可信智能计算服务

快速入门

文档版本 01

发布日期 2023-11-04

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。

华为云计算技术有限公司

地址： 贵州省贵安新区黔中大道交兴功路华为云数据中心 邮编：550029

网址： https://www.huaweicloud.com/

目 录

1 快速入门

1.1 TICS 使用流程简介

本文档是一个TICS入门教程，介绍了如何在TICS控制台完成端到端的全流程使用。

可信智能计算服务TICS（ Trusted Intelligence Computing Service ）打破数据孤岛，在数据隐私保护的前提下，实现行业内部、各行业间的多方数据联合分析和联邦计算。TICS基于安全多方计算MPC、区块链等技术，实现了数据在存储、流通、计算过程中端到端的安全和可审计，推动了跨行业的可信数据融合和协同。

使用 TICS 的用户角色

根据人员的职能进行划分，使用TICS的用户主要可以分为以下两类。

- **组织方**

  面向熟悉业务并具有管理、决策、审核权限的管理人员。组织方具有TICS的所有权限，包括创建空间、邀请空间成员、删除空间等权限。例如，在创建空间模块中，组织方可以对合作方人员发布的数据进行审核，把好质量关。

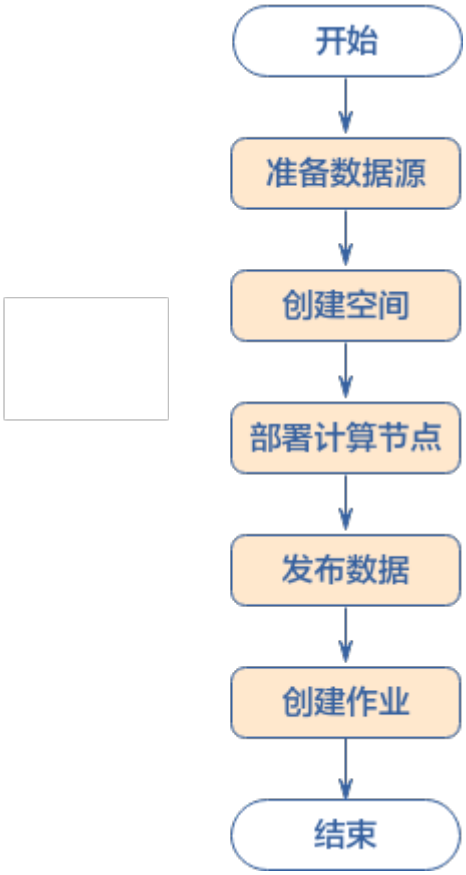
- **合作方**

  合作方使用数据源计算节点模块实现自主可控的数据源注册、隐私策略（脱敏、加密、水印）的设定、元数据的发布等，为数据源计算节点提供全生命周期的可靠性监控、运维管理。

TICS 使用流程简介

TICS典型的端到端开发流程如下图所示：

图 1-1 TICS 使用流程



1.2 步骤 1：准备工作

如果您是第一次使用TICS，请参考**准备工作**，完成注册账号并实名认证、配置CCE服务、购买TICS服务、授权IAM用户使用TICS、准备数据、启用区块链审计服务（可选）等一系列准备工作。

本入门示例，是为了演示TICS使用的全流程。组织方在组建空间时，需要至少添加1位合作方。

1.3 步骤 2：空间组织方邀请成员

完成准备工作后，您已经创建了空间，可以开始配置使用TICS。

为了在TICS平台实现多方作业，必须先在TICS中邀请成员。

邀请成员

步骤1 空间成员登录TICS控制台。

步骤2 在TICS控制台左侧，单击“空间管理”，在“我创建的空间”页签查找需要邀请合作方的空间并单击“邀请合作方”。

步骤3 在弹出的界面配置待邀请的合作方的“租户名称”和“租户别名”，“租户名称”从合作方侧获取即可，保存后单击“确定”，完成邀请合作方操作。

图 1-2 添加合作方

----结束

1.4 步骤 3：成员接受邀请

成员接受邀请

在TICS中，成员需要先接受组织方的邀请加入空间，然后才能发布数据用于创建作业。

步骤1 合作方登录TICS控制台。进入TICS控制台后，单击页面左侧“通知管理”，进入通知管理页面。

步骤2 浏览通知信息，查找要加入的空间，单击其所属的“接受邀请”。

图 1-3 通知管理入口

步骤3 在TICS页面左侧，依次单击“空间管理 > 我参与的空间”，查看空间信息。

----结束

1.5 步骤 4：（可选）下载计算节点配置信息

下载计算节点配置信息

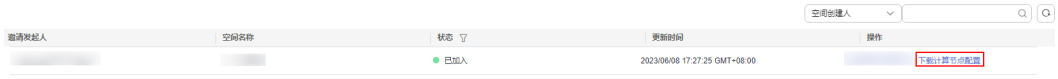
下载计算节点配置相关的信息，下载的信息可在部署计算节点的时候导入。“计算节点配置”代表“部署计算节点”属于哪个空间，用户输入的数据就会在哪个空间中参与计算。

配置信息包含证书，用于计算节点之间通信双向认证。证书保证了空间下的用户，部署的计算节点能够数据交互，参与计算。同时，也隔离了不同空间之间的数据访问。

步骤1 合作方登录TICS控制台。进入TICS控制台后，单击页面左侧“通知管理”，进入通知管理页面。

步骤2 浏览通知信息，单击“下载计算节点配置”，得到agentConfig.zip文件，解压到本地。

图 1-4 下载计算节点配置



----结束

1.6 步骤 5：空间成员部署计算节点

同一个空间中的用户，在使用可信计算服务时（多方安全计算和可信联邦学习），需要部署计算节点，将自己的数据上传，用于可信计算服务的输入。

部署计算节点

步骤1 空间成员登录TICS控制台。进入TICS控制台后，单击页面左侧“通知管理”，进入通知管理页面。

步骤2 浏览通知信息，在对应空间通知处单击“前往购买计算节点”，在弹出的页面配置参数。

图 1-5 部署计算节点

表 1-1 参数配置说明

参数名	参数描述
计算节点位置相关参数	
区域	下拉选择用户将计算节点部署在哪个区域。
项目	下拉选择用户将计算节点部署在区域下的哪一个项目内。
计费方式	选择包年/包月。
购买时长	支持按月或按年购买。
自动续费	支持自动续费。 ● 按月购买时，自动续费周期为1个月。 ● 按年购买时，自动续费周期为1年。
版本类型	当前可选版本只包含企业版。
空间配置相关参数	
导入空间配置（可选）	用户从“前往购买计算节点”进入部署页面则无需该操作。 其它情况下需在TICS“通知管理”页面，单击“下载计算节点配置”，得到agentConfig.zip文件，本地解压后，导入json文件，空间配置信息将会自动填充到“区域”（league_region_name）、“空间名称”（league_name）、“空间ID”（league_id）。
空间区域	导入配置文件会自动填充，若未导入下拉选择空间所在的区域即可。可通过在TICS“通知管理”页面，单击“下载计算节点配置”，得到agentConfig.zip文件，本地解压后，打开json文件，查看参数“league_region_name”。
空间名称	通过“计算节点配置”文件agentConfig.zip中的json文件获取，参数名为“league_name”。
空间ID	通过“计算节点配置”文件agentConfig.zip中的json文件获取，参数名为“league_id”。
计算节点配置相关参数	
计算节点名称	计算节点别名，由用户自定义，用以区分部署的各个计算节点。要求：名称不能以空白字符开头或结尾，也不能包含下列特殊字符：\ / : * ? " < > |，长度要求在1~128之间。
访问密钥ID（AK） 加密密钥（SK）	用户的身份标识，需要用户去IAM服务自行下载。文件获取方式请参考**参考：获取访问密钥**章节。 **说明** ● 如果访问密钥泄露，会带来数据泄露风险。 ● 每个访问密钥只能下载一次，为了账号安全性，建议定期更换访问密钥并妥善保存。
计算节点登录名称	登录计算节点控制台的用户名。用户可通过“计算节点登录名称”和“登录密码”进入计算节点控制台，建立连接器，发布数据。

参数名	参数描述
登录密码	登录计算节点控制台的密码。
确认密码	与“登录密码”保持一致即可。
指定开放端口	计算节点控制台系统的网络端口。
部署配置相关参数	
部署方式	当前版本支持云租户部署和边缘节点部署。 • **云租户部署**：数据上云的用户可以选择“云租户部署”，可信计算节点部署在华为云租户的虚拟私有云VPC中，可信计算节点组件部署在基于华为云CCE服务的容器中。关于CCE集群的更多信息可参考**CCE**。 当前仅支持直接创建CCE集群，不支持选择已有集群。您需要配置CCE集群的部署规格、虚拟私有云、子网、节点密码、弹性IP等信息。 **说明** – CCE集群的部署规格根据您的业务量自行选择。 – 所创建CCE集群的虚拟私有云、子网，应与数据源所在云服务（如MRS Hive、DWS等）的虚拟私有云、子网保持一致，以确保网络互通。 – 自动创建的CCE集群费用不需要单独结算，当前TICS费用已包含CCE集群费用。 • **边缘节点部署**：数据不上云的用户可以选择“边缘节点部署”，数据不需要上传到华为云上，通过纳管节点的方式，即可参与多方安全计算或者联邦学习任务，关于IEF边缘节点的更多信息可参考**IEF**。 您可参考**纳管节点**来纳管节点，注意：纳管节点防火墙需要开通30000-65535端口，且需要建立消息端点和消息路由，步骤如下： 1. 登录IEF服务，选择左侧“边云消息”列，选择“消息端点”。 2. 创建消息端点，填写相关参数。 “消息端点类型”选择“边缘端点（ServiceBus）”； “消息端点名称”参数值为“tics-agent”； “服务端口”参数值为“30000”。 3. 选择左侧“边云消息”列，单击“消息路由”，勾选“专业版服务实例”，填写相关参数。 **“消息路由名称”**参数值为“tics-agent-route”； **“源端点”**参数值为“SystemREST”； **“源端点资源”**参数值为“/tics-agent”； **“目的端点”**参数值为“tics-agent”； **“目的端点资源”**参数值为“/”。
云租户部署参数	

参数名	参数描述
部署规格	• 中规格：适用百万级别数据多方安全计算，五十万内对齐样本联邦建模 • 大规格：适用千万级别数据多方安全计算，百万级别对齐样本联邦建模
虚拟私有云	选择合适的VPC
子网	选择合适的子网地址
NAT网关	选择子网下NAT网关，若子网下不存在NAT网关，默认新建。
弹性IP	选择NAT网关已关联的弹性公网IP。若NAT网关无关联弹性公网IP，默认新建。 弹性公网IP提供外网访问能力，可以灵活绑定及解绑，随时修改带宽。未绑定弹性公网IP的云服务器无法直接访问外网，无法直接对外进行互相通信。
存储方式	提供OBS存储和极速文件存储两种持久化存储卷的选择。
OBS存储	存储方式选择obs存储时，可以选择自动创建OBS桶，也可以通过下拉框的搜索功能寻找已有的OBS桶。选择已有的OBS桶时，需要确认OBS桶的访问权限中包含读取权限和写入权限，否则其上的联邦作业将会失败。
卷名	存储方式选择极速文件存储时，默认选取已有的极速文件存储，也可手动填写SFS ID。
挂载路径	存储方式选择极速文件存储时需填写。默认根路径，若自定义路径，请确保该路径在极速文件存储上存在。
开启AOM日志监控	开启后可收集可信计算节点日志，推荐开启。 对接AOM之后，相应的日志存储在AOM平台上，平台每月提供500M的免费空间，超出则计费。具体的计费规则参见**计费概述**。
节点密码	设置可信计算节点宿主机的登录密码。
确认密码	与“节点密码”保持一致即可。
边缘节点部署参数	
AI加速卡	• 不启用：部署常规的CPU规格计算节点 • 启用：启用边缘节点的AI加速卡，可以大幅减少联邦建模的耗时。通过IEF边缘节点部署时，请确保计算节点的AI加速卡相关功能可用，如需帮助请联系客服或技术支持人员。
纳管节点	用户选择边缘节点部署计算节点时呈现此参数。用户通过IEF服务纳管用户侧的边缘节点，用于部署计算节点。使用边缘节点部署方式，请先参考**纳管节点**执行纳管节点操作。
主机docker IP	请前往ief纳管节点，执行命令ifconfig docker0 | grep inet | grep -v 127.0.0.1 | grep -v inet6 | awk '{print $2}' | tr -d "addr:" 填入所得的ip地址

参数名	参数描述
proxy配置（选填）	用户选择IEF部署计算节点时，可根据实际情况选填该参数。如果纳管节点使用了网络计算节点，请按照实际情况配置proxy信息，也可在部署成功后，通过配置变更项进行修改，具体操作可参考**变更计算节点配置**。
存储方式	选择采用外部文件挂载容器目录的方式。IEF当前仅支持“主机存储”。 • **主机存储**：该方式将计算节点所在的集群节点的主机路径，挂载到计算节点容器的目录上。用户需要选择集群中的节点（对应“纳管节点”下拉选）作为挂载节点，此时，部署的计算节点容器会运行到该节点上。同时，用户需要输入“主机路径”，设置该节点的主机挂载目录。计算节点成功部署后，用户可登录集群该节点，访问输入的“主机路径”来进行文件的上传。
主机路径	“存储方式”选择“主机存储”时呈现此参数，计算节点成功部署后通过输入的“主机路径”来进行文件的上传。 例如：“192.168.0.61/tmp”，如何在后台查找该路径请参考**登录节点**的相关描述。 **说明** 请确保选择的主机路径具有1000:1000属组权限，否则会影响部分功能使用。
资源分配策略	
CPU(Cores)	用户可根据返回资源剩余规格，按照分析与学习需求，灵活分配核数。
内存(GiB)	用户可根据返回资源剩余规格，按照分析与学习需求，灵活分配内存。容器预留部分管理资源，作业可用内存最大值设置为内存数值的0.6倍，且向下取整。
区块链配置	
是否开启区块链审计	勾选该项表示启用区块链审计服务，使用前需要按照“准备工作 > 启用区块链审计服务（可选）”章节的描述完成准备工作。
BCS服务实例	选择BCS空间链。
通道	选择邀空间链邀请租户时选择的通道。
组织	选择链代码部署的组织。

步骤3 单击下一步并提交订单，完成计算节点部署。

说明

- 计算节点在不同时刻有以下7种状态：部署中，部署失败，启动中，运行中，删除中，删除失败，重启中。
- 可以在“？”标识处，查看部署计算节点的概要事件信息。
- 计算节点在部署完成后会向外访问如下地址，发送节点状态信息，用作心跳监测以及执行联邦作业操作命令。

  1.tics.****.myhuaweicloud.com（地址信息以空间所在region为准）

  2.聚合器ip（空间创建时自动申请的聚合器公网ip）

----结束

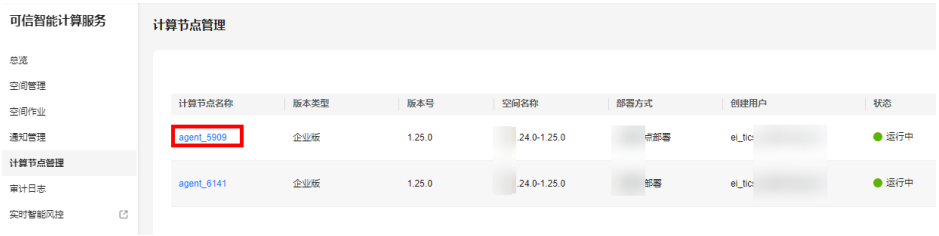
1.7 步骤 6：空间成员发布数据

发布数据

步骤1 空间成员登录TICS控制台。进入TICS控制台后，单击页面左侧“计算节点管理”，进入“计算节点管理”页面。

步骤2 在“计算节点管理”页，查找需要发布数据的计算节点名称，单击“计算节点名称”进入计算节点详情页。

图 1-6 选择计算节点



步骤3 在“计算节点详情”页，单击“前往计算节点”，在登录页输入部署计算节点时设置的“登录用户名”和“密码”。

图 1-7 前往计算节点

步骤4 登录成功后，进入到计算节点界面，选择左侧导航栏中“连接器管理”，单击“创建”，在弹出的界面配置创建连接器的参数，配置完成后单击“确定”。

说明

测试功能为数据源连通性及密码正确性的检查测试。

图 1-8 创建连接器（以 RDS 服务为例）

表 1-2 参数说明

参数名	描述
连接器类型	• “连接器类型”选择Hive连接时，需要选择Hive版本，当前仅支持MRS2.x和MRS3.x版本，选择的MRS集群需与当前计算节点部署CCE或IEF（非云上IEF节点不支持接入Hive）在同一VPC。“用户名”为MRS集群中拥有Hive权限的集群用户，“用户认证凭据”需要上传对应用户的认证凭据，请在MapReduce服务的**下载用户认证文件**中获取。 • “连接器类型”选择RDS服务时，所选择的RDS服务实例需与计算节点在同一VPC下，且端口开放。填写的用户名，需具有数据库的读写权限（参考**修改权限**）。“密码”为该用户登录RDS实例的密码。 • “连接器类型”选择MySql时，需保证计算节点与数据库所在虚机的连通性，“驱动文件”需与目标MySQL数据库版本一致。驱动类名com.mysql.cj.jdbc.Driver，仅支持mysql-connector-java-5.x以后的版本，驱动文件请在**Mysql驱动下载地址**中获取。 • “连接器类型” 选择DWS连接时，填写的用户名，需具有数据库的读写权限（参考**权限管理**）。“密码”为该用户登录DWS实例的密码。 • “连接器类型” 选择ORACLE连接时，需保证计算节点与数据库的连通性，当前仅支持ORACLE 12c和19c版本。驱动文件需与目标ORACLE数据库版本一致，请在**ORACLE驱动下载地址**中获取。 • “连接器类型” 选择API连接时，需保证计算节点与api接口的连通性，当前仅支持基础认证方式。
连接器名称	根据实际情况设置即可。
数据库版本	“连接器类型”选择MySql和ORACLE时，呈现此参数。根据实际情况设置即可。
数据库名称	“连接器类型”选择ORACLE时，呈现此参数。根据实际情况设置即可。
数据库服务器	“连接器类型”选择ORACLE时，呈现此参数。用户根据实际情况设置。
端口	“连接器类型”选择ORACLE时，呈现此参数。用户根据实际情况设置。
实例名称	“连接器类型”选择RDS或DWS服务时，呈现此参数。下拉选择实例即可。
数据库	“连接器类型”选择DWS服务时，呈现此参数。可手动输入DWS服务里面购买的数据库名称。
用户名	用户根据实际情况设置。
密码	用户根据实际情况设置。

参数名	描述
驱动类名	“连接器类型”选择MySql和ORACLE时，呈现此参数。根据实际情况设置，注意驱动类名com.mysql.cj.jdbc.Driver仅支持mysql-connector-java-5.x以后的版本。
JDBC URL	“连接器类型”选择MySql时，呈现此参数。JDBC访问端口。取值样例：198.0.0.1：3306。
驱动文件	“连接器类型”选择MySql和ORACLE时，呈现此参数。JDBC驱动。
其他属性	“连接器类型”选择MySql时，呈现此参数。用户根据实际情况设置任务所需的Key和Value。

步骤5 选择界面左侧“数据管理”，单击“创建”，在弹出的界面配置创建数据的参数，配置完成后单击“确定”。

说明

配置数据参数时，若“连接器”为Hive、MySQL、RDS、DWS、ORACLE类型时，可对字段信息进行隐私策略的配置：

- **字段类别**：
  - **唯一标识**：指用于标识某个事物实体身份的字段。例如身份证、工号、公司代码等。勾选后，会通过一定的语法限制和运行期校验，保护数据集内的id总集，确保无法被恶意逆推。
  - **敏感**：指会参与统计、计算的敏感数据。例如薪水、纳税、用电量。勾选后，其他参与方只能使用敏感数据进行不可逆推的四则运算、聚合计算（sum/avg/variance)、条件过滤（where）。TICS会保护唯一标识和敏感数据不被成对地明文泄露，同时会对敏感数据的求和计算添加差分噪声，以保护敏感数据不被泄露。
  - **非敏感**：指不参与数值分析，也和唯一身份无关的数据。例如等级、公司类型。
- **脱敏**：勾选后，会对数据进行脱敏。

步骤6 在“数据管理”页签找到待发布的数据名称，单击“发布”，数据就会被同步到作业管理的数据集中。

编辑完成后，需再次发布，变更才会生效。

----结束

1.8 步骤 7：空间成员创建作业

创建多方安全计算作业

步骤1 空间成员登录进入计算节点页面。

步骤2 在左侧导航树上依次选择“作业管理 > 多方安全计算”，在页面上方选择作业创建的空间后，单击“创建”。

图 1-9 创建多方安全计算作业

步骤3 在弹出的对话框中，输入作业“名称”和“描述”信息后单击“确定”。

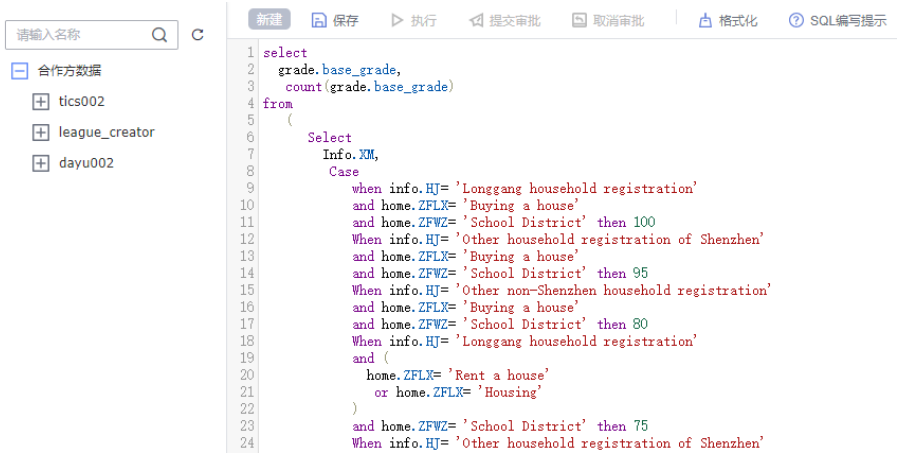
图 1-10 新建作业

步骤4 在作业列表中查找创建的作业，单击“开发”，进入作业开发页面编写SQL语句。SQL语句开发完成后单击“保存”。

说明

- 在作业开发页面“合作方数据”一栏可查看此空间合作方共享的数据。
- 数据第一级是合作方名称，第二级是数据名称。
- SQL语句中用“合作方名.数据名”表示一张表。
- SQL语句开发完成， 可单击页面上方“格式化”来对排版进行美化

图 1-11 编写 SQL 语句



SQL语句的完整内容如下：

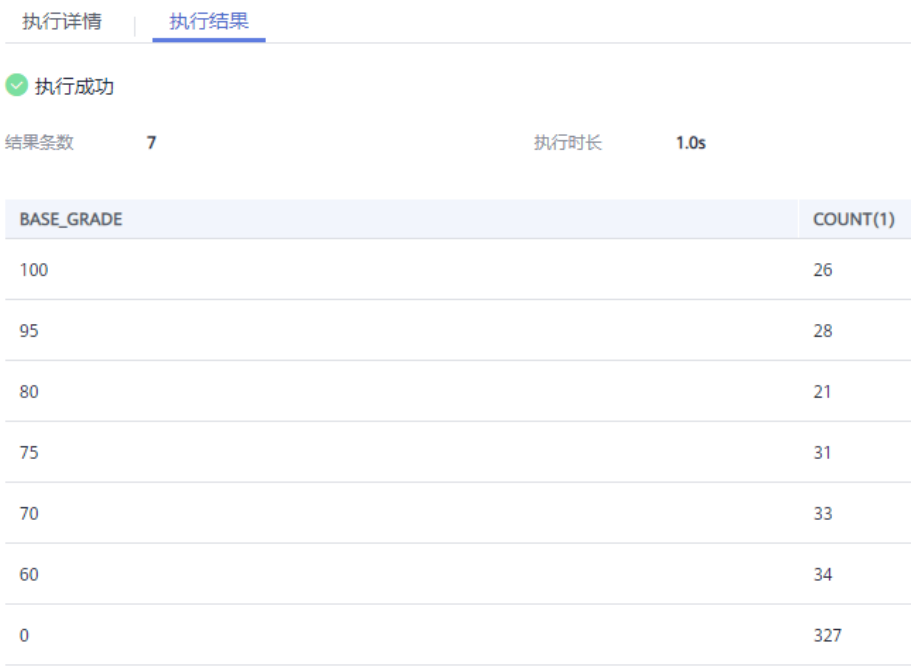
```
select
  grade.base_grade,
  count(grade.base_grade)
from
  (
    Select
      Info.XM,
      Case
        when info.HJ= 'Longgang household registration'
        and home.ZFLX= 'Buying a house'
        and home.ZFWZ= 'School District' then 100
        When info.HJ= 'Other household registration of city A'
        and home.ZFLX= 'Buying a house'
        and home.ZFWZ= 'School District' then 95
        When info.HJ= 'Other non-city A household registration'
        and home.ZFLX= 'Buying a house'
        and home.ZFWZ= 'School District' then 80
        When info.HJ= 'Longgang household registration'
        and (
          home.ZFLX= 'Rent a house'
          or home.ZFLX= 'Housing'
        )
        and home.ZFWZ= 'School District' then 75
        When info.HJ= 'Other household registration of city A'
        and (
          home.ZFLX= 'Rent a house'
          or home.ZFLX= 'Housing'
        )
        and home.ZFWZ= 'School District' then 70
        When info.HJ= 'Other non-city A household registration'
        and (
          home.ZFLX= 'Rent a house'
          or home.ZFLX= 'Housing'
        )
        and home.ZFWZ= 'School District' then 60
        Else 0
      end as base_grade
    from
      JiaoYuJu_FangGuanJu.ZHUFANG home
      join RenSheJu.SHENFENXINXI info on home.SFZID= info.SFZID
  ) grade
group by
  grade.base_grade
Order by grade.base_grade desc
```

步骤5 单击右侧的，进行作业配置。

- **图 1-12** 作业配置

步骤6 单击“保存”，然后“提交审批”并通过后，单击“执行”。等待执行完成后在下方“执行结果”页签查看结果。

图 1-13 执行结果



BASE_GRADE	COUNT(1)
100	26
95	28
80	21
75	31
70	33
60	34
0	327

----结束

1.9 入门实践

当您参考**准备工作**章节完成注册账号并实名认证、配置CCE服务、配置IEF服务、购买购买TICS服务、授权IAM用户使用TICS、准备数据、启用区块链审计服务（可选）等一系列操作后，可以根据自身的业务需求使用TICS提供的常用实践。

表 1-3 常用最佳实践

实践	描述
基于TICS实现端到端的企业积分查询作业	本最佳实践提供了通过统一制定隐私规则，使用TICS进行安全计算，避免真实数据被窃取的使用案例。