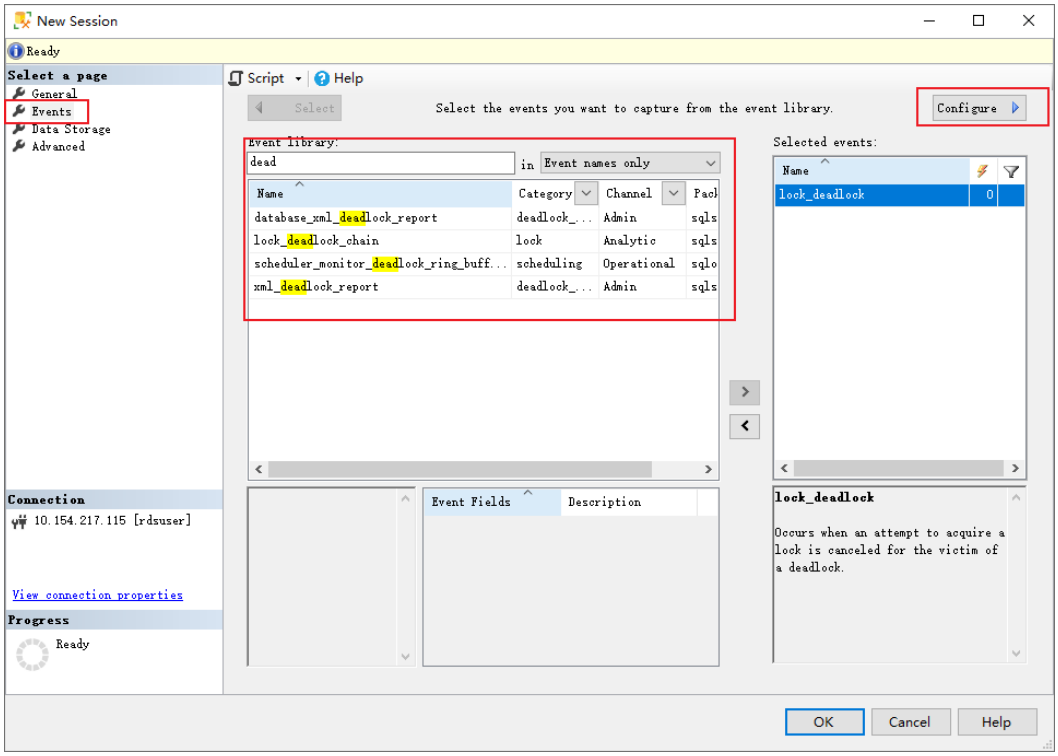
步骤3 单击“General”，定义事件名称。

图 4-40 设置事件名称



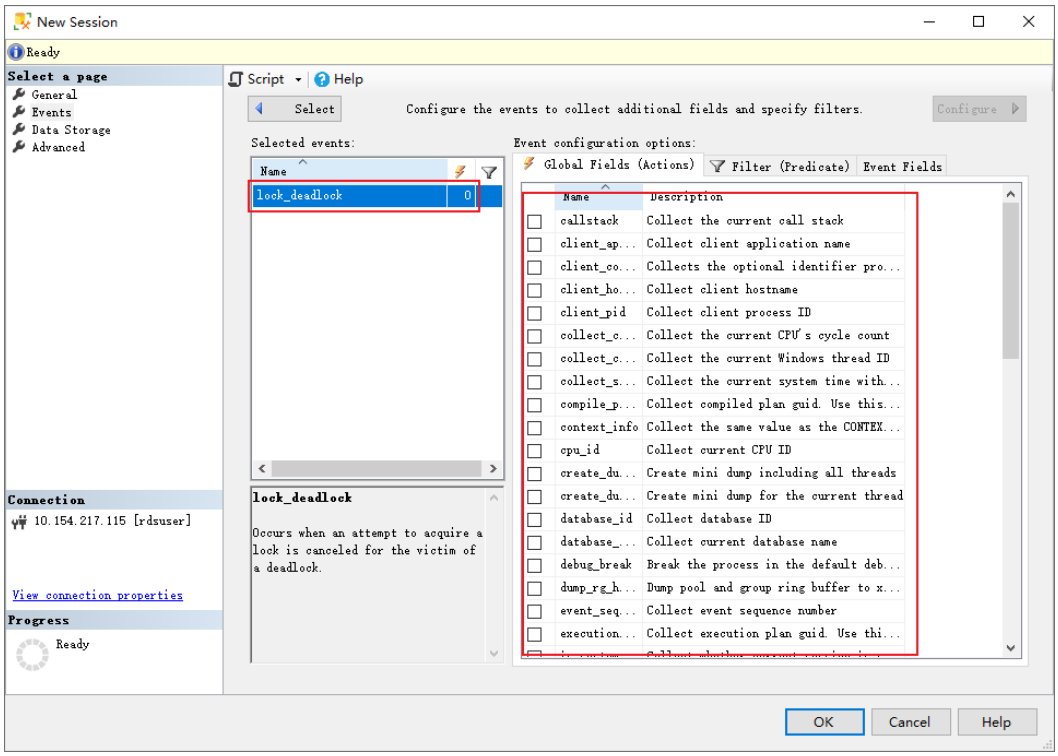
步骤4 单击“Events”，选择事件。

图 4-41 选择事件



步骤5 在**步骤4**的界面单击“Configure”，对事件进行配置。

图 4-42 配置事件

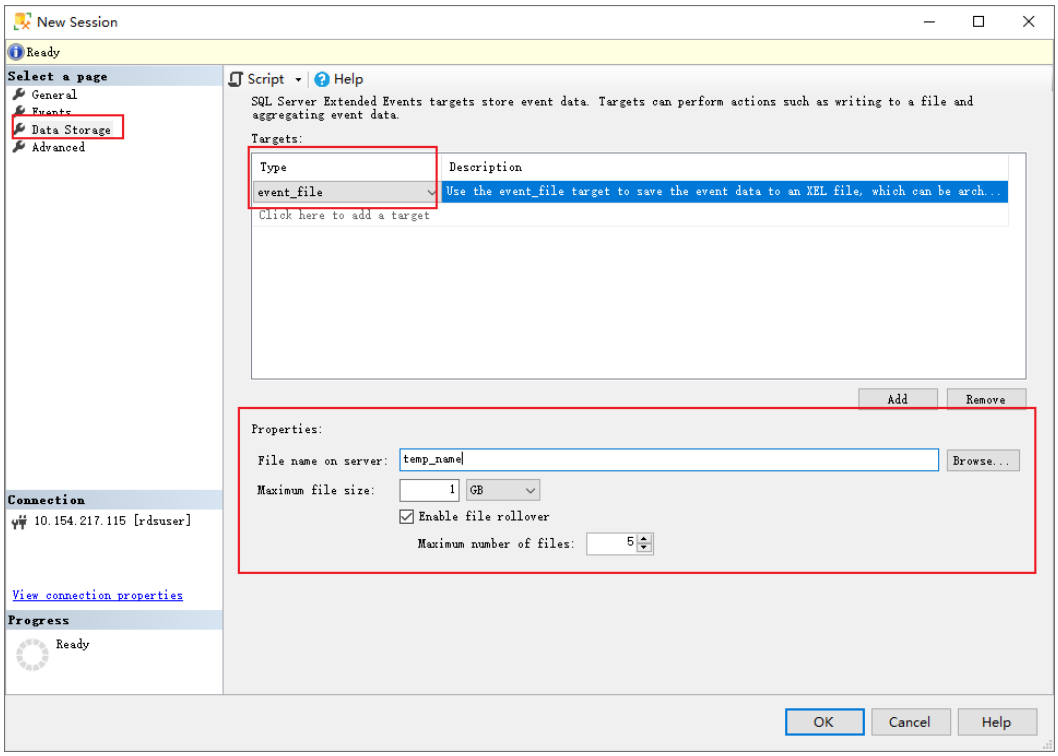


步骤6 单击“Data Storage”，进行数据存储配置。

说明

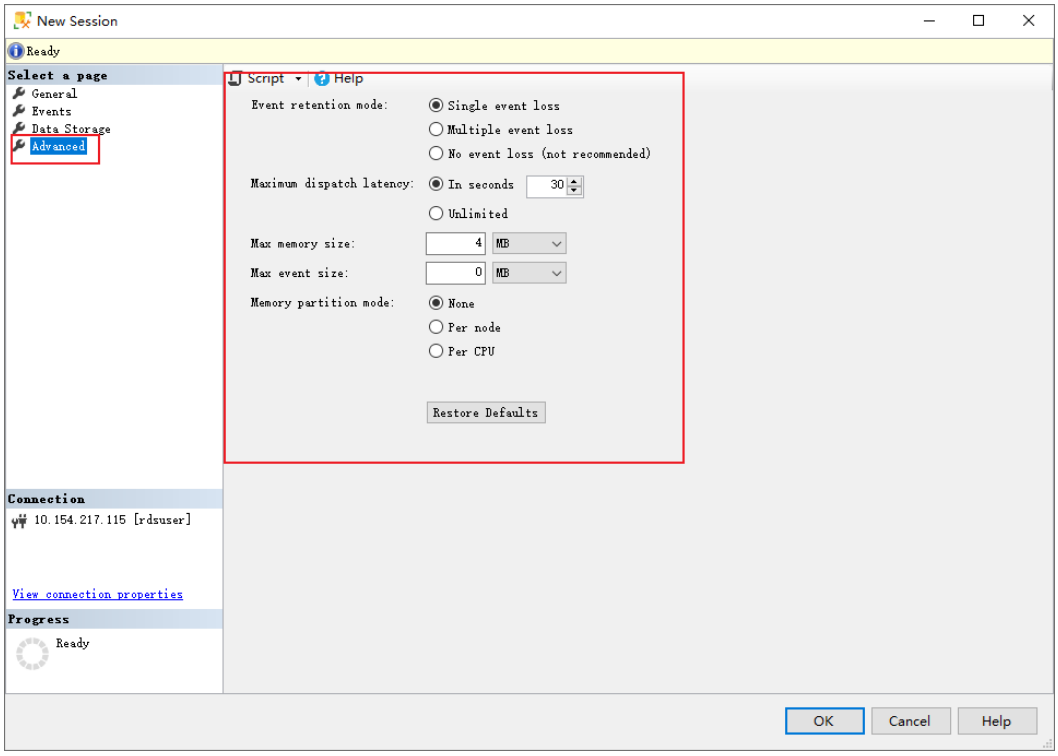
文件名称可自由定义，用户使用Browse浏览的是SSMS所在客户机的文件系统，无法配置RDS for SQL Server服务器的文件系统，因此不推荐使用；且RDS for SQL Server仅支持“D:\RDSDBDATA\Log\error”路径或者不填写路径，因此只建议用户修改文件名称即可。

图 4-43 配置数据存储



步骤7 单击“Advanced”，配置文件生成策略。

图 4-44 配置文件生成策略



步骤8 使用Script生成SQL语句，确认无误后执行SQL创建扩展事件。

```
-- 示例生成的SQL语句，具体语句根据实际使用情况而定
CREATE EVENT SESSION [temp_name] ON SERVER
ADD EVENT sqlserver.lock_deadlock(
ACTION(sqlserver.session_id,sqlserver.sql_text,sqlserver.username))
ADD TARGET package0.event_file(SET filename=N'temp_name')
GO
```

----结束

4.16 RDS for SQL Server 安全最佳实践

SQL Server数据库凭借其强大的事务处理能力、丰富的功能以及对企业级应用的广泛支持，在行业内享有良好的声誉，已经成为众多企业首选的关系数据库之一。RDS for SQL Server是一种基于云计算平台的即开即用、稳定可靠、弹性伸缩、便捷管理的在线云数据库服务，旨在为企业提供更高效、更安全的数据管理解决方案。

为加强RDS for SQL Server数据库安全性，本文将从以下几个维度给出建议，您可以根据业务需要在本指导的基础上进行安全配置。

- **使用高可用实例**
- **开启备份功能**
- **避免绑定EIP直接通过公网访问实例**
- **避免使用默认端口**
- **定期重置数据库账号密码**
- **定期检查并删除业务不再使用的角色**
- **确保数据库账号的最低权限**
- **避免依赖sysadmin权限**
- **开启强制加密**
- **使用TDE功能**
- **设置最大并行度**
- **使用DBSS全量审计**

使用高可用实例

RDS for SQL Server数据库集群版或主备版实例能够在主节点发生异常时自动进行故障切换，将备用节点提升为主节点，从而确保系统的高可用性和持续服务，最大限度地减少停机时间和数据丢失。

开启备份功能

创建RDS for SQL Server实例时，默认开启自动备份策略，默认自动备份保留7天，可根据业务需要调整备份保留时长。RDS for SQL Server实例支持**自动备份**和**手动备份**。您可以定期对数据库进行备份，当数据库故障或数据损坏时，可以通过备份文件恢复数据库，从而保证数据可靠性，具体操作请参见**数据恢复**。

避免绑定 EIP 直接通过公网访问实例

避免RDS for SQL Server部署在公网或者DMZ，应该将RDS for SQL Server部署在华为云内部网络，使用路由器或者防火墙技术把RDS for SQL Server保护起来，避免直接绑

定EIP从公网访问数据库实例，防止未授权的访问及DDos攻击。建议解绑弹性公网IP，如果您的业务必须绑定EIP，请务必**设置安全组规则**限制访问数据库的源IP。

避免使用默认端口

RDS for SQL Server的默认端口号为1433，此端口会更容易受到恶意攻击。建议您为数据库实例**修改端口**。

定期重置数据库账号密码

定期重置密码是提高系统和应用程序安全性的重要措施之一，不仅可以降低密码泄露的风险，还可以帮助用户满足合规要求，减少内部威胁，提高用户的安全意识。通过实施这一策略，可以显著提升账户整体安全水平，保护敏感数据和系统免受潜在的安全威胁。具体操作请参见**重置数据库账号密码**。

定期检查并删除业务不再使用的角色

对于每个查询出来的角色，检查是否必须存在。任何未知的角色都需要被审视，确保每个角色都是正常使用的，否则删除这些角色。

确保数据库账号的最低权限

RDS for SQL Server支持“基于角色”的方法授予账号对数据和命令的访问权限。建议管理员结合业务需要，遵从最低授权原则，创建合适的**数据库账号**，对账号进行授权。如果发现存在不符合该角色的账号权限，请结合业务需要，对账号权限进行更新或者**删除数据库账号**。RDS for SQL Server的**内置账号**用于给数据库实例提供完善的后台运维管理服务，禁止用户使用和删除。

避免依赖 sysadmin 权限

RDS for SQL Server的sysadmin权限为最高权限，此权限使用不当会造成RDS for SQL Server安全运维失效，从而导致数据被损坏、无法恢复数据、无法进行主备倒换等问题。

避免使用sysadmin权限是提高RDS for SQL Server安全性和稳定性的重要措施。通过实施最小权限原则、细化权限管理和增强审计与监控，可以显著降低安全风险，保护数据和系统的安全，有助于提高整体的安全管理水平。

开启强制加密

强制加密可以确保客户端与RDS for SQL Server之间的所有数据传输都经过加密。这样可以有效防止数据在传输过程中被窃听或篡改，增加了数据的隐私性和安全性。一旦开启强制加密连接，所有客户端都将自动使用加密方式与RDS for SQL Server通信，无需针对每个客户端单独配置，使得安全管理更加简便统一。

使用 TDE 功能

RDS for SQL Server的**TDE功能**通过自动加密数据文件和备份文件，提供了高效的数据静态保护，并且加密过程对应用程序透明，满足合规性要求。但是使用TDE功能可能会对性能和存储空间产生一定影响。

设置最大并行度

通过设置参数“max degree of parallelism”的值，可以调整RDS for SQL Server的最大并行度，优化查询性能和资源利用率。该参数设置过大会导致锁阻塞，设置过小会

导致资源利用不充分，建议结合业务使用量和实例规格来设置。一般推荐初始设置为数据库实例的CPU核数的一半或根据实际负载进行微调。具体操作请参见**修改RDS for SQL Server实例参数**。

使用 DBSS 全量审计

审计日志可以捕获审计员通常需要或满足法规要求的详细记录。例如，RDS for SQL Server默认开启DDL审计内容，可以跟踪服务器设置修改、数据库和表的结构更改。另外，建议使用DBSS全量审计获取到全量的审计日志，该审计日志包括DML审计内容，并且能够保存180天或更长时间。