可信智能计算服务

最佳实践

文档版本 01

发布日期 2023-03-31

华为技术有限公司

版权所有 © 华为技术有限公司 2024。 保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

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。

华为技术有限公司

地址： 深圳市龙岗区坂田华为总部办公楼 邮编：518129

网址： https://www.huawei.com

客户服务邮箱： support@huawei.com

客户服务电话： 4008302118

安全声明

漏洞处理流程

华为公司对产品漏洞管理的规定以“漏洞处理流程”为准，该流程的详细内容请参见如下网址：
https://www.huawei.com/cn/psirt/vul-response-process
如企业客户须获取漏洞信息，请参见如下网址：
https://securitybulletin.huawei.com/enterprise/cn/security-advisory

 版权所有 © 华为技术有限公司

目 录

 版权所有 © 华为技术有限公司

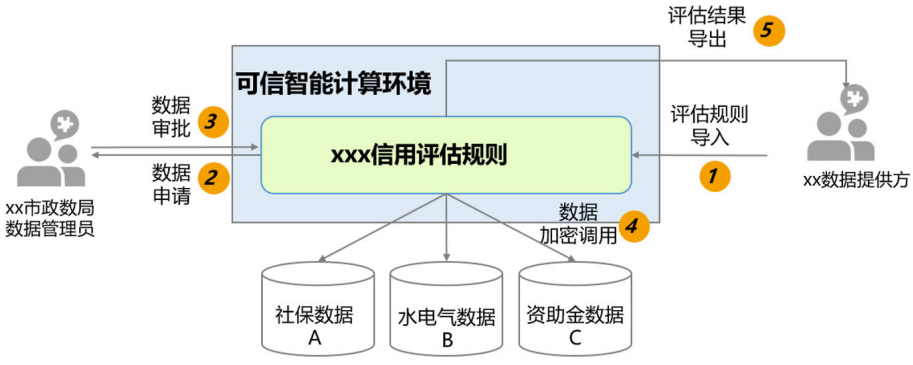
1 基于 TICS 实现端到端的企业积分查询作业

1.1 简介

背景信息

本案例以“小微企业信用评分”的场景为例。 社保、水电气和资助金等数据统一存储在某政务云，由不同的局进行管理，机构想单独申请进行企业相关评分的计算会非常困难。 因此可以由市政数局出面，统一制定隐私规则，审批数据提供方的数据使用申请， 并通过华为TICS可信智能计算平台进行安全计算。

图 1-1 企业信用评估应用场景示意图



 版权所有 © 华为技术有限公司

数据准备

注意

- 以下数据和表结构是根据场景进行模拟的数据，并非真实数据。
- 以下数据需要提前存导入到MySQL\Hive\Oracle等用户所属数据源中，TICS本身不会持有这些数据，这些数据会通过用户购买的计算节点进行加密计算，保障数据安全。
- 政府信息提供方的数据tax和support，在用户计算节点agent_gov上发布。
- 能源信息提供方的数据power，在用户计算节点agent_power上发布。

表 1-1 企业税收和资助金情况表 tax

列名	含义	字段分类
Id	企业id	唯一标识
tax_bal	税收	敏感
Industry	行业类型	不敏感

表 1-2 企业政府资助金数据表 support

列名	含义	字段分类
Id	企业id	唯一标识
supp_bal	资助金的金额	敏感
Industry	行业类型	不敏感

表 1-3 企业水电情况表 power

列名	含义	字段分类
Id	企业id	唯一标识
electric_bal	电费	敏感
water_bal	水费	敏感

从业务角度考虑，安排五个阶段，来对TICS系统进行验证和测试。本章重点讲述如何端到端实现一个该场景下的隐私计算作业完整执行流程。

版权所有 © 华为技术有限公司

导入数据

步骤1 在第一个合作方Partner1的MySQL数据源中，通过如下的SQL语句创建数据表：

```
CREATE TABLE tax (
        id integer COMMENT '企业id' ,
        tax_bal integer COMMENT '税收金额' ,
        industry varchar(150) COMMENT '行业'
);
CREATE TABLE support (
        id integer COMMENT '企业id' ,
        supp_bal integer COMMENT '资助金额',
        industry varchar(150) COMMENT '行业'
);
```

步骤2 在第二个合作方Partner2的MySQL数据源中，通过如下的SQL语句创建数据表：

```
CREATE TABLE power (
        id integer COMMENT '企业id' ,
        electric_bal integer COMMENT '电费',
        water_bal integer COMMENT '水费'
);
```

步骤3 将下面的数据分别导入csv文件并上传到MySQL数据源所在服务器。

- Tax表的数据如下：

```
id,tax_bal,industry
123400999,745,互联网
123400998,324,其他
123400997,664,其他
123400996,243,金融
123400995,715,互联网
123400994,475,通讯
123400993,526,其他
123400992,272,互联网
123400991,646,金融
123400990,510,其他
```

- Support表的数据如下：

```
id,supp_bal,industry
123400999,314,互联网
123400998,405,其他
123400997,371,其他
123400996,484,金融
123400995,381,互联网
123400994,405,通讯
123400993,292,其他
123400992,503,互联网
123400991,303,金融
123400990,412,其他
```

- Power表的数据如下：

```
id,electric_bal,water_bal
123400999,79,48
123400998,57,70
123400997,69,37
123400996,50,57
123400995,66,50
123400994,56,55
123400993,63,53
123400992,45,76
123400991,80,36
123400990,39,63
```

步骤4 执行如下SQL语句，将csv文件内的数据导入创建的数据表。

```
LOAD DATA INFILE 'csv数据文件名' INTO TABLE 表名
```

或者执行如下的插入语句：

- Tax表：

 版权所有 © 华为技术有限公司

```
insert into tax values
(123400999,745,'互联网'),
(123400998,324,'其他' ),
(123400997,664,'其他' ),
(123400996,243,'金融' ),
(123400995,715,'互联网' ),
(123400994,475,'通讯' ),
(123400993,526,'其他'),
(123400992,272,'互联网' ),
(123400991,646,'金融' ),
(123400990,510,'其他');
```

- Support表：

```
insert into support values
(123400999,314,'互联网' ),
(123400998,405,'其他' ),
(123400997,371,'其他' ),
(123400996,484,'金融' ),
(123400995,381,'互联网' ),
(123400994,405,'通讯' ),
(123400993,292,'其他' ),
(123400992,503,'互联网' ),
(123400991,303,'金融' ),
(123400990,412,'其他');
```

- Power表：

```
insert into power values
(123400999,79,48),
(123400998,57,70),
(123400997,69,37),
(123400996,50,57),
(123400995,66,50 ),
(123400994,56,55),
(123400993,63,53),
(123400992,45,76),
(123400991,80,36),
(123400990,39,63);
```

----结束

1.2 阶段一：数据发布

前提条件

完成**数据准备**工作。

操作步骤

步骤1 进入TICS服务控制台。

步骤2 在计算节点管理中，找到购买的计算节点，通过登录地址，进入计算节点控制台。

图 1-2 前往计算节点

 版权所有 © 华为技术有限公司

步骤3 登录计算节点后，在下图所述位置新建连接器。

图 1-3 新建连接器

步骤4 输入正确的连接信息，建立数据源和计算节点之间的安全连接。

图 1-4 输入信息

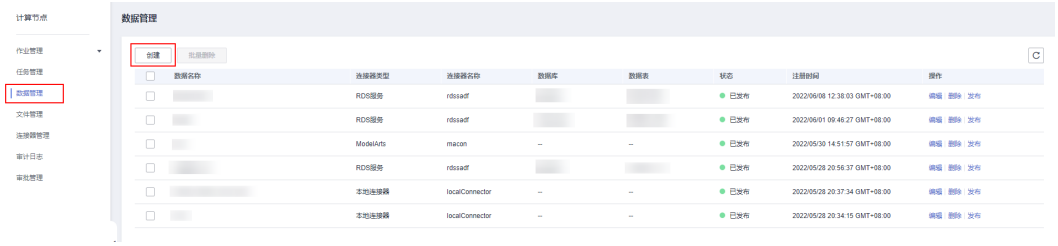
步骤5 建立完成后，连接器显示正常说明连接正常。

图 1-5 连接正常

步骤6 进入数据管理，进行数据集发布。

版权所有 © 华为技术有限公司

图 1-6 新建数据管理



步骤7 填写参数信息。

图 1-7 填写参数

----结束

重复步骤1~7，发布support资助金数据表和power_data能源表。

说明

数据发布的过程并不会直接从数据源中导出用户数据，仅从数据源处获取了数据集相关的元数据信息，用于任务的解析、验证等。

版权所有 © 华为技术有限公司

1.3 阶段二：隐私规则防护

使用TICS的隐私规则防护能力确保数据安全。

前提条件

完成**数据发布**。

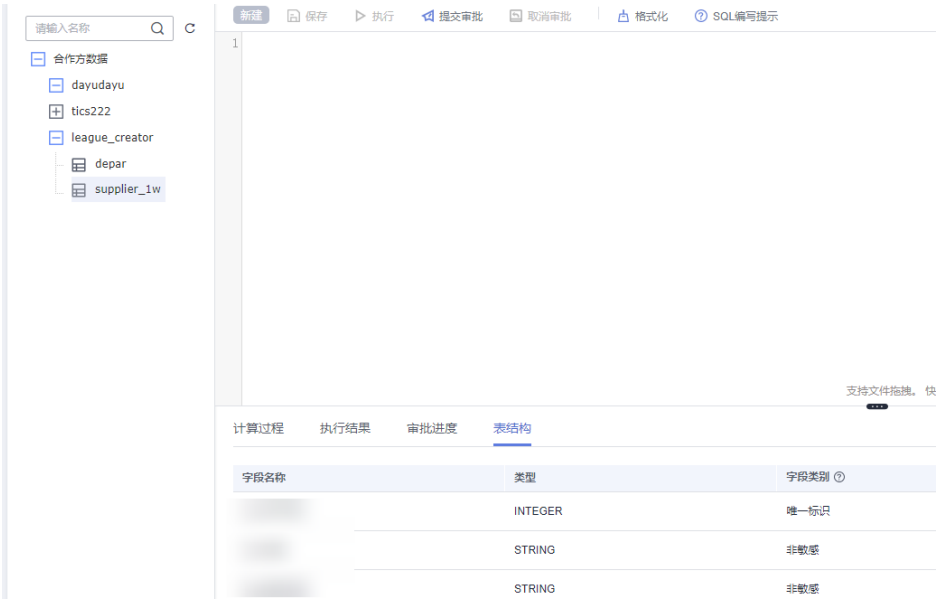
操作步骤

步骤1 进入多方安全计算的作业执行界面，单击创建。

图 1-8 创建作业

步骤2 在作业界面中，按照1~4提供的案例和SQL语句进行作业测试。

图 1-9 作业界面



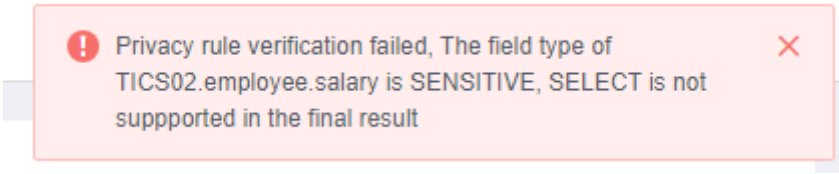
1. 假设有人输入以下代码试图直接查询敏感数据。

```
select
  tax_bal, id
from
  league_creator.tax
```

 版权所有 © 华为技术有限公司

2. 系统提示不支持进行敏感数据的SELECT操作。

图 1-10 不支持敏感操作



3. 若试图在敏感数据中追加自己的数据， 从结果倒推敏感数据，即求原数据。

```
Select
  tax_bal + electric_bal
from
  LEAGUE_CREATOR.tax a
  join ZZZZZZ.power_data b on a.id = b.id
```

4. TICS会识别并提示。

图 1-11 执行失败告警

----结束

说明

上述隐私规则，均为TICS系统提供的默认规则。

1.4 阶段三：审批防护

开启审批防护功能

前提条件

完成**隐私规则防护**。

操作步骤

步骤1 敏感数据被查询时，可以在审批详情中，看到是否使查询敏感数据的结果可见，可由该提供方进行识别，并进行拒绝操作。

 版权所有 © 华为技术有限公司

图 1-12 审批详情

步骤2 在审批详情中也可看到两个字段相加的情况，如下图所示。

 版权所有 © 华为技术有限公司

图 1-13 字段相加

步骤3 通过查看字段是否可见，以及字段用途，能够确认该字段的应用是否符合自己的安全预期。

----结束

1.5 阶段四：基本计算能力验证

验证TICS的基础计算能力，以计算各企业在2021年的价值评分，用于评估信贷能力，其中的公式仅为简单的参考计算式。

前提条件

完成**审批防护**。

操作步骤

步骤1 执行如下的sql作业。

```
select
  c.id as `企业id`,
  0.5 * a.tax_bal + 0.8 * b.supp_bal + (0.05 * c.electric_bal + 0.05 * c.water_bal) * 0.1  as `企业评分`
from
  Partner1.TAX a,
  Partner1.SUPPORT b,
  Partner2.POWER_DATA c
where
  b.id = c.id
  and a.id = b.id
```

 版权所有 © 华为技术有限公司

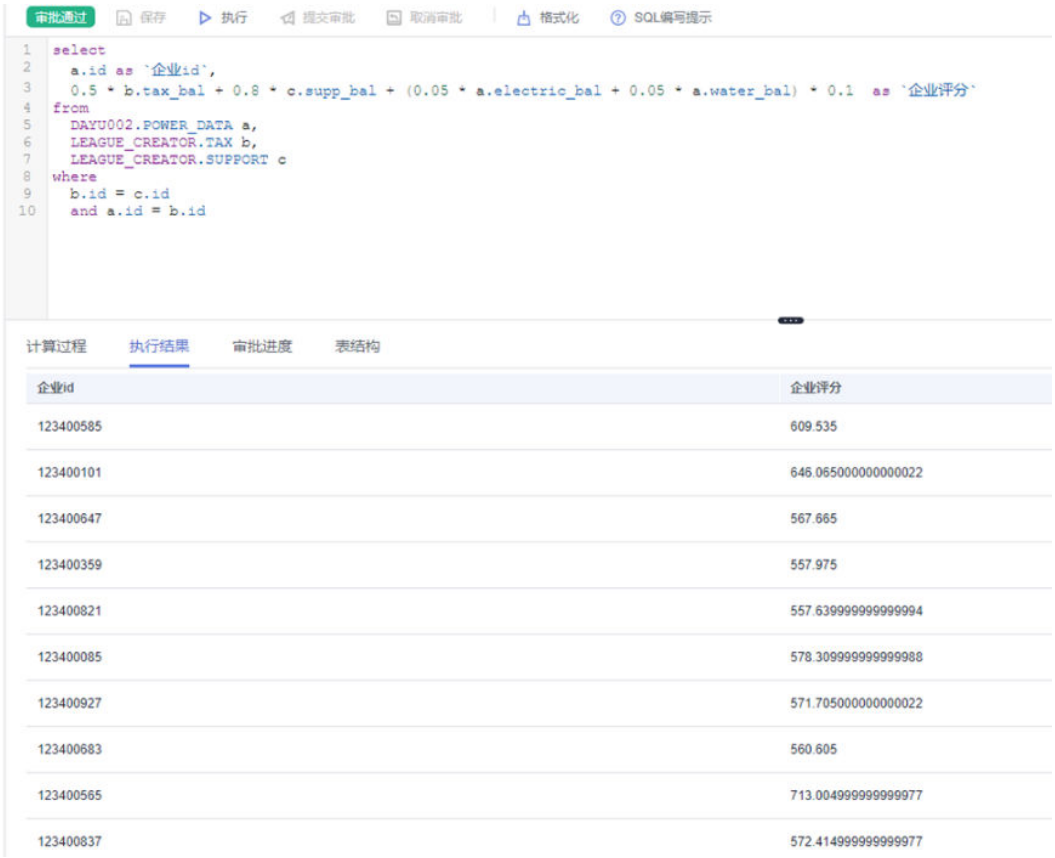
步骤2 审批时可以看到如下的信息，涉及关联字段较多，其使用方式都能够在审批界面中展示出来。

图 1-14 基础信息

步骤3 执行结果如下。

 版权所有 © 华为技术有限公司

图 1-15 执行结果



步骤4 结果显示，TICS支持大量基础的SQL语法。

图 1-16 SQL 编写提醒

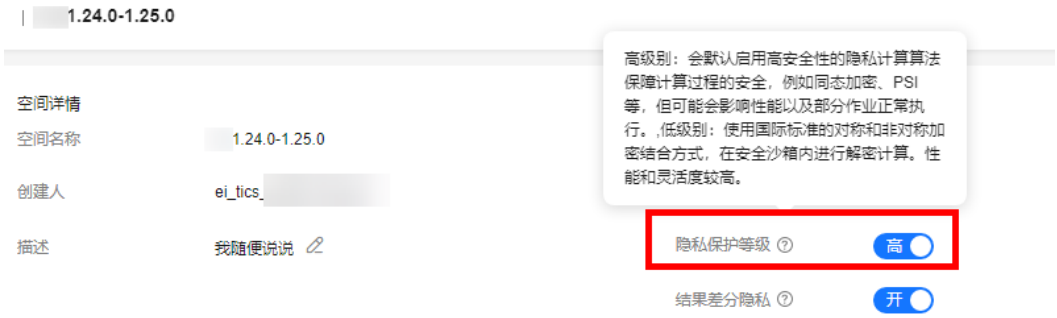
----结束

 版权所有 © 华为技术有限公司

1.6 阶段五：基于 MPC 算法的高安全级别计算

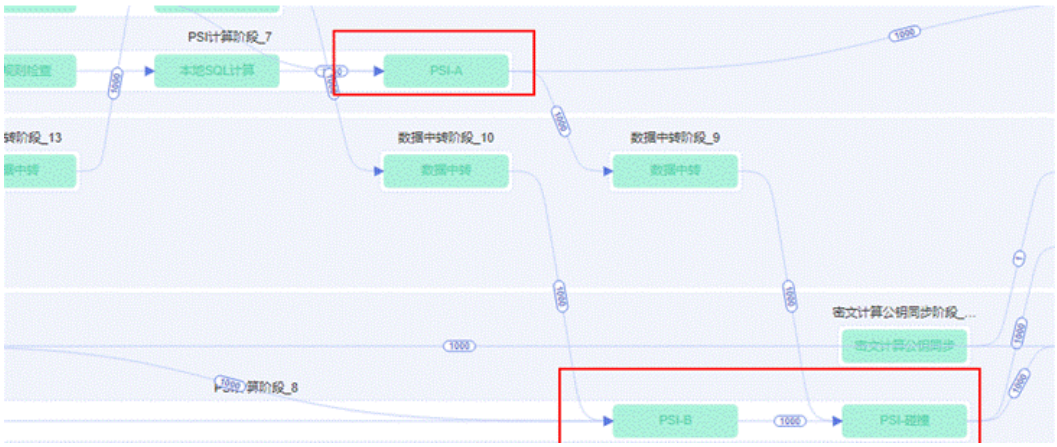
完成demo验证阶段，为提升数据保护级别，接入以**纯密文的状态做计算**的更高安全级别的数据，可以通过开启高隐私级别开关，提升空间安全级别。

图 1-17 高隐私级别开关



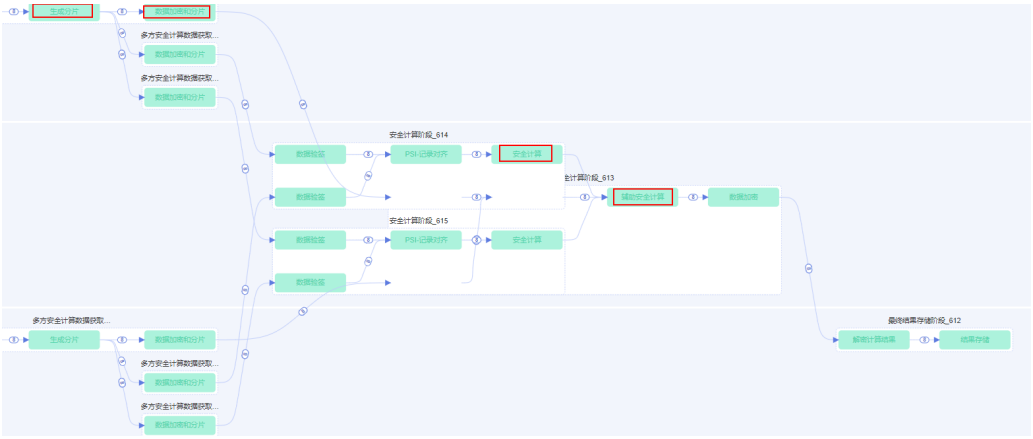
再次单击作业，审批进行的同时敏感数据被进行了秘密分享加密。DAG图显示了“psi + 秘密分享”的全过程流向，基本符合业界已公开的PSI算法流程和秘密分享流程。

图 1-18 加密流程



版权所有 © 华为技术有限公司

图 1-19 加密流程



1.7 阶段六：统计型作业的差分隐私保护

本示例作业，以统计各行业的“企业税收总和”与“用电量总和”，进行统计分析：

```
Select
  industry,
  sum(tax_bal),
  sum(electric_bal)
from
  LEAGUE_CREATOR.tax a join
  dayu002.power_data b
  on a.id = b.id
group by
  industry
```

⚠ 注意

统计分析型的作业，可能被作业执行方通过增删某个碰撞的id，得到两次作业之间的差值，从而推算出实际taxpay和water_fee。

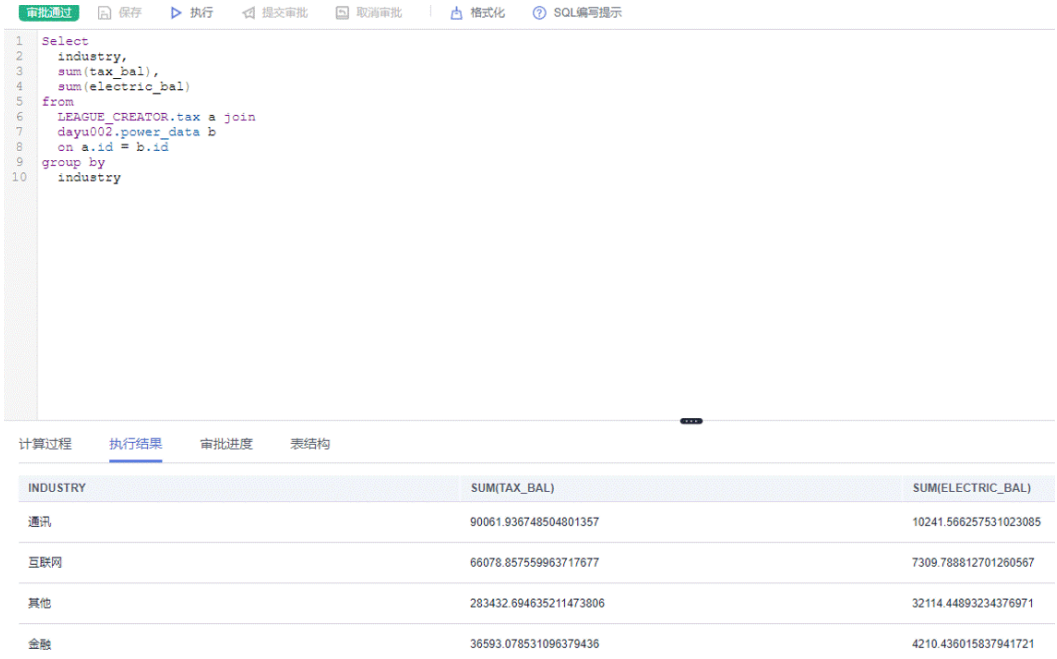
步骤1 开启空间中的差分隐私开关保护敏感数据，符合差分隐私条件的统计作业，会自动应用差分隐私算法对计算结果进行加噪保护， 在一定误差范围内保证数据无法被恶意偷取。

图 1-20 差分隐私开关

步骤2 第一次执行作业的结果如下：

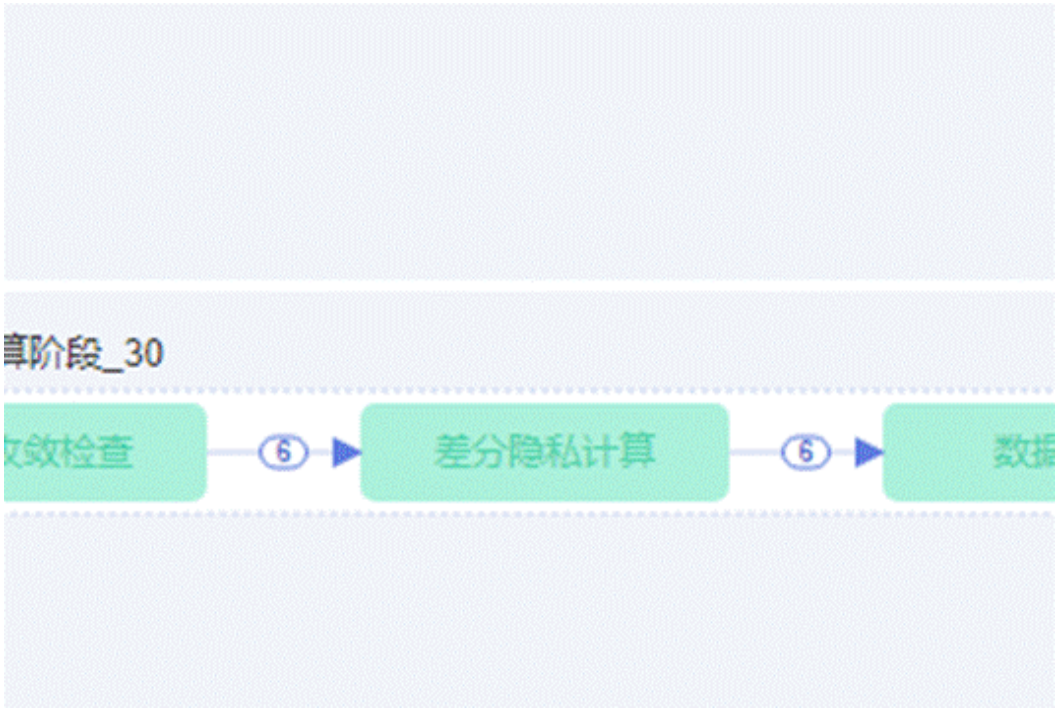
 版权所有 © 华为技术有限公司

图 1-21 作业结果



步骤3 在返回最终统计结果前，增加了一个差分隐私计算的任务节点，如图3所示。

图 1-22 差分隐私计算任务节点



步骤4 再执行如下sql，sql中过滤掉了某个企业，试图用差值去计算这个企业的税收值。

```
Select
  industry,
  sum(tax_bal),
  sum(electric_bal)
from
  LEAGUE_CREATOR.tax a join
```


版权所有 © 华为技术有限公司

```
  dayu002.power_data b
  on a.id = b.id
  where a.id <> '123400558'
group by
  industry
```

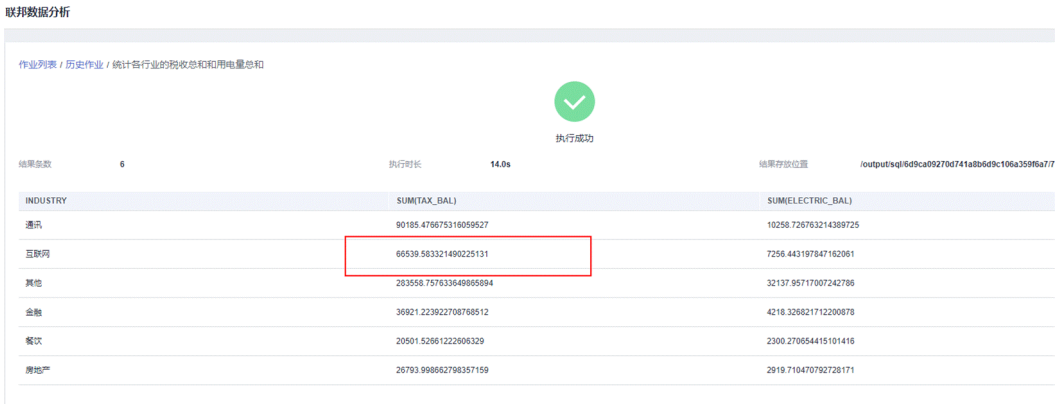
这个企业的实际tax为274：

图 1-23 tax

```
id,tax_bal,industry
123400558,274,互联网
```

得到新的结果如下：

图 1-24 新结果



经过计算，66539.583321490225131-66078.857559963717677=461，

通过差分隐私算法保护聚合操作的安全性，使开启算法保护的计算差值与预期得到的实际差值274不同，避免真实数据被窃取。

----结束

 版权所有 © 华为技术有限公司