可信智能计算服务

用户指南

文档版本	01
发布日期	2025-07-24

华为技术有限公司

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。

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

目 录

1 TICS 使用简介

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。

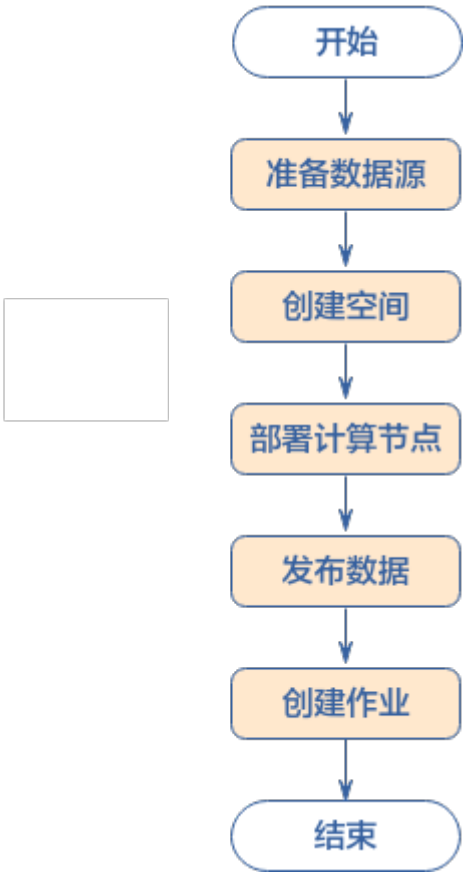
- **合作方**

  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



2 准备工作

2.1 准备工作简介

如果您是第一次使用TICS，需要完成以下准备工作：

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）

2.2 注册账号并实名认证

账号是您访问华为云的责任主体，有关账号的详细介绍请参见**账号中心**。此处介绍如何注册一个华为账号。若您已有华为账号，可以略过此部分内容。

1. 打开华为云网站**www.huaweicloud.com**。
2. 单击页面右上角的“注册”按钮。
3. 在注册页面，根据页面提示完成账号注册。

为了能够给您提供更好的云服务使用体验，建议您优先完成实名认证。实名认证分为个人账号和企业账号认证，不同账号类型认证的方法请参考以下链接。若您的账号已通过实名认证，可以略过此部分内容。

- **个人账号如何完成实名认证**
- **企业账号如何完成实名认证**

说明

- 实名认证信息提交后，请耐心等待审核结果，最长3个工作日内完成审核。
- 实名认证通过后需要40分钟才能生效。

2.3 配置 CCE 服务

背景信息

如果您规划在购买TICS服务时选择基于“**云租户部署**”，则您在购买TICS服务前需要对CCE服务进行相关配置，避免影响TICS服务的正常使用。

⚠ 注意

请自行关注部署节点的系统安全防护与配置加固，确保机器在安全的前提下进行隐私计算节点部署。

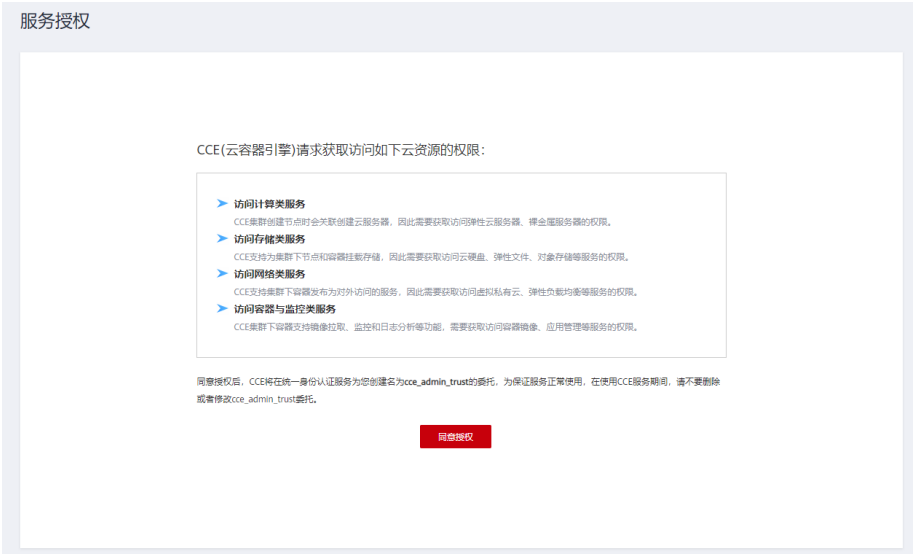
CCE 服务委托授权

由于CCE在运行中对计算、存储、网络以及监控等各类云服务资源都存在依赖关系，因此当您首次登录CCE控制台时，CCE将自动请求获取当前区域下的云资源权限，从而更好地为您提供服务。

说明

CCE的服务授权为全局配置，只要您所使用的账号在当前Region曾经进行过服务授权，则无需重新配置，可以跳过本节操作。

图 2-1 服务授权



当您同意授权后，CCE将在IAM中创建名为“cce_admin_trust”委托，统一使用系统账户“op_svc_cce”对您的其他云服务资源进行操作，cce_admin_trust委托具有Tenant Administrator权限。Tenant Administrator拥有除IAM管理外的全部云服务管理员权限，用于对CCE所依赖的其他云服务资源进行调用，且该授权仅在当前区域生效。关于资源委托详情，您可参考**委托**进行了解。

2.4 配置 IEF 服务

背景信息

如果您规划在购买TICS服务时选择基于“**边缘节点部署**”，则您在购买TICS服务前需要对IEF服务进行相关配置，避免影响TICS服务的正常使用。

⚠ 注意

请自行关注部署节点的系统安全防护与配置加固，确保机器在安全的前提下进行隐私计算节点部署。

IEF 服务委托授权

使用主账号访问IEF服务首页，单击“同意授权”，IEF将在统一身份认证服务为您创建名为ief_admin_trust的委托。

图 2-2 IEF 服务授权

ief_admin_trust委托具有Tenant Administrator权限。Tenant Administrator拥有除IAM管理外的全部云服务管理员权限，用于对IEF所依赖的其他云服务资源进行调用，且该授权仅在当前区域生效。

2.5 TICS 服务委托授权

背景信息

为保证正常创建TICS服务，需要先设置服务委托。

前提条件

- 服务授权需要主账号或者admin用户组中的子账号进行操作。
- 授权委托需查看IAM委托列表，如果存在名为tics_admin_trust的委托和tics_role_trust的权限，需要先删除。

服务授权操作

步骤1 进入TICS服务控制台，为保证正常创建TICS服务，需要先设置服务委托。

步骤2 进入计算节点购买页面，在“部署配置”区域，设置部署方式为“边缘节点部署”，在弹出的对话框单击“同意授权”。

同意授权后，TICS将在统一身份认证服务IAM下为您创建名为tics_admin_trust的委托，委托绑定的权限名为tics_role_trust。授权成功后，可以进入委托列表查看。

图 2-3 授权访问权限名

说明

委托tics_admin_trust和权限tics_role_trust创建成功后，请勿删除。

表 2-1 TICS 委托权限列表

权限名	详细信息	备注
tics_role_trust	TICS服务计算节点依赖IEF作为底层资源，因此需要tics_role_trust角色来部署应用。	由于云服务缓存需要时间，该权限3分钟左右才能生效。

----结束

2.6 购买 TICS 服务

前提条件

购买TICS服务前，已完成**配置CCE服务**、**配置IEF服务**和**TICS服务委托授权**。

购买 TICS 服务并进入控制台

购买TICS服务即创建空间。一个空间的成员包括组织方和合作方。用户参与的空间情况，可以在“空间管理”中查看。

1. 以主账号登录管理控制台。在控制台左上方，单击“服务列表”按钮 ☰ ，选择“EI企业智能 > 可信智能计算服务 TICS”，进入TICS控制台。

   如果需要以IAM子账号购买TICS服务，则需要先授予IAM子账号相应权限，详情请参见**创建TICS服务时依赖的CCE权限**和**创建TICS服务时依赖的IEF权限**。
2. 在TICS控制台页面，单击“购买可信智能计算服务”。

   配置购买参数，各参数说明如**表2-2**和**表2-3**所示。

表 2-2 空间信息配置参数

参数名称	样例	说明
区域	华北-北京四	选择服务的区域，不同区域的资源之间内网不互通。
项目	cn-north-4	选择该区域内的项目。
空间名称	TICS-test	由用户自定义，用以区分各个空间。要求：空间名称不允许重复，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。
区块链存证	打开	若您希望空间启用区块链服务（BCS）来审计任务信息，请打开此选项。 使用前需要按照**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。
区块链签名证书	-	上传签名证书文件（选择按照**启用区块链审计服务（可选）**章节步骤七描述中保存至本地的证书文件“/msp/signcert/xxx.pem”）。
区块链私钥文件	-	上传私钥证书文件（选择按照**启用区块链审计服务（可选）**章节步骤七描述中保存至本地的证书文件“/msp/keystore/xxx_sk”）

表 2-3 计算节点配置参数

参数名	样例	参数描述
计费方式	包年/包月	当前仅支持“包年/包月”。
购买时长	1个月	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	企业版	当前可选版本只包含企业版
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）	-	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**获取访问密钥**章节。AK、SK需与用户当前所在的项目保持一致。 **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。
加密密钥（SK）	-	
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。
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。
支持国密	否	若选择是，则登录计算节点必须使用国密浏览器（如奇安信浏览器）。
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		

参数名	样例	参数描述
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	样例	参数描述
部署规格	中规格	• 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。

参数名	样例	参数描述
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
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。

3. 确认无误后单击下一步并提交订单。
4. 付款成功，显示空间部署和可信计算节点部署，二者部署成功后即可在首页看到已创建的空间。

2.7 授权 IAM 用户使用 TICS

如果您需要对您所拥有的TICS进行精细的权限管理，您可以使用统一身份认证服务（Identity and Access Management，简称IAM）。通过IAM，您可以：

- 根据企业的业务组织，在您的华为账号中，给企业中不同职能部门的员工创建IAM用户，让员工拥有唯一安全凭证，并使用TICS资源。
- 根据企业用户的职能，设置不同的访问权限，以达到用户之间的权限隔离。
- 将TICS资源委托给更专业、高效的其他华为账号或者云服务，这些账号或者云服务可以根据权限进行代运维。

如果华为账号已经能满足您的要求，不需要创建独立的IAM用户，您可以跳过本章节，不影响您使用TICS服务的其它功能。

本章节为您介绍对用户授权的方法，操作流程如**创建IAM用户并授予TICS权限**所示。

背景信息

给用户组授权之前，请您了解用户组可以添加的TICS系统策略，并结合实际需求进行选择。TICS支持的系统权限，请参见**TICS权限管理**。

创建 IAM 用户并授予 TICS 权限

1. 创建用户组并授权。使用华为账号登录IAM控制台，创建用户组，并授予TICS的普通用户操作权限，如“TICS CommonOperations”。

   创建用户组并授权的具体操作，请参见**创建用户组并授权**。

   说明

   配置用户组的TICS权限时，注意选择权限的作用范围为“区域级项目”，搜索框中输入权限名“TICS”进行搜索，然后勾选需要授予用户组的权限，如“TICS CommonOperations”。

2. 创建用户并加入用户组。在IAM控制台创建用户，并将其加入步骤**1**中创建的用户组。

   创建用户并加入用户组的具体操作，请参见**创建用户并加入用户组**。

创建 TICS 服务时依赖的 CCE 权限

如果您需要授予IAM用户基于“**云租户部署**”购买TICS服务的权限，则您需要为用户组配置系统角色CCE Administrator和OBS Administrator。

1. 创建用户组tics_cce_min。

   图 2-4 创建用户组

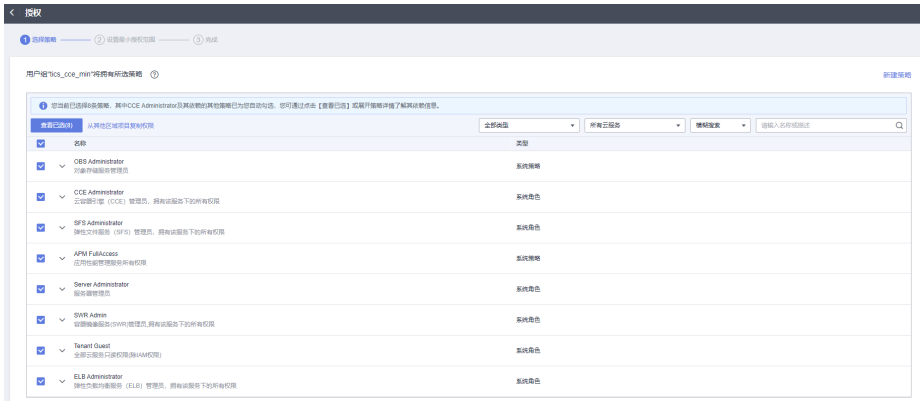
2. 为用户组授权。

   单击用户组后的“授权”后进入选择策略界面，选择系统角色CCE Administrator和OBS Administrator完成授权。

说明

选择CCE Administrator和OBS Administrator系统角色后，系统会自动勾选其依赖的其他系统角色，因此实际中授权更多的系统角色。

图 2-5 授权



3. 将所需授权的用户加入用户组tics_cce_min，即可为用户授予相关权限。
4. 创建cce类型的计算节点之后，假如需要缩小权限，可自行把子用户从tics_cce_min用户组中删除。

创建 TICS 服务时依赖的 IEF 权限

如果您需要授予IAM用户基于“**边缘节点部署**”购买TICS服务的权限，则您需要为用户组配置IEF服务的自定义策略tics-ief-iam-min和系统角色IEF Administrator。

1. 创建自定义策略tics-ief-iam-min，主要内容为创建IEF所需的iam权限。

图 2-6 创建自定义策略

策略内容如下：

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "iam:agencies:listAgencies",
                "iam:permissions:listRolesForAgency",
                "iam:roles:getRole"
            ]
        }
    ]
}
```

图 2-7 策略内容

2. 创建用户组tics_ief_min。

图 2-8 创建用户组

3. 为用户组授权。

   单击用户组后的“授权”后进入选择策略界面，选择自定义策略tics-ief-iam-min和IEF Administrator系统角色完成授权。

图 2-9 授权

4. 将所需授权的用户加入用户组tics_ief_min，即可为用户授予相关权限。

2.8 准备数据

（可选）准备 MRS Hive 数据源

如果您的数据需通过MRS Hive发布到TICS，则您需要提前准备MRS Hive数据源。

准备数据步骤如下：

步骤1 购买MRS服务，操作步骤参考**创建集群**章节，且MRS服务的VPC必须与计算节点部署节点处于同一个VPC内。

注意事项：

- “区域”必须与CCE集群在同一个VPC下。

图 2-10 区域配置

- “Kerberos”认证无论是否勾选，当前的MRS Hive连接器都支持。
- “虚拟私有云”与后续要建立的CCE集群必须在同一个VPC下。
- “安全组”建议在同一个安全组内且对同组节点开放必要端口。

步骤2 准备MRS Hive用户，操作步骤参考**准备开发用户**。需要注意的是用户必须具有Hive权限以及对应库表的访问权限。

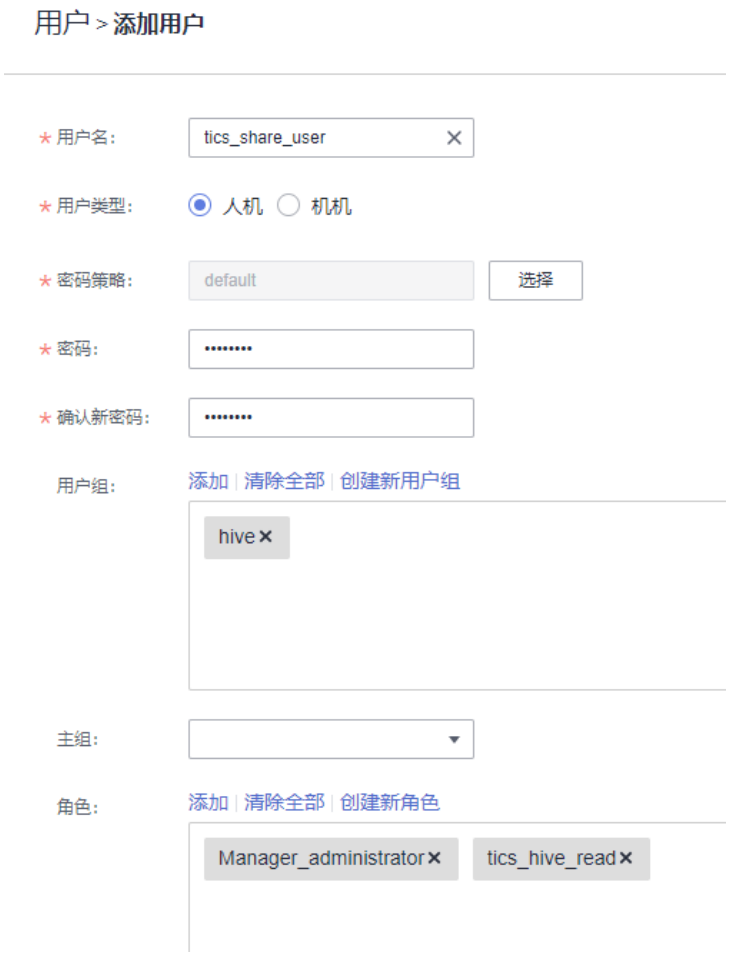
如果要创建MRS安全集群的数据连接，不能使用admin用户。因为admin用户是默认的管理页面用户，这个用户无法作为安全集群的认证用户来使用。您可以参考以下步骤创建一个新的MRS用户：

1. 使用admin账号登录MRS Manager页面。
2. 单击“系统 > 权限 > 角色管理”，选择添加角色，角色名称为“tics_hive_read”，配置角色权限依次单击“***集群名***> Hive > Hive读写权限”，勾选后续需要发布的Hive库表的读或者写权限。

图 2-11 添加角色权限

3. 登录MRS Manager，在页面的“系统设置”中，单击“用户管理”，在用户管理页面，添加用户，添加一个专有用户作为Kerberos认证用户，并且为这个用户添加用户组和分配角色权限，用户组至少选择Hive组，角色至少要勾选新建的角色（用于访问Hive）和Manager_administrator（用于下载安全认证配置），然后根据页面提示完成用户的创建。

图 2-12 新建用户



4. 使用新建的用户登录MRS Manager页面，更新初始密码。

步骤3 将数据资源导入MRS中的Hive，操作步骤参考**从零开始使用Hive**中关于导入数据的描述。

步骤4 配置安全组，操作步骤请参考**如何配置安全组**。

安全组配置示例

该步骤是为了确保计算节点的部署节点能够与该MRS集群通信以获取Hive数据。

一种方式是让计算节点与MRS集群的master节点处于同一个安全组。

另一个方式，是配置MRS集群的安全组策略，开放部分端口提供给计算节点。

必须确保互通的ip和端口：

- KrbServer的ip，以及tcp端口21730 和udp端口（21732，21731）
- zookeeper的ip和端口（2181）
- Hive-server的ip和端口（10000）
- MRS Manager的TCP端口（9022）

参考如下：

图 2-13 添加入方向规则

----结束

（可选）准备 RDS（MySQL）数据源

如果您的数据需通过RDS（MySQL）发布到TICS，则您需要提前准备RDS（MySQL）数据源。

JDBC数据源支持原生MySQL及RDS（MySQL）的连接。这里介绍RDS（MySQL）准备数据的步骤：

步骤1 购买RDS服务，操作步骤参考**购买RDS（MySQL）数据库实例**，且RDS服务的VPC必须与计算节点部署节点处于同一个VPC内。

参数配置注意事项：

- “区域”必须与后续要建立的CCE集群在同一个区域下。
- “虚拟私有云”与CCE集群必须在同一个VPC下。
- “安全组”/usermanual-rds/rds_05_0019.html建议在同一个安全组内且对同组节点开放数据库端口。
- 当前暂不支持开启“SSL连接”。

步骤2 准备数据库数据及访问用户，操作步骤参考**数据库与用户创建**。需要注意的是的访问用户必须具有对应库表的访问权限。

步骤3 将数据导入RDS库表中。

步骤4 在RDS服务控制台，单击实例名进入RDS实例，在“连接管理 -> 安全组规则”处配置安全组。确保数据库端口对计算节点开放。

----结束

（可选）准备 DWS 数据源

如果您的数据需通过DWS发布到TICS，则您需要提前准备DWS数据源。

JDBC数据源支持DWS（GaussDB SQL）的连接，目前仅支持默认数据库为postgres的DWS数据源。这里介绍DWS（GaussDB SQL）准备数据的步骤：

步骤1 购买DWS服务，选择默认数据库为postgres的数仓，创建DWS集群，操作步骤参考**创建DWS集群**。

参数配置注意事项：

- “安全组”建议自动创建安全组，或选择与计算节点在同一个安全组内且对同组节点开放数据库端口。
- 当前暂不支持开启“SSL连接”。
- 若购买“公网访问”，按照实际带宽需求来进行购买。

步骤2 准备数据库数据及访问用户。需要注意的是访问用户必须具有对应库表的访问权限。

步骤3 将数据导入DWS库表中。

步骤4 在DWS服务控制台，单击实例名进入DWS集群详情页面，在“网络 -> 安全组”，检查安全组配置。确保数据库端口对计算节点开放。

----结束

（可选）准备 API 数据源

如果您的数据需通过API发布到TICS，则您需要提交准备API数据源。

1. 目前API数据源支持基础认证方式。
2. API数据源可以是GET或者POST请求。
3. API数据源的返回格式如下，使用json格式

[{"id":"1","x0":"3232","x1":15}]

准备本地横向联邦数据资源

1. 上传数据集文件（作业参与方）

   上传数据集文件到计算节点挂载路径下，供计算节点执行的脚本读取。如果是主机挂载，上传到宿主机的挂载路径下。如果是OBS挂载，使用华为云提供的对象存储服务，上传到当前计算节点使用的对象桶中。

   图 2-14 对象桶名称

   此处以主机挂载为例：

   a. 创建一个主机挂载的计算节点Agent1，挂载路径为/tmp/tics1/。

   b. 使用文件上传工具上传包含数据集iris1.csv的dataset文件夹到宿主机/tmp/tics1/目录下。

      iris1.csv内容如下：

      ```
      sepal_length,sepal_width,petal_length,petal_width,class
      5.1,3.5,1.4,0.3,Iris-setosa
      ```

```
5.7,3.8,1.7,0.3,Iris-setosa
5.1,3.8,1.5,0.3,Iris-setosa
5.4,3.4,1.7,0.2,Iris-setosa
5.1,3.7,1.5,0.4,Iris-setosa
4.6,3.6,1,0.2,Iris-setosa
5.1,3.3,1.7,0.5,Iris-setosa
4.8,3.4,1.9,0.2,Iris-setosa
5,3,1.6,0.2,Iris-setosa
5,3.4,1.6,0.4,Iris-setosa
5.2,3.5,1.5,0.2,Iris-setosa
5.2,3.4,1.4,0.2,Iris-setosa
4.7,3.2,1.6,0.2,Iris-setosa
4.8,3.1,1.6,0.2,Iris-setosa
5.4,3.4,1.5,0.4,Iris-setosa
5.2,4.1,1.5,0.1,Iris-setosa
5.5,4.2,1.4,0.2,Iris-setosa
4.9,3.1,1.5,0.1,Iris-setosa
5,3.2,1.2,0.2,Iris-setosa
5.5,3.5,1.3,0.2,Iris-setosa
4.9,3.1,1.5,0.1,Iris-setosa
4.4,3,1.3,0.2,Iris-setosa
5.1,3.4,1.5,0.2,Iris-setosa
5,3.5,1.3,0.3,Iris-setosa
4.5,2.3,1.3,0.3,Iris-setosa
4.4,3.2,1.3,0.2,Iris-setosa
5,3.5,1.6,0.6,Iris-setosa
5.1,3.8,1.9,0.4,Iris-setosa
4.8,3,1.4,0.3,Iris-setosa
5.1,3.8,1.6,0.2,Iris-setosa
4.6,3.2,1.4,0.2,Iris-setosa
5.3,3.7,1.5,0.2,Iris-setosa
5,3.3,1.4,0.2,Iris-setosa
6.8,2.8,4.8,1.4,Iris-versicolor
6.7,3,5,1.7,Iris-versicolor
6,2.9,4.5,1.5,Iris-versicolor
5.7,2.6,3.5,1,Iris-versicolor
5.5,2.4,3.8,1.1,Iris-versicolor
5.5,2.4,3.7,1,Iris-versicolor
5.8,2.7,3.9,1.2,Iris-versicolor
6,2.7,5.1,1.6,Iris-versicolor
5.4,3,4.5,1.5,Iris-versicolor
6,3.4,4.5,1.6,Iris-versicolor
6.7,3.1,4.7,1.5,Iris-versicolor
6.3,2.3,4.4,1.3,Iris-versicolor
5.6,3,4.1,1.3,Iris-versicolor
5.5,2.5,4,1.3,Iris-versicolor
5.5,2.6,4.4,1.2,Iris-versicolor
6.1,3,4.6,1.4,Iris-versicolor
5.8,2.6,4,1.2,Iris-versicolor
5,2.3,3.3,1,Iris-versicolor
5.6,2.7,4.2,1.3,Iris-versicolor
5.7,3,4.2,1.2,Iris-versicolor
5.7,2.9,4.2,1.3,Iris-versicolor
6.2,2.9,4.3,1.3,Iris-versicolor
5.1,2.5,3,1.1,Iris-versicolor
5.7,2.8,4.1,1.3,Iris-versicolor
6.3,3.3,6,2.5,Iris-virginica
5.8,2.7,5.1,1.9,Iris-virginica
7.1,3,5.9,2.1,Iris-virginica
6.3,2.9,5.6,1.8,Iris-virginica
6.5,3,5.8,2.2,Iris-virginica
7.6,3,6.6,2.1,Iris-virginica
4.9,2.5,4.5,1.7,Iris-virginica
7.3,2.9,6.3,1.8,Iris-virginica
6.7,2.5,5.8,1.8,Iris-virginica
7.2,3.6,6.1,2.5,Iris-virginica
6.5,3.2,5.1,2,Iris-virginica
6.4,2.7,5.3,1.9,Iris-virginica
6.8,3,5.5,2.1,Iris-virginica
```



```
5.7,2.5,5,2,Iris-virginica
5.8,2.8,5.1,2.4,Iris-virginica
6.4,3.2,5.3,2.3,Iris-virginica
6.5,3,5.5,1.8,Iris-virginica
7.7,3.8,6.7,2.2,Iris-virginica
7.7,2.6,6.9,2.3,Iris-virginica
6,2.2,5,1.5,Iris-virginica
6.9,3.2,5.7,2.3,Iris-virginica
5.6,2.8,4.9,2,Iris-virginica
7.7,2.8,6.7,2,Iris-virginica
6.3,2.7,4.9,1.8,Iris-virginica
6.7,3.3,5.7,2.1,Iris-virginica
7.2,3.2,6,1.8,Iris-virginica
```

c. 为了使容器内的计算节点程序有权限能够读取到文件，使用命令chown -R 1000:1000 /tmp/tics1/修改挂载目录下的文件的属主和组为1000:1000。

d. 在第二台主机上创建计算节点Agent2，挂载路径为/tmp/tics2/。上传包含数据集iris2.csv的dataset文件夹到宿主机目录下，修改属主。

iris2.csv的内容如下：

```
sepal_length,sepal_width,petal_length,petal_width,class
5.1,3.5,1.4,0.2,Iris-setosa
4.9,3,1.4,0.2,Iris-setosa
4.7,3.2,1.3,0.2,Iris-setosa
4.6,3.1,1.5,0.2,Iris-setosa
5,3.6,1.4,0.2,Iris-setosa
5.4,3.9,1.7,0.4,Iris-setosa
4.6,3.4,1.4,0.3,Iris-setosa
5,3.4,1.5,0.2,Iris-setosa
4.4,2.9,1.4,0.2,Iris-setosa
4.9,3.1,1.5,0.1,Iris-setosa
5.4,3.7,1.5,0.2,Iris-setosa
4.8,3.4,1.6,0.2,Iris-setosa
4.8,3,1.4,0.1,Iris-setosa
4.3,3,1.1,0.1,Iris-setosa
5.8,4,1.2,0.2,Iris-setosa
5.7,4.4,1.5,0.4,Iris-setosa
5.4,3.9,1.3,0.4,Iris-setosa
7,3.2,4.7,1.4,Iris-versicolor
6.4,3.2,4.5,1.5,Iris-versicolor
6.9,3.1,4.9,1.5,Iris-versicolor
5.5,2.3,4,1.3,Iris-versicolor
6.5,2.8,4.6,1.5,Iris-versicolor
5.7,2.8,4.5,1.3,Iris-versicolor
6.3,3.3,4.7,1.6,Iris-versicolor
4.9,2.4,3.3,1,Iris-versicolor
6.6,2.9,4.6,1.3,Iris-versicolor
5.2,2.7,3.9,1.4,Iris-versicolor
5,2,3.5,1,Iris-versicolor
5.9,3,4.2,1.5,Iris-versicolor
6,2.2,4,1,Iris-versicolor
6.1,2.9,4.7,1.4,Iris-versicolor
5.6,2.9,3.6,1.3,Iris-versicolor
6.7,3.1,4.4,1.4,Iris-versicolor
5.6,3,4.5,1.5,Iris-versicolor
5.8,2.7,4.1,1,Iris-versicolor
6.2,2.2,4.5,1.5,Iris-versicolor
5.6,2.5,3.9,1.1,Iris-versicolor
5.9,3.2,4.8,1.8,Iris-versicolor
6.1,2.8,4,1.3,Iris-versicolor
6.3,2.5,4.9,1.5,Iris-versicolor
6.1,2.8,4.7,1.2,Iris-versicolor
6.4,2.9,4.3,1.3,Iris-versicolor
6.6,3,4.4,1.4,Iris-versicolor
6.8,2.8,4.8,1.4,Iris-versicolor
6.2,2.8,4.8,1.8,Iris-virginica
6.1,3,4.9,1.8,Iris-virginica
6.4,2.8,5.6,2.1,Iris-virginica
7.2,3,5.8,1.6,Iris-virginica
```

```
7.4,2.8,6.1,1.9,Iris-virginica
7.9,3.8,6.4,2,Iris-virginica
6.4,2.8,5.6,2.2,Iris-virginica
6.3,2.8,5.1,1.5,Iris-virginica
6.1,2.6,5.6,1.4,Iris-virginica
7.7,3,6.1,2.3,Iris-virginica
6.3,3.4,5.6,2.4,Iris-virginica
6.4,3.1,5.5,1.8,Iris-virginica
6,3,4.8,1.8,Iris-virginica
6.9,3.1,5.4,2.1,Iris-virginica
6.7,3.1,5.6,2.4,Iris-virginica
6.9,3.1,5.1,2.3,Iris-virginica
5.8,2.7,5.1,1.9,Iris-virginica
6.8,3.2,5.9,2.3,Iris-virginica
6.7,3.3,5.7,2.5,Iris-virginica
6.7,3,5.2,2.3,Iris-virginica
6.3,2.5,5,1.9,Iris-virginica
6.5,3,5.2,2,Iris-virginica
6.2,3.4,5.4,2.3,Iris-virginica
5.9,3,5.1,1.8,Iris-virginica
```

2. 准备模型文件/初始权重（作业发起方）

   作业发起方需要提供模型、初始权重（非必须），上传到Agent1的挂载目录下并使用命令chown -R 1000:1000 /tmp/tics1/修改挂载目录下的文件的属主和组。

   使用python代码创建模型文件，保存为二进制文件model.h5，以鸢尾花为例，生成如下的模型：

```
import tensorflow as tf
import keras

model = keras.Sequential([
    keras.layers.Dense(4, activation=tf.nn.relu, input_shape=(4,)),
    keras.layers.Dense(6, activation=tf.nn.relu),
    keras.layers.Dense(3, activation='softmax')
])

model.compile(loss='categorical_crossentropy', optimizer='adam', metrics=['accuracy'])
model.save("d:/model.h5")
```

   初始权重的格式是浮点数的数组，与模型对应。使用联邦学习训练出来的结果result_1可以作为初始权重，样例如下：

```
-0.23300957679748535,0.7804553508758545,0.0064492723904550076,0.5866460800170898,0.676144003868103,-0.7883696556091309,0.5472091436386108,-0.20961782336235046,0.58524489402771,-0.5075979598426818848,-0.47474920749664307,-0.3519996106624603,-0.10822880268096924,-0.5457949042320251,-0.28117161989212036,-0.7369481325149536,-0.04728877171874046,0.003856887575238943,0.051739662885665894,0.033792052417993546,-0.31878742575645447,0.7511205673217773,0.3158722519874573,-0.7290999293327332,0.7187696695327759,0.09846954792737961,-0.06735057383775711,0.7165604829788208,-0.730293869972229,0.4473201036453247,-0.27151209115982056,-0.6971480846405029,0.7360773086547852,0.819558322429657,0.4984433054924011,0.05300116539001465,-0.6597640514373779,0.7849202156066895,0.6896201372146606,0.11731931567192078,-0.5380218029022217,0.18895208835601807,-0.18693888187408447,0.357051283121109,0.05440644919872284,0.042556408792734146,-0.04341210797429085,0.0,-0.04367709159851074,-0.031455427408218384,0.24731603264808655,-0.062861368060112,-0.4265706539154053,0.32981523871421814,-0.021271884441375732,0.15228557586669922,0.1818728893995285,0.4162319302558899,-0.22432318329811096,0.7156463861465454,-0.13709741830825806,0.7237883806228638,-0.5489991903305054,0.47034209966659546,-0.04692812263965607,0.7690137028694153,0.40263476967811584,-0.4405142068862915,0.016018997877836227,-0.04845477640628815,0.037553105503320694
```

3. 编写训练脚本（作业发起方）

   作业发起方还需要编写联邦学习训练脚本，其中需要用户自行实现读取数据、训练模型、评估模型、获取评估指标的逻辑。计算节点会将数据集配置文件中的path属性作为参数传递给训练脚本。

   JobParam属性如下：

```
class JobParam:
    """训练脚本参数
    """
```



```
    # 作业id
    job_id = ''
    # 当前轮数
    round = 0
    # 迭代次数
    epoch = 0
    # 模型文件路径
    model_file = ''
    # 数据集路径
    dataset_path = ''
    # 是否仅做评估
    eval_only = False
    # 权重文件
    weights_file = ''
    # 输出路径
    output = ''
    # 其他参数json字符串
    param = ''
```

鸢尾花的训练脚本iris_train.py样例如下：

```
# -*- coding: utf-8 -*-
import getopt
import sys
from sklearn.model_selection import train_test_split
from sklearn.preprocessing import LabelBinarizer
import keras
import pandas as pd
import horizontal.horizontallearning as hl
def train():
    # 解析命令行输入
    jobParam = JobParam()
    jobParam.parse_from_command_line()
    job_type = 'evaluation' if jobParam.eval_only else 'training'
    print(f"Starting round {jobParam.round} {job_type}")

    # 加载模型，设置初始权重参数
    model = keras.models.load_model(jobParam.model_file)
    hl.set_model_weights(model, jobParam.weights_file)
    # 加载数据、训练、评估 -- 用户自己实现
    print(f"Load data {jobParam.dataset_path}")
    train_x, test_x, train_y, test_y, class_dict = load_data(jobParam.dataset_path)
    if not jobParam.eval_only:
        b_size = 1
        model.fit(train_x, train_y, batch_size=b_size, epochs=jobParam.epoch, shuffle=True, verbose=1)
        print(f"Training job [{jobParam.job_id}] finished")
    eval = model.evaluate(test_x, test_y, verbose=0)
    print("Evaluation on test data: loss = %0.6f accuracy = %0.2f%% \n" % (eval[0], eval[1] * 100))
    # 结果以json格式保存 -- 用户读取评估指标
    result = {}
    result['loss'] = eval[0]
    result['accuracy'] = eval[1]
    # 生成结果文件
    hl.save_train_result(jobParam, model, result)
# 读取CSV数据集，并拆分为训练集和测试集
# 该函数的传入参数为CSV_FILE_PATH: csv文件路径
def load_data(CSV_FILE_PATH):

    IRIS = pd.read_csv(CSV_FILE_PATH)
    target_var = 'class'  # 目标变量
    # 数据集的特征
    features = list(IRIS.columns)
    features.remove(target_var)
    # 目标变量的类别
    Class = IRIS[target_var].unique()
    # 目标变量的类别字典
    Class_dict = dict(zip(Class, range(len(Class))))
    # 增加一列target, 将目标变量进行编码
    IRIS['target'] = IRIS[target_var].apply(lambda x: Class_dict[x])
    # 对目标变量进行0-1编码(One-hot Encoding)
    lb = LabelBinarizer()
```



```
    lb.fit(list(Class_dict.values()))
    transformed_labels = lb.transform(IRIS['target'])
    y_bin_labels = []  # 对多分类进行0-1编码的变量
    for i in range(transformed_labels.shape[1]):
        y_bin_labels.append('y' + str(i))
        IRIS['y' + str(i)] = transformed_labels[:, i]
    # 将数据集分为训练集和测试集
    train_x, test_x, train_y, test_y = train_test_split(IRIS[features], IRIS[y_bin_labels],
                                                        train_size=0.7, test_size=0.3, random_state=0)
    return train_x, test_x, train_y, test_y, Class_dict
class JobParam:
    """训练脚本参数
    """
    # required parameters
    job_id = ''
    round = 0
    epoch = 0
    model_file = ''
    dataset_path = ''
    eval_only = False

    # optional parameters
    weights_file = ''
    output = ''
    param = ''

    def parse_from_command_line(self):
        """从命令行中解析作业参数
        """
        opts, args = getopt.getopt(sys.argv[1:], 'hn:w:',
                                   ['round=', 'epoch=', 'model_file=', 'eval_only', 'dataset_path=',
                                    'weights_file=', 'output=', 'param=', 'job_id='])
        for key, value in opts:
            if key in ['--round']:
                self.round = int(value)
            if key in ['--epoch']:
                self.epoch = int(value)
            if key in ['--model_file']:
                self.model_file = value
            if key in ['--eval_only']:
                self.eval_only = True
            if key in ['--dataset_path']:
                self.dataset_path = value
            if key in ['--weights_file']:
                self.weights_file = value
            if key in ['--output']:
                self.output = value
            if key in ['--param']:
                self.param = value
            if key in ['--job_id']:
                self.job_id = value
if __name__ == '__main__':
    train()
```

准备本地纵向联邦数据资源

纵向联邦学习的数据方分为标签方（数据集中有标签列的一方）和特征方（数据集中没有标签列的一方），目前仅支持CSV格式的文本文件，以及包含CSV文本的数据目录。目录数据集下必须至少包含一个CSV文件，且多个CSV文件表头结果必须保持一致。以下示例中如果没有特别说明，一般都是CSV格式的文件。

例如，标签方有30条数据，每条数据有1列ID、7列特征和1列标签：

```
ID,f1,f2,f3,f4,f5,f6,f7,LABEL
0,2,7,27,92,950,1128,1139,1
1,2,8,17,157,763,1127,1140,1
2,1,9,12,48,846,1129,1131,1
3,2,8,28,113,1119,1126,1136,0
4,1,6,37,313,762,1127,1132,1
```



```
5,2,6,28,329,718,1128,1136,1
6,2,6,29,114,592,1127,1140,1
7,2,7,26,153,927,1127,1132,1
8,2,10,28,161,1000,1127,1136,0
9,2,8,30,117,762,1127,1140,1
10,2,8,23,176,841,1126,1136,0
11,1,10,23,176,928,1127,1140,1
12,2,8,23,53,624,1126,1136,1
13,1,8,23,70,455,1126,1140,1
14,2,10,17,177,791,1126,1138,1
15,2,7,29,156,429,1128,1131,0
16,2,6,28,304,999,1127,1140,1
17,2,7,12,48,446,1126,1136,1
18,2,6,27,372,1000,1127,1131,0
19,1,8,20,343,1106,1128,1131,0
20,2,8,38,301,1039,1128,1136,0
21,1,8,30,134,768,1128,1139,0
22,2,7,26,294,636,1129,1140,1
23,1,7,16,101,944,1127,1136,0
24,2,8,11,43,834,1129,1140,0
25,2,7,32,175,1040,1129,1136,0
26,1,7,22,196,787,1127,1136,1
27,1,10,29,74,555,1127,1131,0
28,1,8,21,364,984,1128,1140,1
29,2,8,15,85,718,1128,1140,1
```

特征方有30条数据，每条数据有1列ID和6列特征：

```
ID,f8,f9,f10,f11,f12,f13
0,20,642,1559,1864,1877,2617
1,67,341,1158,1872,1878,2616
2,28,522,1400,1857,1876,2627
3,50,593,1505,1866,1877,2549
4,57,196,1006,1873,1877,2632
5,50,99,907,1866,1877,2313
6,67,348,1165,1872,1878,2627
7,57,132,940,1873,1877,2628
8,50,401,1248,1866,1877,2933
9,67,336,1152,1872,1878,2632
10,50,394,1241,1866,1877,2057
11,67,448,1303,1872,1878,2627
12,50,221,1033,1866,1877,1975
13,11,113,921,1872,1877,2632
14,14,305,1118,1865,1877,2627
15,61,628,1542,1857,1876,2627
16,67,341,1158,1872,1878,2616
17,50,603,1515,1866,1877,2617
18,62,320,1135,1857,1876,2627
19,28,205,1015,1857,1876,2617
20,50,160,968,1866,1877,2064
21,42,418,1269,1864,1877,2630
22,36,235,1047,1859,1877,2616
23,50,97,905,1866,1877,2064
24,1,191,1001,1874,1878,2837
25,50,226,1038,1866,1877,1930
26,50,391,1238,1866,1877,1936
27,56,565,1456,1857,1876,2627
28,71,513,1383,1872,1878,2617
29,67,336,1152,1872,1878,2634
```

参考**准备本地横向联邦数据资源 -> 上传数据集文件**，将该文件上传到**两个不同计算节点**的挂载路径下，即完成纵向联邦数据集配置。

如果数据集文件不含有csv文件表头，需要用户提供额外的配置文件用来说明数据集每一列的信息。示例如下：

以上述特征方数据为例，没有表头的数据集文件示例：

```
0,20,642,1559,1864,1877,2617
1,67,341,1158,1872,1878,2616
2,28,522,1400,1857,1876,2627
```



```
3,50,593,1505,1866,1877,2549
4,57,196,1006,1873,1877,2632
5,50,99,907,1866,1877,2313
6,67,348,1165,1872,1878,2627
7,57,132,940,1873,1877,2628
8,50,401,1248,1866,1877,2933
9,67,336,1152,1872,1878,2632
10,50,394,1241,1866,1877,2057
11,67,448,1303,1872,1878,2627
12,50,221,1033,1866,1877,1975
13,11,113,921,1872,1877,2632
14,14,305,1118,1865,1877,2627
15,61,628,1542,1857,1876,2627
16,67,341,1158,1872,1878,2616
17,50,603,1515,1866,1877,2617
18,62,320,1135,1857,1876,2627
19,28,205,1015,1857,1876,2617
20,50,160,968,1866,1877,2064
21,42,418,1269,1864,1877,2630
22,36,235,1047,1859,1877,2616
23,50,97,905,1866,1877,2064
24,1,191,1001,1874,1878,2837
25,50,226,1038,1866,1877,1930
26,50,391,1238,1866,1877,1936
27,56,565,1456,1857,1876,2627
28,71,513,1383,1872,1878,2617
29,67,336,1152,1872,1878,2634
```

为尽可能说明配置文件（.json）中的各参数写法，典型示例如下，其中参数介绍如**表2-4**所示。

```
{
   "schema": [
    {
      "column_name": "id",
      "data_type": "INTEGER",
      "is_unique_id": true,
      "column_sensitive_level": "SENSITIVE",
      "feature_type": "CONTINUOUS",
      "privacy_policy": "NONE",
      "comments": "id_Description"
    },
    {
      "column_name": "x0",
      "data_type": "FLOAT",
      "is_unique_id": false,
      "column_sensitive_level": "SENSITIVE",
      "feature_type": "CONTINUOUS",
      "privacy_policy": "NONE"
    },
    {
      "column_name": "x1",
      "data_type": "FLOAT",
      "is_unique_id": false,
      "column_sensitive_level": "NON_SENSITIVE",
      "feature_type": "DISCRETE",
      "privacy_policy": "NONE"
    },
    {
      "column_name": "x2",
      "data_type": "FLOAT",
      "is_unique_id": false,
      "column_sensitive_level": "NON_SENSITIVE",
      "feature_type": "MULTIHOT",
      "privacy_policy": "MASK"
    },
    {
      "column_name": "x3",
      "data_type": "FLOAT",
      "is_unique_id": false,
```



```
    "column_sensitive_level": "NON_SENSITIVE",
    "feature_type": "MULTIHOT",
    "privacy_policy": "NONE"
   },
   {
    "column_name": "x4",
    "data_type": "FLOAT",
    "is_unique_id": false,
    "column_sensitive_level": "NON_SENSITIVE",
    "feature_type": "MULTIHOT",
    "privacy_policy": "NONE"
   },
   {
    "column_name": "x5",
    "data_type": "FLOAT",
    "is_unique_id": false,
    "column_sensitive_level": "NON_SENSITIVE",
    "feature_type": "MULTIHOT",
    "privacy_policy": "NONE"
   },
   {
    "column_name": "x6",
    "data_type": "FLOAT",
    "is_unique_id": false,
    "column_sensitive_level": "NON_SENSITIVE",
    "feature_type": "CONTINUOUS",
    "privacy_policy": "NONE"
   }
  ],
  "ext": {
        "multihot_settings": [{
              "features": ["x2", "x3"],
               "field_size": 30
        },
        {
               "features": ["x4", "x5"],
               "field_size": 25
        }]
  }
}
```

表 2-4 配置文件参数介绍

参数	介绍
***column_name**	必选参数，字段名称。
***data_type**	必选参数，字段类型。 当前支持的取值为：INTEGER、FLOAT、STRING。
is_unique_id	true：表示该字段为唯一标识。 false：表示该字段为非唯一标识。
column_sensitive_level	SENSITIVE：表示该字段敏感。 NON_SENSITIVE：表示该字段非敏感。
feature_type	CONTINUOUS：表示该字段特征类型为连续。 DISCRETE：表示该字段特征类型为离散。 MULTIHOT：表示该字段特征类型为MULTIHOT。当数据集需要配置MULTIHOT分组时，配置文件需要添加ext字段，补充multihot_settings信息。

参数	介绍
privacy_policy	NONE：表示该字段不需要脱敏。 MASK：表示该字段需要脱敏。

如果数据集文件不包含ID，该数据集将不能进行样本对齐，且特征选择、联邦训练、评估时会校验特征方、标签方的数据量是否相等，若不相等作业会报错。用户可以提供额外的数据ID文件用来说明数据每一行的ID。以上述特征数据集为例，有表头没有ID的数据集文件和数据ID文件格式如下：

数据集文件内容：

```
f8,f9,f10,f11,f12,f13
20,642,1559,1864,1877,2617
67,341,1158,1872,1878,2616
28,522,1400,1857,1876,2627
50,593,1505,1866,1877,2549
57,196,1006,1873,1877,2632
50,99,907,1866,1877,2313
67,348,1165,1872,1878,2627
57,132,940,1873,1877,2628
50,401,1248,1866,1877,2933
67,336,1152,1872,1878,2632
50,394,1241,1866,1877,2057
67,448,1303,1872,1878,2627
50,221,1033,1866,1877,1975
11,113,921,1872,1877,2632
14,305,1118,1865,1877,2627
61,628,1542,1857,1876,2627
67,341,1158,1872,1878,2616
50,603,1515,1866,1877,2617
62,320,1135,1857,1876,2627
28,205,1015,1857,1876,2617
50,160,968,1866,1877,2064
42,418,1269,1864,1877,2630
36,235,1047,1859,1877,2616
50,97,905,1866,1877,2064
1,191,1001,1874,1878,2837
50,226,1038,1866,1877,1930
50,391,1238,1866,1877,1936
56,565,1456,1857,1876,2627
71,513,1383,1872,1878,2617
67,336,1152,1872,1878,2634
```

数据ID文件内容：

```
id
0
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
```

```
19
20
21
22
23
24
25
26
27
28
29
```

准备本地多方安全计算数据资源

本地多方安全计算数据目前仅支持csv格式的文本文件。以下示例中如果没有特别说明，一般都是CSV格式的文件。

例如，数据表中有三列字段：

```
employee_id,name,salary
491915,tony,5000
491916,mark,7000
491917,jack,9000
491918,tom,9000
491919,hony,9000
500000,jim,20000
500001,tom,9000
500002,hony,9000
```

参考**准备本地横向联邦数据资源 -> 上传数据集文件**，将该文件上传到计算节点的挂载路径下，即完成多方安全计算数据集配置。

如果数据集文件不含有csv文件表头，需要用户提供额外的配置文件用来说明数据集每一列的信息。以上述标签方数据集为例，没有表头的数据集文件和数据配置文件的格式如下：

```
491915,tony,5000
491916,mark,7000
491917,jack,9000
491918,tom,9000
491919,hony,9000
500000,jim,20000
500001,tom,9000
500002,hony,9000
```

配置文件（.json）：

```
{
  "schema": [
    {
      "column_name": "employee_id",
      "data_type": "STRING",
      "is_unique_id": true,
      "column_sensitive_level": "SENSITIVE",
      "privacy_policy": "NONE"
    },
    {
      "column_name": "name",
      "data_type": "STRING",
      "is_unique_id": false,
      "column_sensitive_level": "NON_SENSITIVE",
      "privacy_policy": "MASK"
    },
    {
      "column_name": "salary",
      "data_type": "INTEGER",
      "is_unique_id": false,
```



```
    "column_sensitive_level": "SENSITIVE",
    "privacy_policy": "NONE"
   },
 ]
}
```

表 2-5 配置文件参数介绍

参数	介绍
***column_name**	必选参数，字段名称。
***data_type**	必选参数，字段类型。 当前支持的取值为：INTEGER、FLOAT、STRING。
is_unique_id	true：表示该字段为唯一标识。 false：表示该字段为非唯一标识。
column_sensitive_level	SENSITIVE：表示该字段敏感。 NON_SENSITIVE：表示该字段非敏感。
feature_type	CONTINUOUS：表示该字段特征类型为连续。 DISCRETE：表示该字段特征类型为离散。 MULTIHOT：表示该字段特征类型为MULTIHOT。当数据集需要配置MULTIHOT分组时，配置文件需要添加ext字段，补充multihot_settings信息。
privacy_policy	NONE：表示该字段不需要脱敏。 MASK：表示该字段需要脱敏。

2.9 启用区块链审计服务（可选）

若您希望空间启用区块链服务（BCS）来审计任务信息，请仔细阅读本章节。

步骤1 空间发起方需要根据**基于CCE集群创建联盟链**完成联盟链的创建过程。

说明

“区块链类型”参数值需要选择“联盟链”，否则将影响后续操作。

步骤2 发起方按照**组建联盟链**中“邀请成员”部分的描述，邀请参与方加入联盟链。

步骤3 参与方登录区块链服务（BCS）按照**组建联盟链**中“同意/拒绝邀请”部分的描述，创建BCS实例并加入联盟链。

步骤4 发起方、参与方各自根据**合约仓库**章节中下载模板的描述，下载“数据上链存证和查询合约模板（又称链代码）”并保存到本地。

步骤5 发起方、参与方各自按照**链代码管理**章节中“安装链代码”部分的描述，上传步骤4中已保存至本地的链代码压缩包。

注意事项：

- “链代码名称”参数值须为“ticsrule”。

- “链代码版本”须为“1.0”。
- 勾选需要背书的组织及Peer节点。

  说明

  链代码背书的组织名称必须选择organization。

步骤6 发起方按照**链代码管理**章节中“实例化链代码”部分的描述，完成实例化链代码操作。

注意事项：

- “**初始化函数**”参数值须为“init”。
- “**背书策略**”勾选“任意组织背书”

完成上述步骤后用户可前往**区块浏览器**查看上链的初始化日志信息。

----结束

2.10 参考：获取认证信息

在使用TICS时，您可能需要获取访问密钥、项目ID等信息，获取方式如下：

获取访问密钥

您可以通过如下方式获取访问密钥。

1. 登录控制台，在用户名下拉列表中选择“我的凭证”。
2. 进入“我的凭证”页面，选择“访问密钥 > 新增访问密钥”，如**图2-15**所示。

图 2-15 单击新增访问密钥

3. 单击“确定”，根据浏览器提示，保存密钥文件。密钥文件会直接保存到浏览器默认的下载文件夹中。打开名称为“credentials.csv”的文件，即可查看访问密钥（Access Key Id和Secret Access Key）。

   说明

   - 每个用户仅允许新增两个访问密钥。
   - 为保证访问密钥的安全，访问密钥仅在初次生成时自动下载，后续不可再次通过管理控制台界面获取。请在生成后妥善保管。

获取项目 ID 和账号 ID

项目ID表示租户的资源，账号ID对应当前账号。用户可在对应页面下查看不同Region对应的项目ID和账号ID。

1. 注册并登录管理控制台。
2. 在用户名的下拉列表中单击“我的凭证”。

3. 在“API凭证”页面，查看账号名和账号ID，在项目列表中查看项目ID。

2.11 配置 IEF 高可用节点

IEF高可用节点实现该功能要手动操作，使用rsync命令在多台虚机间定时同步文件，操作步骤如下：

说明

以下教程适用于ECS机器系统为Centos 7.5。操作前需要购买两台同网段同文件系统的ecs节点A与节点B。

步骤1 在两台虚机上安装rsync及corntab服务，已安装则跳过（HCS底座发行的系统镜像是默认安装的；客户提供的机器，需要客户运维侧保障）。

步骤2 参照**如何在两个节点间免密ssh登录**完成节点免密设置。

步骤3 在节点A任意目录下创建该脚本sync_tics.sh，建议放在 /opt/tics目录下，确保脚本文件具备可执行权限。

```
#!/bin/bash
if [[ -n $(docker ps | grep k8s_db) ]];then
  echo "has install postgres"
  rsync -avzrog --exclude=postmaster.pid /var/lib/tics_db/ 对端节点ip:/var/lib/tics_db/
fi
  chmod 755 /home/tics/
  rsync -avzrog /home/tics/ 对端节点ip:/home/tics/
```

步骤4 在节点A上执行如下命令启动定时同步任务。

```
crontab -e
```

在弹出的编辑框中输入。

```
*/1 * * * *  /opt/tics/sync_tics.sh
```

保存后退出。

步骤5 在节点B上重复**步骤3~步骤4**操作，注意**步骤3**中脚本内容应替换为对端节点A的ip。

说明

使用tail /var/log/cron 可以查看定时命令执行情况，务必保证同步命令执行正常。

----结束

如何在两个节点间免密 ssh 登录

步骤1 登录机器A，执行如下命令

```
ssh-keygen
```



```
[root@ecs-9662 ~]# ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_rsa
Your public key has been saved in /root/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:JKe58nBb03xRKFlHZegOxISRxeKgWs1cLmEW4i4npBs root@ecs-9662
The key's randomart image is:
+---[RSA 3072]----+
|       . ...0+.ooo|
|      . .= =o+o.. |
|     . oBo*oo...  |
|    o .o*= o....  |
|   E oo= S.  .o   |
|    o.+ . o   ..  |
|   . o o o o .    |
|      = o . .     |
|       o          |
+-----[SHA256]-----+
```

遇到需要Overwrite(y/n)时输入y，其他提示均回车即可

步骤2 在机器A上继续执行如下命令，按照提示输入B的登录密码即可

```
ssh-copy-id -i 图中红框部分 root@机器B的ip
```

注：以上操作为节点采用密钥登录，无密码的场景下

若所建节点采用密钥对登录的形式，可手动复制公钥文件id_rsa.pub到对端节点的指定用户的home路径下（root用户的路径为/root）

在对端节点下操作：

查看指定用户home目录下有无.ssh文件夹，没有的话创建一个，复制中的id_rsa.pub的内容到authorized_keys文件

```
[root@yuancheng ~]# cd .ssh
[root@yuancheng .ssh]# cat ../id_rsa.pub | tee -a authorized_keys
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQDINuohcfbWG8DMHY7mwnAIkp7jgUczOrk1ie5stdSF9GLroot@yuancheng
[root@yuancheng .ssh]# ll
total 12
-rw-r--r-- 1 root root  408 Aug 10 09:58 authorized_keys
```

设置authorized_keys文件的权限为600

步骤3 在机器B上执行1、2步骤。

步骤4 接下来两台机器，即可相互直接ssh不需要输入密码

----结束

2.12 配置 CCE 集群子账号权限

前提条件

已使用云租户部署计算节点。

操作步骤

步骤1 以主账号登录CCE管理控制台。

步骤2 在控制台左侧，单击“权限管理”，在“权限管理”页面，选择需要增加权限的CCE集群，单击右上角“添加权限”，进入添加权限页面。

图 2-16 CCE 管理控制台权限管理

步骤3 在添加权限页面，在用户下拉框选择需要添加权限的子账号，权限类型选择“运维权限”，然后单击右下角“确认”按钮。

图 2-17 添加子用户权限

----结束

2.13 购买 Model Lite 资源池

前提条件

已购买ModelArts服务。

操作步骤

步骤1 以主账号登录ModelArts管理控制台。

步骤2 在控制台左下方，单击“专属资源池”下拉框，选择“弹性集群”，进入资源池创建页面。

步骤3 在资源池创建页面，单击“创建”，进入购买专属资源池页面。

步骤4 进入购买专属资源池页面后，配置购买参数，各参数说明如表**表2-6**所示。

表 2-6 资源池配置参数

参数名称	说明	样例
名称	资源池的名称，创建时会随机生成一个名字。	pool-6e8a
描述	对创建的资源池进行说明。	-
使用场景	分为Standard弹性集群与Lite弹性集群，联邦学习对接MA需要选择Lite弹性集群。	ModelArts Lite
计费模式	选择Lite弹性集群目前默认包年/包月计费模式。	包年/包月
CCE集群	选择创建完成的CCE集群，如果没有可用的CCE集群，可单击右边的“创建集群”按钮，购买CCE集群。	-
自定义节点名称	集群节点名称，会随机生成，用户也可以根据自己需求来指定节点前缀名。	-
规格管理	选择规则类型、可用区、节点数量等。	-
购买时长	购买资源池的时间，用户可以根据续期选择，到期后，会自动清理。	-
自动续费	用户根据需求选择是否选择自动续费。	-

参数名称	说明	样例
登录方式	选择登录方式，有密码和密钥对两种方式。 ● 选择密码登录，默认用户名为“root”，需要设置密码用来登录节点后台。 ● 选择密钥对，需要选择密钥对，如果没有密钥对，可以单击右边“创建密钥对”按钮创建。	-

----结束

3 空间管理

3.1 组建空间

本章节将介绍如何通过TICS平台购买服务并组建空间。

空间是联邦计算的载体。合作方只有加入空间才能参与联邦计算。创建空间需要配置空间基本信息，包括空间的名称，版本类型等。

约束限制

- 创建空间时，空间名在创建者租户范围内唯一，即创建者不能创建同名的空间。
- 退出空间，参与方可单方面的退出空间，退出空间时会删除该参与方在这个空间的所有作业和注册的数据集。
- 删除空间时，只有空间创建者才能删除空间，且所有租户都选择同意删除，空间才算删除完成。
- 若需启用区块链审计服务，请先完成**启用区块链审计服务（可选）**中发起方角色涉及的操作，再创建空间。

创建空间

步骤1 用户登录TICS控制台。

步骤2 进入TICS控制台后，单击页面左侧“空间管理”，进入空间管理页面。

步骤3 在TICS控制台页面，单击“购买可信智能计算服务”。

配置购买参数，各参数说明如**表3-1**和**表3-2**所示。

表 3-1 空间信息配置参数

参数名称	样例	说明
区域	华北-北京四	选择服务的区域，不同区域的资源之间内网不互通。
项目	cn-north-4	选择该区域内的项目。

参数名称	样例	说明
空间名称	TICS-test	由用户自定义，用以区分各个空间。要求：空间名称不允许重复，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。
区块链存证	打开	若您希望空间启用区块链服务（BCS）来审计任务信息，请打开此选项。 使用前需要按照**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。
区块链签名证书	-	上传签名证书文件（选择按照**启用区块链审计服务（可选）**章节步骤七描述中保存至本地的证书文件“/msp/signcert/xxx.pem”）。
区块链私钥文件	-	上传私钥证书文件（选择按照**启用区块链审计服务（可选）**章节步骤七描述中保存至本地的证书文件“/msp/keystore/xxx_sk”）

表 3-2 计算节点配置参数

参数名	样例	参数描述
计费方式	包年/包月	当前仅支持“包年/包月”。
购买时长	1个月	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	企业版	当前可选版本只包含企业版
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。

参数名	样例	参数描述
访问密钥ID（AK）	-	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**获取访问密钥**章节。AK、SK需与用户当前所在的项目保持一致。 **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。
加密密钥（SK）	-	
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。
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。
支持国密	否	若选择是，则登录计算节点必须使用国密浏览器（如奇安信浏览器）。
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		

参数名	样例	参数描述
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		
部署规格	中规格	• 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

参数名	样例	参数描述
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	样例	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。

步骤4 参数配置完成后单击“立即创建”，完成创建空间操作。用户可在“空间管理”页面查看已创建的空间。

----结束

邀请成员

步骤1 用户登录TICS控制台。

步骤2 进入TICS控制台后，单击页面左侧“空间管理”，进入空间管理页面。

步骤3 在空间管理页面，打开“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”。

图 3-1 邀请合作方操作入口

步骤4 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”，保存后单击“确定”，完成邀请合作方操作。

“租户名称”是指合作方的华为账号，如何获取请参考**合作方如何获取租户名称**。

“租户别名”是合作方在TICS中的别名，由用户自定义即可，设置该参数的目的是保护合作方的信息安全。

图 3-2 添加合作方

----结束

删除成员

在邀请成员后，如果发现邀请错误且成员未接受邀请，可以将其在空间中删除。

步骤1 用户登录TICS控制台。

步骤2 进入TICS控制台后，单击页面左侧“空间管理”，进入空间管理页面。

步骤3 在空间管理页面，打开“我创建的空间”页签，查找需要删除成员的空间并单击“邀请合作方”，打开成员列表。

图 3-3 邀请合作方操作入口

步骤4 在弹出的界面单击“已有合作方列表”操作栏的删除图标。

图 3-4 删除合作方

----结束

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 用户登录TICS控制台。

步骤2 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3 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 3-5 通知管理入口

步骤4 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

下载计算节点配置信息

下载计算节点配置信息，下载的信息可在部署计算节点的时候导入。“空间信息”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。

配置包含空间证书，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 用户登录TICS控制台。

步骤2 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3 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。内容如下：

- json文件：对应空间配置，包含“空间区域”、“空间名称”、“空间ID”、“证书密码”等。
- p12文件：计算节点的密钥文件。
- jks文件：CA的“证书”，密钥和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。

图 3-6 下载计算节点配置

----结束

3.2 管理空间

查看空间详情

步骤1 空间发起人登录TICS控制台。

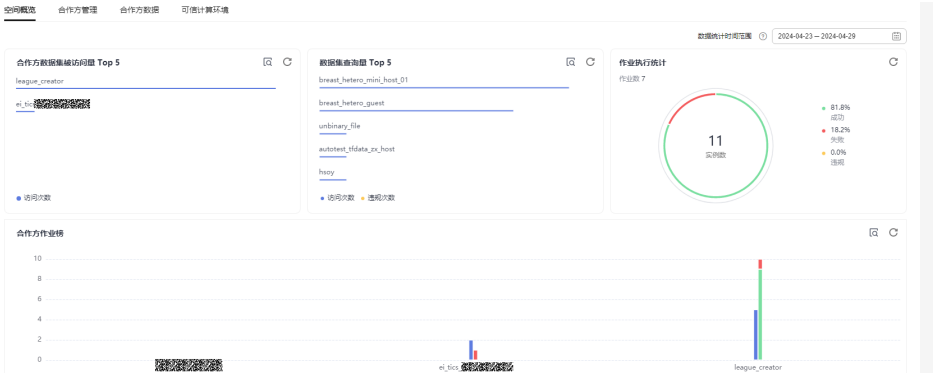
步骤2 进入TICS控制台后，单击页面左侧“空间管理”，进入空间管理页面。

步骤3 在“空间管理”页打开“我参与的空间”页签，单击“空间名称”进入详情页。

- **查看空间统计信息**

  在详情页下方单击“空间概览”页签查看空间统计信息，该统计信息不是实时的，当前只显示统计到前一天的数据。

图 3-7 空间统计信息



- **查看空间的合作方列表**

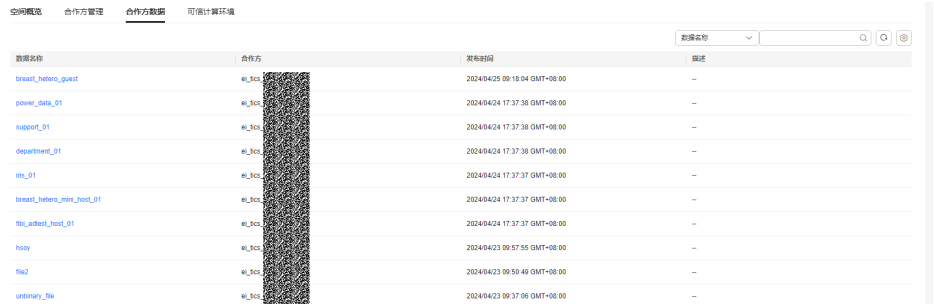
  在详情页下方单击“合作方管理”页签查看空间的合作方列表。

图 3-8 合作方列表

- **查看空间的合作方数据**

  在详情页下方单击“合作方数据”页签查看注册到空间的合作方数据列表。

图 3-9 合作方数据



- **查看可信计算环境**

  在详情页下方单击“可信计算环境”页签查看注册到空间的可信节点列表。

图 3-10 可信计算环境

----结束

修改空间配置

支持用户在空间详情页修改“空间描述信息”、“联合审批”开关、“隐私保护等级”开关、“结果差分隐私”开关。其中“联合审批”开关、“隐私保护等级”开关、“结果差分隐私”开关只有空间创建者可以修改。

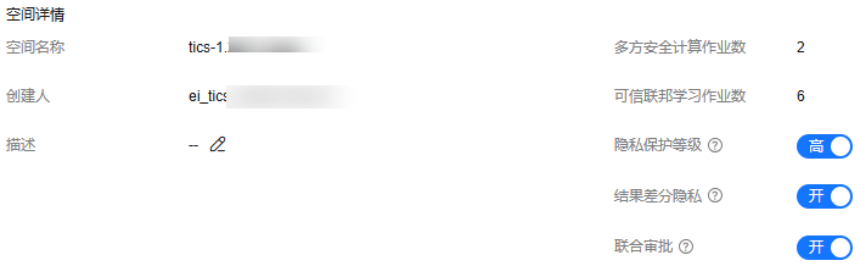
- 联合审批：启用后，所有作业均需经数据提供方审批，以确认SQL语句返回结果的安全性。若未启用，则使用TICS系统内置的隐私规则来识别语句安全性，并拒绝不符合要求的SQL作业。关闭时，需要经过所有合作方共同审批，全部通过后方可关闭，关闭审批详情可到“通知管理 > 联合审批通知”查看。
- 隐私保护等级：高级别时，默认启用高安全性的隐私计算的算法保障计算过程的安全，例如秘密分享加密、PSI等，但可能会影响性能以及部分作业正常执行。低级别时，使用国际标准的对称和非对称加密结合方式，在安全沙箱内进行解密计算。性能和灵活度较高。
- 结果差分隐私：开启时，使用差分隐私算法对多方安全计算作业的执行结果添加隐私保护，避免历史差分攻击。使用该功能会在计算节点发布数据集时将数据集信息的取值范围、频度进行统计，并同步到TICS中心节点。若需要已发布数据集支持差分隐私功能，需要通知所有合作方重新发布数据集。

步骤1 用户登录TICS控制台。

步骤2 进入TICS控制台后，单击页面左侧“空间管理”，进入空间管理页面。

步骤3 在“空间管理”页打开“我创建的空间”页签，单击“空间名称”进入详情页，查看详情并修改空间配置。

图 3-11 修改描述信息



----结束

退出空间

参与方可单方面的退出空间，退出时需要删除所有计算节点。

步骤1 用户登录TICS控制台。

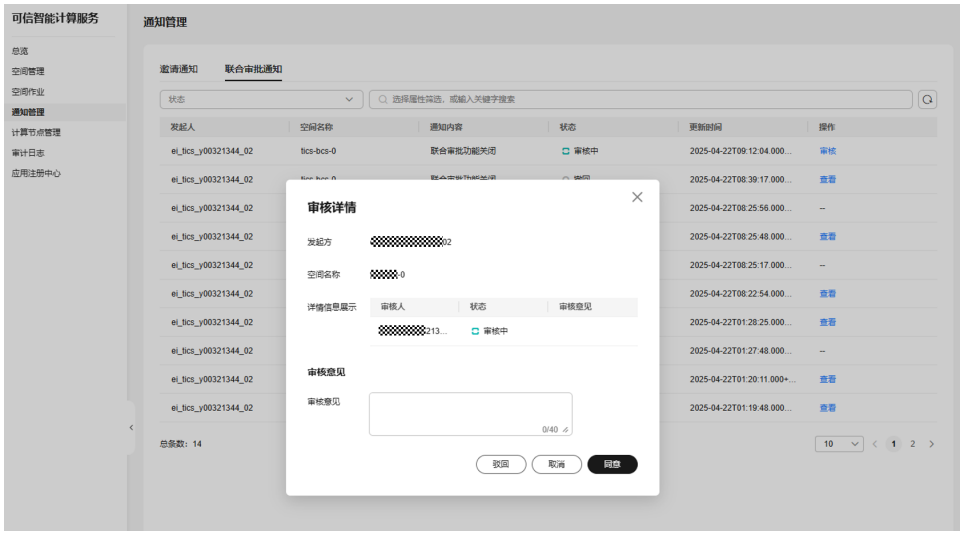
步骤2 进入TICS控制台后，单击页面左侧“空间管理”，进入空间管理页面。

步骤3 在“空间管理”页打开“我参与的空间”页签，查找待退出的空间，单击“退出空间”。

图 3-12 退出空间

步骤4 参与方在“通知管理”页打开“联合审批通知”页签，查看详情并审核相关通知。

图 3-13 查看联合审批通知



----结束

删除空间

用户不使用空间时，需要空间创建者删除空间。只有空间创建者才有删除空间的权限。

删除空间之前，需要先进行删除计算节点操作，否则会导致空间删除失败。

步骤1 用户登录TICS控制台。

步骤2 进入TICS控制台后，单击页面左侧“空间管理”，进入空间管理页面。

步骤3 在“空间管理”页打开“我创建的空间”页签，查找待删除的空间，单击“删除”进行删除。空间状态会更新为删除中。

图 3-14 删除空间

----结束

查看空间操作记录

TICS提供透明的空间操作记录。空间的创建、部署、删除、升级回滚操作都会被详细记录。

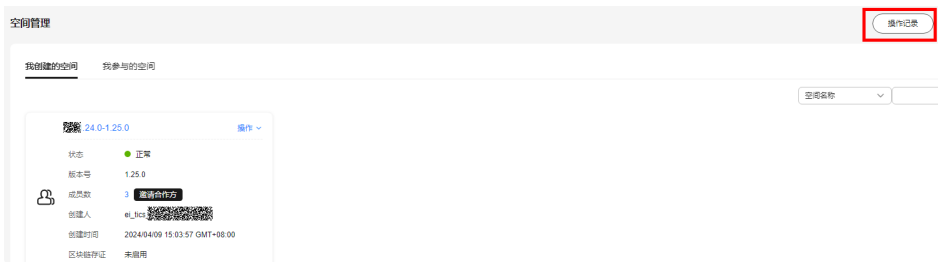
在详情中，操作进程以可视化的方式展示，清晰展示空间的部署、升级、回滚、删除步骤，在出现问题时便于分析排查。

步骤1 用户登录TICS控制台。

步骤2 进入TICS控制台后，单击页面左侧“空间管理”，进入空间管理页面。

步骤3 单击页面右上角的“操作记录”按钮，查看操作记录。

图 3-15 入口



步骤4 单击“查看详情”，可查看空间操作的具体信息。

图 3-16 查看详情

操作详情以可视化的形式展示，使操作进程更直观、更清晰。

图 3-17 可视化页面

----结束

3.3 空间升级与回滚

本章节将介绍如何对已创建的空间进行升级与回滚。

3.3.1 空间升级

约束限制

- 只有空间有新版本或者空间升级失败时，才能再次进行空间升级。
- 删除中的空间无法进行空间升级。
- 空间升级过程中会导致空间的不可用。
- 升级过程的相关操作记录将会保存。

- 由于1.20.0版本架构变化，如果需要跨1.20.0版本升级，则需要联系客服或技术支持人员，先刷新后台数据库，再通过TICS控制台进行空间升级。

警告

如果未刷新数据库，直接通过TICS控制台将TICS 1.20.0之前版本升级到1.20.0及后续版本，则会导致升级后业务功能故障、且无法回滚。

空间升级

步骤1 用户登录TICS控制台。

步骤2 进入TICS控制台后，单击页面左侧“空间管理”，进入空间管理页面。

步骤3 在“空间管理”页找到需要升级的空间，单击“操作 -> 升级”。等待升级完成后即可查看操作记录。

图 3-18 升级空间

----结束

3.3.2 空间回滚

约束限制

- 只有空间升级失败或者回滚失败，才能进行回滚。
- 删除中的空间无法进行空间回滚。
- 空间回滚的过程中会导致空间的不可用。
- 回滚过程的相关操作记录将会保存。

- 由于1.20.0版本架构变化，如果需要跨1.20.0版本回滚，则需要联系客服或技术支持人员，先刷新后台数据库，再通过TICS控制台进行空间回滚。

警告

如果未刷新数据库，直接通过TICS控制台将TICS 1.20.0及后续版本回滚到1.20.0之前版本，则会导致回滚后业务功能故障。

空间回滚

步骤1 用户登录TICS控制台。

步骤2 进入TICS控制台后，单击页面左侧“空间管理”，进入空间管理页面。

步骤3 在“空间管理”页找到需要回滚的空间，单击“操作 -> 回滚”。等待回滚完成后即可查看操作记录。

图 3-19 空间回滚

----结束

3.4 替换证书

为网络安全考虑，您需要定期更换证书，以免证书过期。

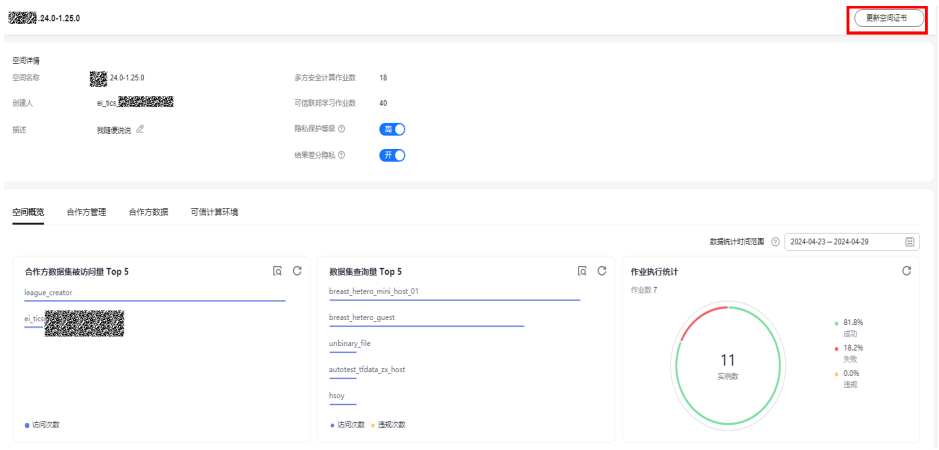
更新空间证书

步骤1 登录TICS控制台。

步骤2 进入TICS控制台后，单击页面左侧“空间管理”，进入空间管理页面。

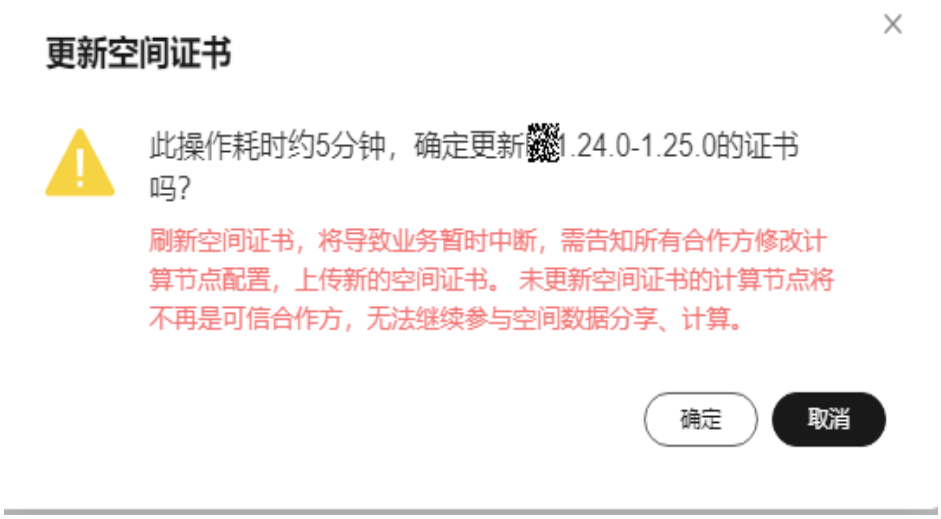
步骤3 进入空间详情页面，单击页面右上角的更新空间证书。

图 3-20 空间详情



步骤4 在弹出的提示框中阅读更新空间证书的注意事项，单击确定。

图 3-21 注意事项



步骤5 单击页面左侧“通知管理”，进入通知管理页面。

步骤6 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。内容如下：

- json文件：对应空间配置，包含“空间区域”、“空间名称”、“空间ID”、“证书密码”等。
- p12文件：计算节点的密钥文件。
- jks文件：CA的“证书”，密钥和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。

图 3-22 下载计算节点配置

步骤7 单击页面左侧“计算节点管理”，进入计算节点管理页面。在操作列单击“更多 ->配置变更”。

图 3-23 配置变更

步骤8 在配置变更的操作栏中添加步骤6的文件，单击确定。

图 3-24 添加配置变更文件

步骤9 配置变更成功，计算节点进入重启状态。待状态变为“运行中”，空间证书更新完成。

图 3-25 计算节点重启

----结束

4 计算节点管理

4.1 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，将数据上传，作为可信计算服务的输入，通过执行多方安全计算和可信联邦学习作业后，最终拿到结果。

计算节点以容器的形式部署，支持云容器引擎（CCE，Cloud Container Engine）服务和智能边缘平台（IEF，Intelligent EdgeFabric）服务部署，用户可根据数据上云的实际需求，采用合适的计算节点部署方案。

- 云容器引擎（CCE，Cloud Container Engine）提供高可靠高性能的企业级容器应用管理服务，支持Kubernetes社区原生应用和工具，简化云上自动化容器运行环境搭建。
- 智能边缘平台（Intelligent EdgeFabric）通过纳管您的边缘节点，提供将云上应用延伸到边缘的能力，联动边缘和云端的数据，满足客户对边缘计算资源的远程管控、数据处理、分析决策、智能化的诉求。同时，在云端提供统一的设备/应用监控、日志采集等运维能力，为企业提供完整的边缘和云协同的一体化服务的边缘计算解决方案。

前提条件

1. 本地存在下载好的空间信息和证书文件，下载方式参考**下载计算节点配置信息**。
2. 若需将执行过程记录审计至区块链，请确保当前加入的空间已开启区块链审计服务，同时完成**启用区块链审计服务（可选）**中对应角色（发起方/参与方）的准备工作，保证当前各参与方均处于区块空间链中。
3. 根据实际情况选择部署方式，参考**计算节点部署方式**，并执行相关操作。

约束限制

- IEF边缘节点部署计算节点：

  纳管节点只负责运行TICS的计算节点服务；每个纳管节点，只能运行一个计算节点。

  IEF边缘节点上部署的计算节点不支持创建DWS类型的连接器。

  IEF边缘节点服务器上的dokcer版本需要大于或等于20.10.10。

计算节点部署方式

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。

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。

关于CCE集群的更多信息可参考**CCE**。

选择边缘节点部署计算节点：

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“/”。

部署计算节点

步骤1 用户登录TICS控制台。

步骤2 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3 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 4-1 部署计算节点

表 4-1 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）	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。
加密密钥（SK）	
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。
登录密码	登录计算节点控制台的密码。

参数名	参数描述
确认密码	与“登录密码”保持一致即可。
支持国密	若选择是，则登录计算节点必须使用国密浏览器（如奇安信浏览器）。
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4 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）。

步骤5 给CCE类型计算节点的最终租户增加CCE命名空间运维权限。

图 4-2 添加运维权限-入口

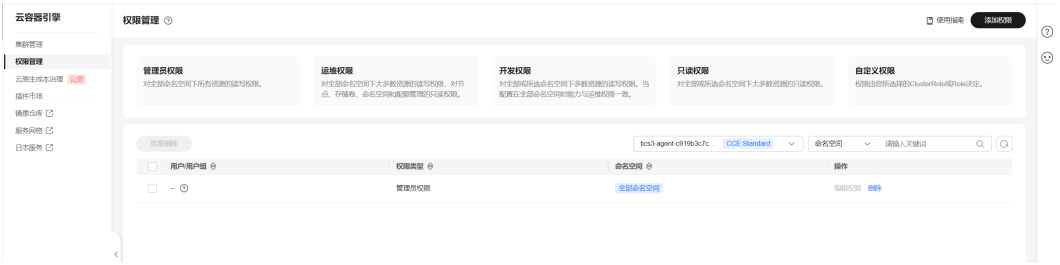


图 4-3 添加运维权限-类型

----结束

4.2 管理计算节点

计算节点升级

用户可在空间特性升级后，对已有的计算节点进行版本升级，体验最新功能特性与安全保障。

步骤1 用户登录TICS控制台。

步骤2 在计算节点管理界面查找需要升级的计算节点，单击“升级”。查看升级版本介绍，并在弹出框勾选“确认已经与空间其他参与方达成共识”，单击“确定”，开始计算节点升级。

说明

- 空间进行特性版本升级后，计算节点才可升级至最新特性版本。
- 更新计算节点期间会导致服务不可用，如果有其他参与方正在使用该计算节点的数据集，请联系达成共识后再操作。
- “计算节点升级”默认升级到空间版本兼容的最新计算节点版本，无中间版本选择。

图 4-4 升级

----结束

计算节点回滚

用户可通过回滚，对升级失败或回滚失败的计算节点进行回滚操作，从而避免进行卸载再重新部署。

步骤1 用户登录TICS控制台。

步骤2 在计算节点管理界面查找需要回滚的计算节点，单击“更多 -> 回滚”，开始计算节点版本回滚。

图 4-5 回滚

----结束

变更计算节点配置

用户可通过配置变更，对已有的计算节点CPU和内存进行修改，而无需卸载计算节点，再重新部署计算节点。

步骤1 用户登录TICS控制台。

步骤2 在计算节点管理界面查找需要变更配置的计算节点，单击“更多 -> 配置变更”。

说明

计算节点有作业在执行时，请不要进行计算节点配置变更，否则会导致作业执行异常。

图 4-6 配置变更

步骤3 在弹出框输入规格参数值，单击“确定”。

- **CPU(Cores)**：用户填写容器使用的CPU配额，范围为2~999的正整数。

- **内存(GIB)**：用户填写容器使用的内存配额，范围为4~999的正整数。为了达到计算资源最佳使用效率，建议内存配额控制在43G以内。
- **计算节点密钥(.p12)**：请从通知管理下载的空间配置的压缩包中，提取计算节点密钥(.p12格式) 并导入上传。
- **CA证书(.jks)**：请从通知管理下载的空间配置的压缩包中，提取CA证书(.jks格式)并导入上传。
- **证书密码**：请从通知管理下载的空间配置的压缩包中，提取空间信息(.json) 并导入上传。

图 4-7 规格参数

----结束

切换计算节点状态

用户需要计算节点短暂脱离空间，一段时间内不想被其他参与方使用自己的数据时，可以手动触发计算节点下线。即“计算节点状态”为“在线”时，触发单击下线，计算节点会切换成离线状态，180秒后空间其他参与方无法使用该计算节点已发布的数据集运行作业。

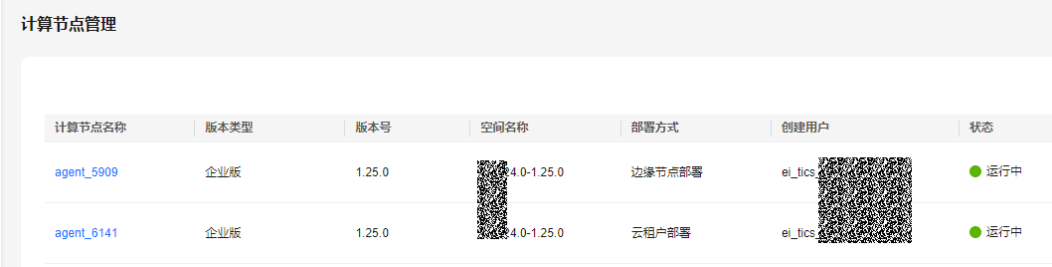
用户想要加入空间，想被其他参与方使用自己的数据时，可以手动触发计算节点上线。即“计算节点状态”为“离线”时，触发单击上线，计算节点会切换成上线状态，90秒后，空间其他参与方可以使用该计算节点已发布的数据集运行作业。

步骤1 用户登录TICS控制台。

步骤2 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3 在“计算节点管理”页面，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 4-8 选择计算节点



步骤4 在“计算节点详情”页，单击“前往计算节点”，在登录页正确输入部署计算节点时设置的“登录用户名”和“密码”。

图 4-9 前往计算节点

步骤5 在左侧导航树上单击“基本信息”，在“基本信息”页面找到“计算节点状态”部分，触发计算节点状态切换操作。

图 4-10 单击切换状态

----结束

重启计算节点

当计算节点存在以下异常状态时，可尝试通过重启计算节点，进行恢复：

- Agent-console显示计算节点未认证。
- 计算节点连接器异常。

说明

IEF边缘部署计算节点不支持重启操作。

操作如下：

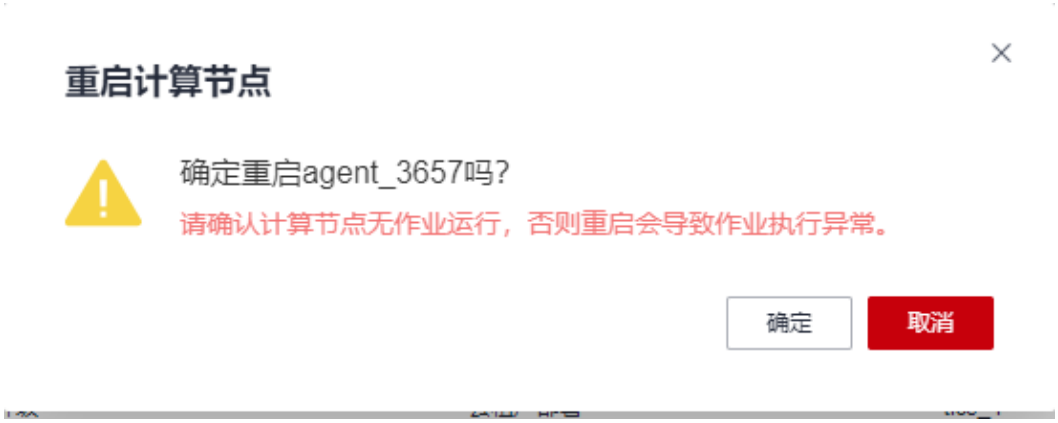
步骤1 用户登录TICS控制台。

步骤2 在计算节点管理界面查找需要重启的计算节点，单击“重启”。计算节点有作业在执行时，请不要进行重启，否则会导致作业执行异常。

图 4-11 重启计算节点

步骤3 单击“确定”。

图 4-12 重启



----结束

删除计算节点

步骤1 用户登录TICS控制台。

步骤2 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3 在计算节点管理界面查找需要删除的计算节点，单击“删除”。

说明

- 删除操作无法撤销，请谨慎操作。
- 计算节点的状态长时间为“启动中”，建议删除计算节点，重新部署。部署时请仔细检查参数配置，包括导入的空间信息、AK、SK、计算节点密钥、CA证书。
- 请避免在CCE侧执行直接删除负载和节点的操作。

图 4-13 删除计算节点

----结束

退购计算节点

步骤1 用户登录TICS控制台。

步骤2 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3 在计算节点管理界面查找需要退购的计算节点，单击“更多”下拉找到“退购”。

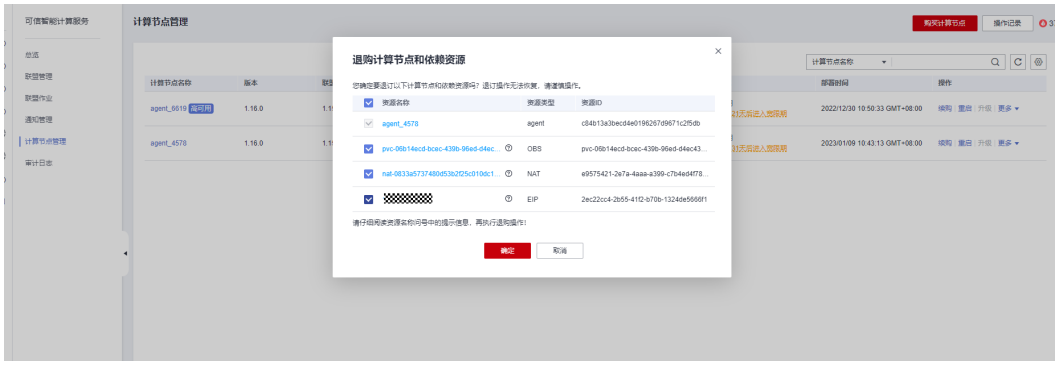
说明

- 退购操作在资源退订确认之前可以撤销，请谨慎操作。
- 单击退购按钮之后，会跳出弹窗，显示计算节点新建的依赖资源，用户可以选择删除，删除前，请查看对应的提示信息，确保删除的成功。
- 在删除依赖资源确认之后，会跳转删除资源确认页面，删除操作无法撤销，请谨慎操作。
- 直接在CCE侧退购负载和节点，会影响系统运行，请避免此类操作。

图 4-14 退购计算节点

图 4-15 退购计算节点资源确认页面

图 4-16 删除依赖资源确认弹窗



----结束

查看计算节点操作记录

用户可在操作记录页面查看计算节点版本创建、升级、删除及回滚操作详情。在详情中，操作进程以可视化的方式展示，清晰展示计算节点的部署、升级、回滚、删除步骤，在出现问题时便于分析排查。

步骤1 用户登录TICS控制台。

步骤2 进入TICS控制台。单击页面左侧“计算节点管理”，进入“计算节点管理”页面。

步骤3 单击页面右上角的“操作记录”按钮，查看操作记录。

图 4-17 入口

步骤4 单击“查看详情”，查看计算节点操作的具体信息。

图 4-18 查看详情

操作详情以可视化的形式展示，使操作进程更直观、更清晰。

图 4-19 操作可视化显示

----结束

4.3 管理实例

实例管理是可信智能计算服务提供的一项查看计算节点作业实例的功能。通过实例管理，用户可以查看到该计算节点所有作业的执行实例，并查看作业的状态、计算过程、执行结果。

步骤1 用户登录TICS控制台。

步骤2 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3 在“计算节点管理”页面，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 4-20 选择计算节点

步骤4 在“计算节点详情”页，单击“前往计算节点”，在登录页正确输入部署计算节点时设置的“登录用户名”和“密码”。

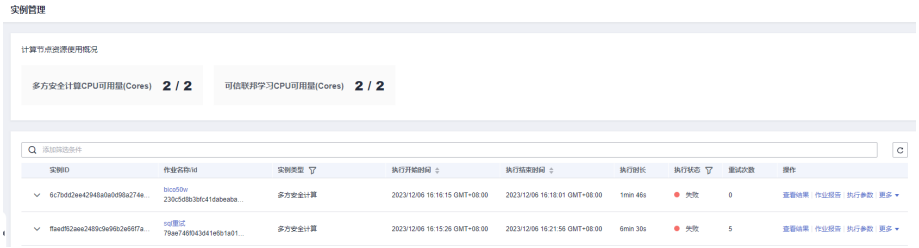
图 4-21 前往计算节点

步骤5 进入计算节点管理界面后，选择左侧“实例管理”。

实例管理页面上方展示了计算节点资源使用概况，分别为当前节点的多方安全计算和可信联邦学习的CPU资源当前使用量，并每分钟刷新一次。下方列表默认优先展示失败状态的实例，可通过列表调整按照执行时间排序，并支持以下筛选条件：

- 实例ID：全匹配或前N位模糊匹配
- 作业ID：全匹配
- 作业名称：模糊匹配
- 实例类型、执行状态：列表筛选

图 4-22 实例管理页面



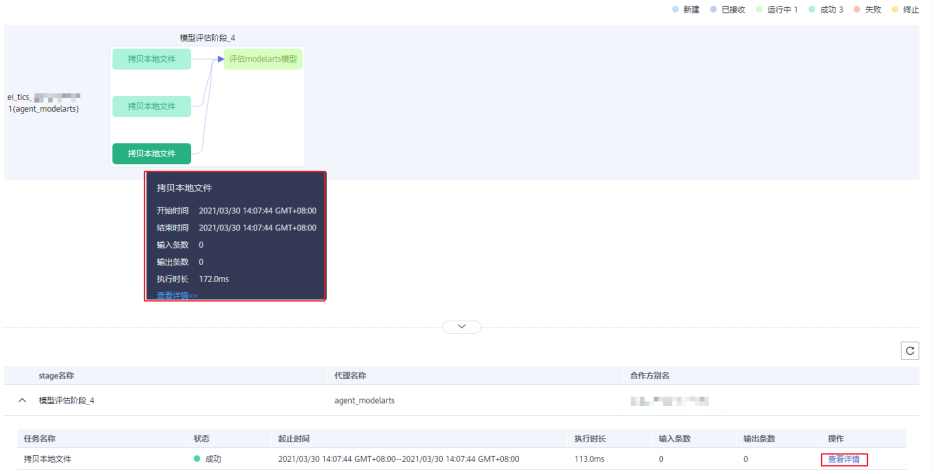
步骤6 在实例列表中，单击操作栏的“编辑”，可在弹出页面修改对应作业；单击操作栏的“查看结果”或者“作业报告”，可在弹出的页面查看执行结果和作业报告；

步骤7 在实例列表中，查找待查看计算过程的作业，单击实例ID展开，在操作栏单击“计算过程”。

图 4-23 在计算节点侧查看作业计算过程

计算过程页面可以单击任务节点，查看开始和结束时间等信息。在计算过程页面下方详情列表打开任务详情，可以查看更详细的计算过程信息。

图 4-24 作业计算过程信息详情（截图为多方安全计算作业示例，请以实际作业为准）



----结束

4.4 管理任务

任务管理是可信智能计算服务提供的一项查看计算节点参与任务的功能。通过任务管理，用户可以查看到曾在该计算节点上执行过的所有作业，并查看自己这个计算节点在作业中的位置以及数据流向。

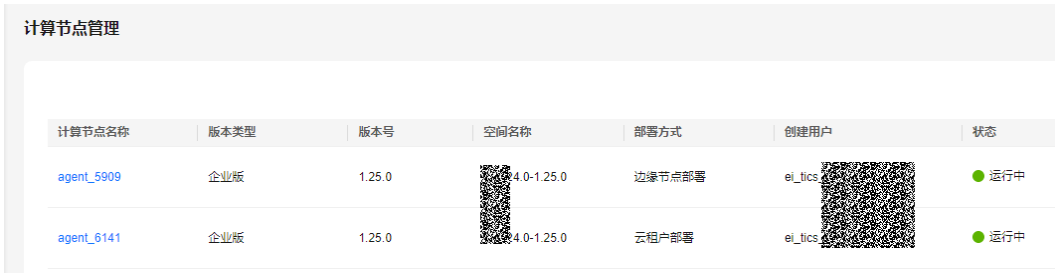
通过任务管理，用户可以查看自己的计算节点在空间中的作业参与度，并通过“计算过程”来确认数据是否合理、安全地被使用。

步骤1 用户登录TICS控制台。

步骤2 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3 在“计算节点管理”页面，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 4-25 选择计算节点

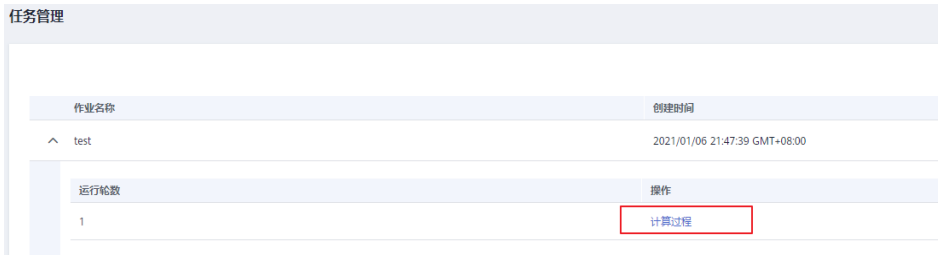


步骤4 在“计算节点详情”页，单击“前往计算节点”，在登录页正确输入部署计算节点时设置的“登录用户名”和“密码”。

图 4-26 前往计算节点

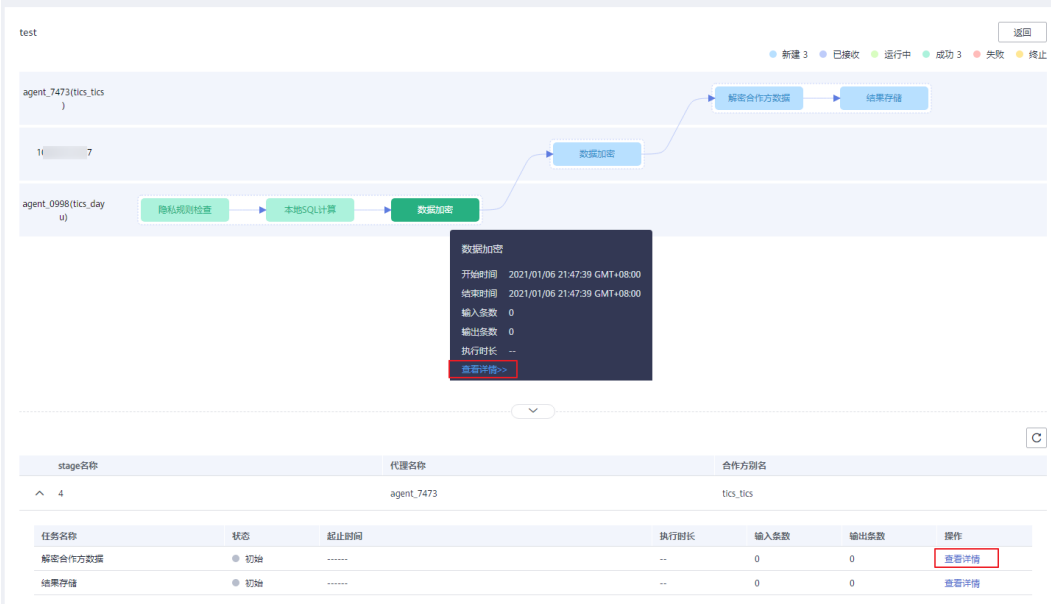
步骤5 进入计算节点管理界面后，选择左侧“任务管理”，单击待查看计算过程的“作业名称”。

图 4-27 计算过程查看入口



步骤6 计算过程页面可以单击任务节点，查看开始和结束时间等信息。可以在下方详情列表打开任务详情，查看更详细的任务信息。

图 4-28 查看任务节点信息



----结束

4.5 管理文件

文件管理是可信智能计算服务提供的一项管理联邦学习模型文件的功能。通过文件管理，参与方无需通过登录后台手动导入模型文件，而是直接将模型文件上传到数据目录进行管理。

使用文件管理功能后，创建联邦学习作业时用户可以便捷地选择自己以前上传的执行脚本、训练模型、数据文件、权重参数文件，极大地提高了系统的易用性及可维护性。

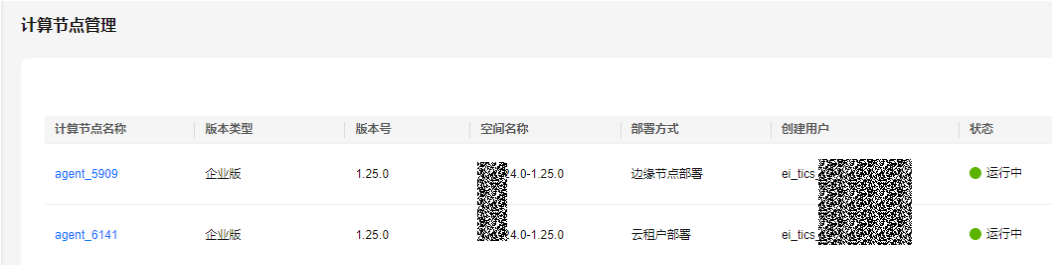
创建文件

步骤1 用户登录TICS控制台。

步骤2 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3 在“计算节点管理”页面，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 4-29 选择计算节点



步骤4 在“计算节点详情”页，单击“前往计算节点”，在登录页正确输入部署计算节点时设置的“登录用户名”和“密码”。

图 4-30 前往计算节点

步骤5 进入计算节点管理界面后，选择左侧“文件管理”，单击“创建”。

图 4-31 创建文件

步骤6 在弹出的页面上，选择要上传的文件类型，填写文件相关信息，添加文件并上传，单击“确定”。

说明

- 部署计算节点时“存储挂载方式”选择“主机挂载”，那么文件将放置在“主机路径/uploadfiles”文件夹下；
- 部署计算节点时“存储挂载方式”选择“OBS挂载”，那么文件将放置在对应OBS桶“/uploadfiles”文件夹下。
- 单次上传文件时默认限制最大50MB，“/uploadfiles”文件夹大小默认限制最大500MB。如需修改请参考**修改上传文件和文件夹大小限制**。

图 4-32 上传文件

----结束

删除文件

步骤1 用户登录TICS控制台。

步骤2 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3 在“计算节点管理”页面，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 4-33 选择计算节点

步骤4 在“计算节点详情”页，单击“前往计算节点”，在登录页正确输入部署计算节点时设置的“登录用户名”和“密码”。

图 4-34 前往计算节点

步骤5 进入计算节点管理界面后，选择左侧“文件管理”，勾选需要删除的文件，单击“批量删除”。

图 4-35 删除文件

说明

删除操作无法撤销，请谨慎操作。

步骤6 单击“确定”。

----结束

修改上传文件和文件夹大小限制

默认上传文件和文件夹大小限制支持修改，根据计算节点的部署方式不同，修改方法分别介绍如下：

- 云租户部署计算节点：
  a. 进入CCE服务控制台，找到对应部署计算节点的CCE集群。

  图 4-36 查找 CCE 集群

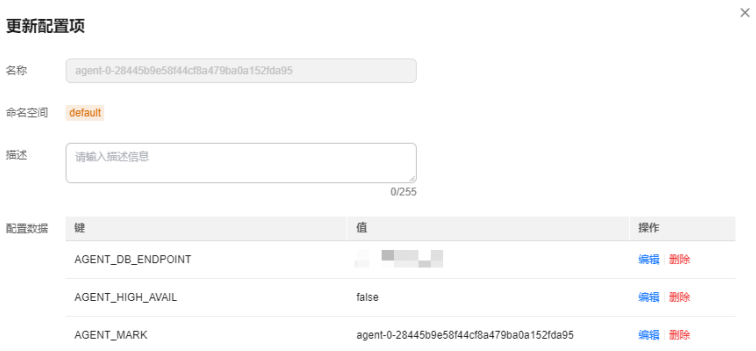
  

  b. 单击集群名，进入集群详情，然后切换到“配置与密钥”选项，进入“配置项”页签。

图 4-37 进入配置项页签

c. 在配置项页签找到命名如“agent-x-xxxxx”的配置项，单击操作栏的“更新”按钮，进入更新配置项窗口。

图 4-38 更新配置项窗口

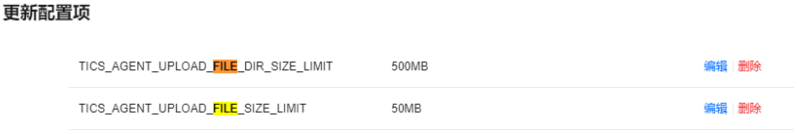


d. 在更新配置项窗口，搜索“FILE”关键字，找到“TICS_AGENT_UPLOAD_FILE_SIZE_LIMIT”和“TICS_AGENT_UPLOAD_FILE_DIR_SIZE_LIMIT”，单击操作栏中的“编辑”修改对应键值，即可修改上传文件和文件夹大小限制。

说明

键值中的数值可自定义，支持MB和GB两种单位。

图 4-39 修改键值

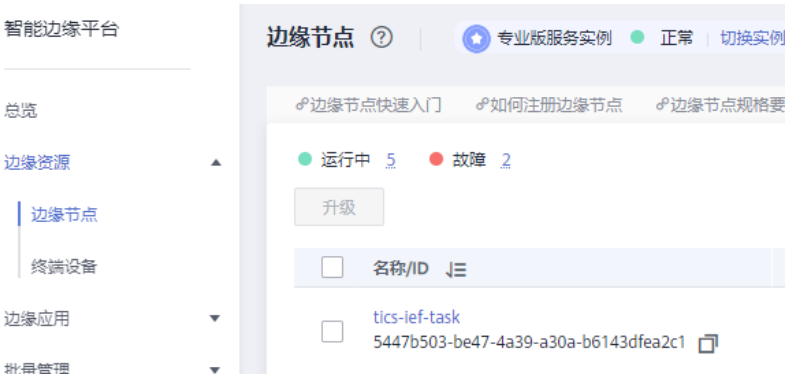


e. 编辑键值后，单击确定保存配置。稍等约10秒钟后，配置即可生效。

- 边缘节点部署计算节点：

a. 进入IEF服务控制台，找到对应部署计算节点的边缘节点。

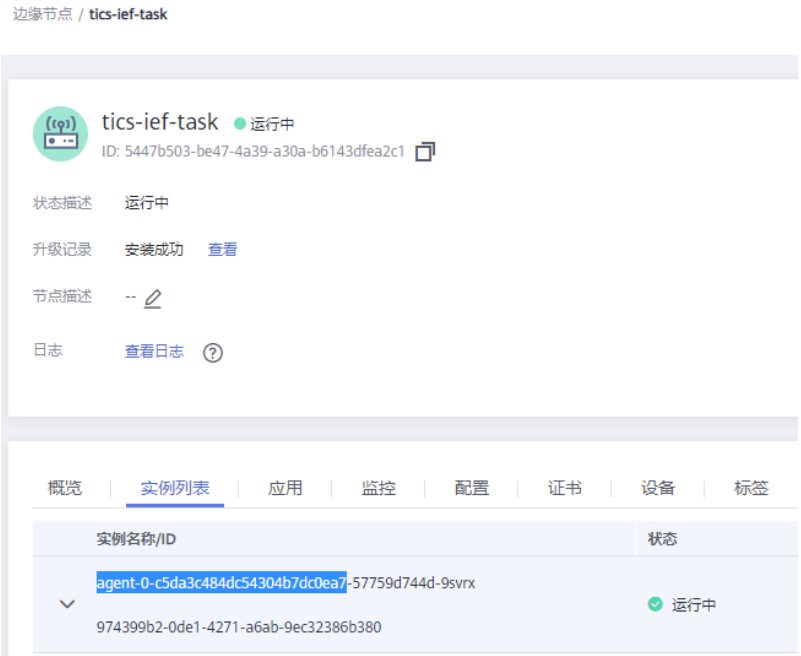
图 4-40 查找边缘节点



b. 单击边缘节点名，进入节点详情，然后切换到实例列表页签。

c. 在实例列表页签找到命名如“agent-x-xxxxx”的实例，记录实例名称前三段，如图所示。

图 4-41 记录实例名称



d. 在IEF服务控制台，单击“边缘应用 > 应用配置”，进入配置项页签。

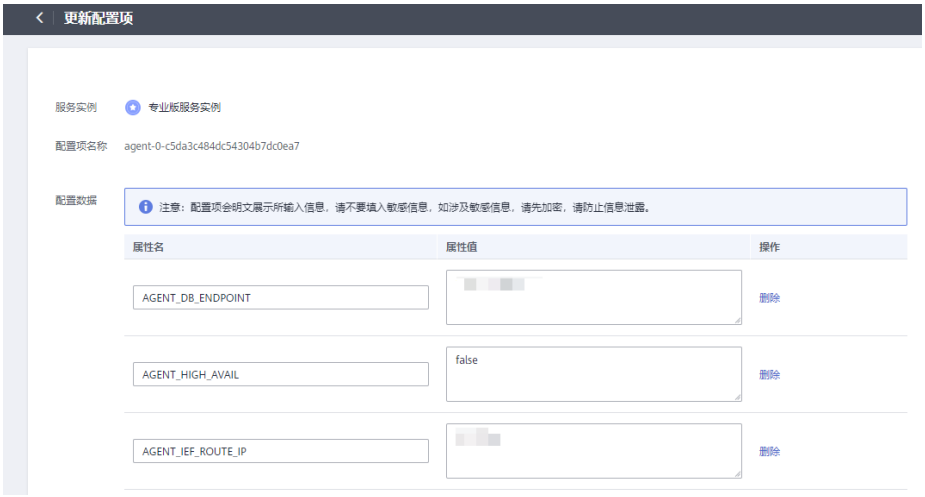
图 4-42 进入配置项页签

e. 在配置项列表上方的搜索栏中输入3中记录的实例名称前三段，搜索配置项。

图 4-43 搜索配置项

f. 单击搜索到的配置项对应操作栏中的“更新”，进入更新配置项页面。

图 4-44 更新配置项

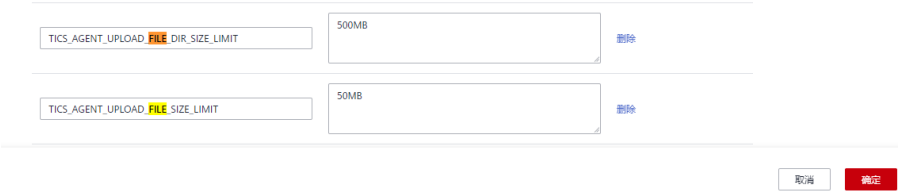


g. 在更新配置项页面，搜索“FILE”关键字，找到“TICS_AGENT_UPLOAD_FILE_SIZE_LIMIT”和“TICS_AGENT_UPLOAD_FILE_DIR_SIZE_LIMIT”属性，修改对应属性值，即可修改上传文件和文件夹大小限制。

说明

属性值中的数值可自定义，支持MB和GB两种单位。

图 4-45 修改属性值



h. 编辑属性值后，单击确定保存配置。稍等约10秒钟后，配置即可生效。

4.6 管理数据

4.6.1 数据管理概述

TICS的数据管理由“连接器管理”和“数据管理”两部分来实现：

- 连接器是可信智能计算服务提供的一项访问参与方数据资源的功能。参与方填写连接信息来创建对应类型的连接器，并通过这些连接器访问到各类型资源的结构化信息。当前支持MRS服务(Hive)、本地数据集、RDS数据集、DWS数据集、Oracle数据集、Mysql数据集，后续会支持更多华为云服务及原生服务的资源访问功能。连接信息中的敏感部分不会离开参与方侧。
- 数据管理包含创建数据和数据预处理，是可信智能计算服务的一项获取、配置及发布数据资源的功能。参与方进入数据管理>数据创建页面，选择对应连接器（连接器管理中已建立完备），将需要共享的数据发布至空间侧，并支持通过转换函数将特征数据转换成更加适合算法模型的特征数据。

使用场景

- 连接器使用场景：参与方的数据信息分布在不同的资源服务上，即可通过连接器管理功能来快速连接到名下的各类资源服务。
- 数据创建使用场景：参与方加入空间后，需要提供自己的数据集信息，用户即可通过数据创建功能，获取到名下详细的资源列表。同时，有敏感信息的数据，还可以单独设置隐私策略，并在发布到空间侧后对其他参与方生效，限制敏感信息的使用。
- 数据预处理使用场景：训练机器学习模型前，可通过转换函数将特征数据转换成更加适合算法模型的特征数据。

4.6.2 创建连接器

连接器用来快速连接到用户名下的各类资源服务。

前提条件

- 计算节点处于运行中，且所在空间信息的“认证状态”为“已认证”。
- 建议使用者提前了解MapReduce服务（MRS Hive）集群。
- “连接器类型”选择MapReduce服务（MRS Hive）时，选择的MRS集群需与当前计算节点部署CCE在同一VPC。填写的用户名，需具有Hive的读写权限。“集群名称”为用户所需要使用的MRS Hive数据源所在的MRS集群。“用户名”为MRS集群中拥有Hive权限的集群用户。

注意事项

- IEF上部署的计算节点不支持创建MRS Hive、ModelArts和DWS类型的连接器。
- MRS Hive、MySQL、DWS、RDS、ORACLE连接器当前只支持在多方安全计算作业中使用。
- API连接器当前只支持在实时预测作业和实时隐匿查询中使用。

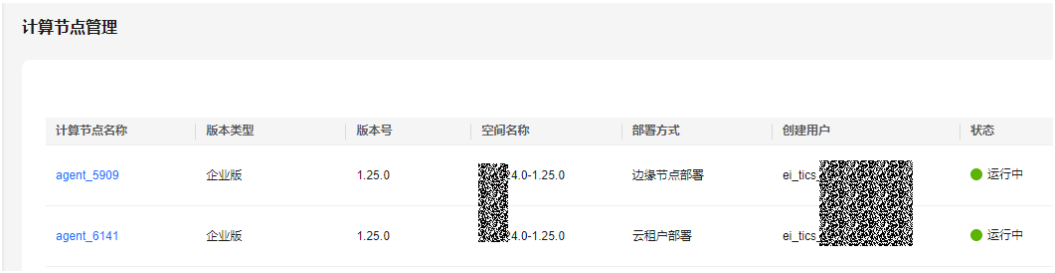
创建连接器

步骤1 用户登录TICS控制台。

步骤2 进入TICS控制台后，单击页面左侧“计算节点管理”。

步骤3 在“计算节点管理”页面，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 4-46 选择计算节点



步骤4 在“计算节点详情”页，单击“前往计算节点”，在登录页正确输入部署计算节点时设置的“登录用户名”和“密码”。

图 4-47 前往计算节点

步骤5 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 4-48 创建连接器（以 RDS 服务为例）

表 4-2 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。

参数名	描述
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。
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。

----结束

管理连接器

步骤1 在“计算节点详情”页，单击“前往计算节点”，在登录页正确输入部署计算节点时设置的“登录用户名”和“密码”。

图 4-49 前往计算节点

步骤2 登录成功后，单击左侧导航栏中“连接器管理”，在操作栏中通过单击编辑、删除，来进行连接器管理操作。

图 4-50 连接器管理

----结束

4.6.3 创建数据集

通过数据集，用户可获取到名下详细的资源列表。同时，对于有敏感信息的数据集，还可以单独设置隐私策略，并在发布到空间侧后对其他参与方生效，限制敏感信息的使用，保障数据安全。

创建结构化数据集

创建数据集前需存在已创建好的连接器，参考**创建连接器**。

步骤1 用户登录TICS控制台。

步骤2 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3 在“计算节点管理”页面，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 4-51 选择计算节点

步骤4 在“计算节点详情”页，单击“前往计算节点”，在登录页正确输入部署计算节点时设置的“登录用户名”和“密码”。

图 4-52 前往计算节点

步骤5 选择界面左侧“数据管理>数据创建”，单击“创建”，可选“本地连接器”或者“关系型数据库连接器”。

- **本地连接器**：在弹出的界面选择本地连接器（localConnector），选择“结构化”数据类型，再配置创建数据的参数，配置完成后单击“确定”。
- **关系型数据库连接器**：在弹出的界面选择关系型数据库连接器，例如RDS、MYSQL、DWS、HIVE等，关系型数据库的数据集默认是“结构化”数据类型。“选择“数据库”以及“数据表”，再配置创建数据的参数，配置完成后单击“确定”。

说明

结构化数据是指具有标准化行、列数据属性的数据，例如sql、csv数据等。

步骤6 配置结构化数据集时，需要注意以下几点：

1. **选择数据文件**：仅本地连接器需要配置。

   数据文件仅支持csv文件和数据目录两种形式。选择数据目录时，必须保证目录下至少包含一个csv文件，且所有csv文件的特征数保持一致。此外，选择数据集的原始文件，需要指定csv文件的“分隔符”、“是否包含表头”。“是否包含表头”是指文件的第一行是否是每一个字段的名称。

2. **数据结构**：配置每个字段的类别标签，包括以下几种：

   a. “字段类型”：支持BOOLEAN、TINYINT、SMALLINT、INTEGER、BIGINT、FLOAT、DOUBLE、DECIMAL、STRING、TIMESTAMP、DATE，必须保证填写正确的字段类型。TIMESTAMP类型仅支持yyyy-MM-dd HH:mm:ss.SSS格式，DATE类型仅支持yyyy-MM-dd格式。

   b. “唯一标识”：用于唯一确定数据集中关键事物的实体身份字段。例如身份证、公司代码等。

   c. 敏感级别：包含敏感、非敏感两个选项。

      敏感：涉及隐私的数据， 例如薪水、 消费金额等。

      非敏感：不涉及隐私的数据， 例如所处城市、公司类型等。

   d. 脱敏：勾选后，该字段内容将在分析结果中加密呈现，否则明文呈现。默认不勾选（作业发起方所属字段不做脱敏）。

   e. 分布类型：包括连续、离散、MULTIHOT三种特征类型，联邦学习时可能会使用到该信息。

      离散：离散变量是在任意两个值之间具有可计数的值的数值变量。离散变量始终为数值变量。例如，客户投诉数量或者瑕疵或缺陷数。

      连续：连续变量是在任意两个值之间具有无限个值的数值变量。连续变量可以是数值变量，也可以是日期/时间变量。例如，零件的长度，或者收到付款的日期和时间。

      MULTIHOT：使用multihot编码的特征，常见于类别特征，例如app列表、性格等。

3. **MULTIHOT分组配置**：

   用户可单击“添加分组”创建MULTIHOT分组，分组包含特征集、字典数两部分。特征集表示分组内所选MULTIHOT特征集合，每个MULTIHOT特征有且只能属于一个分组。字典数表示分组内所有MULTIHOT特征取值总维度，非必填字段，但必须保证全填或全不填该字段。

----结束

创建非结构化数据集

创建数据集前需存在已创建好的连接器，参考**创建连接器**。

步骤1 用户登录TICS控制台。

步骤2 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3 在“计算节点管理”页面，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 4-53 选择计算节点

步骤4 在“计算节点详情”页，单击“前往计算节点”，在登录页正确输入部署计算节点时设置的“登录用户名”和“密码”。

图 4-54 前往计算节点

步骤5 选择界面左侧“数据管理”，单击“创建”，在弹出的界面选择本地连接器（localConnector），选择“非结构化”任务类型，配置创建数据的参数，配置完成后单击“确定”。

配置非结构化数据集需注意：

选择数据文件：数据文件仅支持csv文件和数据目录两种形式。选择数据目录时，必须保证目录下至少包含一个csv文件，且所有csv文件的特征数保持一致。

说明

非结构化数据是指数据结构属性不规则、不完整的数据，例如二进制文件、图片等。

----结束

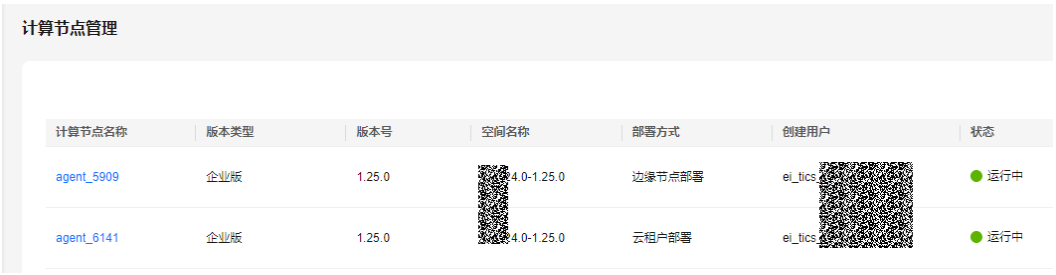
创建 api 数据集

步骤1 用户登录TICS控制台。

步骤2 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3 在“计算节点管理”页面，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 4-55 选择计算节点



步骤4 在“计算节点详情”页，单击“前往计算节点”，在登录页正确输入部署计算节点时设置的“登录用户名”和“密码”。

图 4-56 前往计算节点

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

图 4-57 创建数据

说明

API数据集配置的外部数据源需满足如下要求：

- 请求方式为GET或POST
- 由查询条件可以查出对应一条或多条数据
- 当配置隐匿查询作业的外部数据源时，接口需支持模糊查询id经过sha256转换后的值。 类似MySQL中的如下语句，其中x为查询的具体值。
  ```
  select * from table where SHA2(id,256)  like 'x%' ;
  ```
- 返回json格式数组：
  [{"id":"7748076420210162913","x0":"3232","x1":15,"x2":16},
  {"id":"7748076420210162912","x0":"3232","x1":105,"x2":106},
  {"id":"3","x0":"3232","x1":115,"x2":116}]

----结束

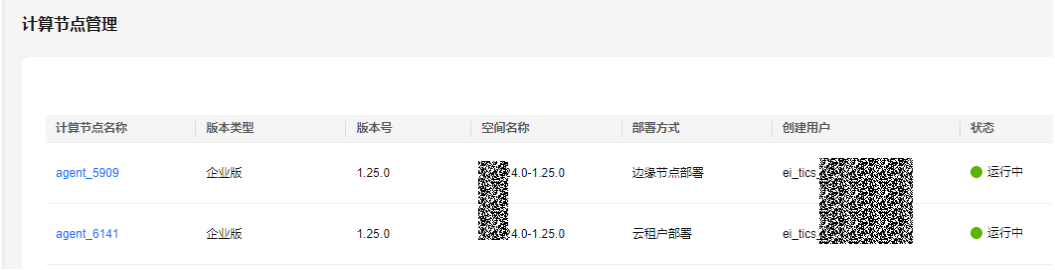
批量删除数据集

步骤1 用户登录TICS控制台。

步骤2 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3 在“计算节点管理”页面，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 4-58 选择计算节点



步骤4 在“计算节点详情”页，单击“前往计算节点”，在登录页正确输入部署计算节点时设置的“登录用户名”和“密码”。

图 4-59 前往计算节点

步骤5 选择界面左侧“数据管理”，勾选需要删除的数据集，单击“批量删除”。

图 4-60 批量删除

----结束

4.6.4 发布数据

前提条件

- 计算节点已创建完成，创建方法请参考**部署计算节点**。

发布数据

发布数据前，若不存在已创建好的连接器和数据，需先执行**创建连接器**和**创建数据集**操作。

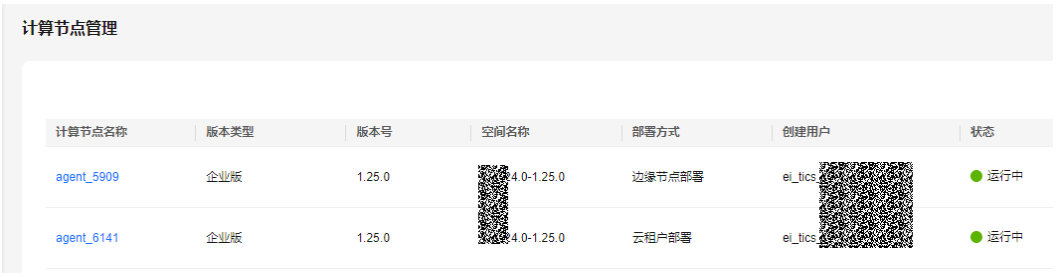
若待发布的数据已经创建完成，参照以下流程进入“数据管理”页，执行以下操作即可。

步骤1 用户登录TICS控制台。

步骤2 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3 在“计算节点管理”页面，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 4-61 选择计算节点

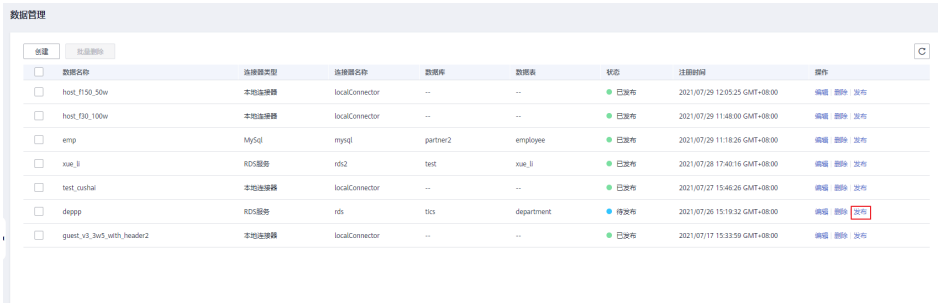


步骤4 在“计算节点详情”页，单击“前往计算节点”，在登录页正确输入部署计算节点时设置的“登录用户名”和“密码”。

图 4-62 前往计算节点

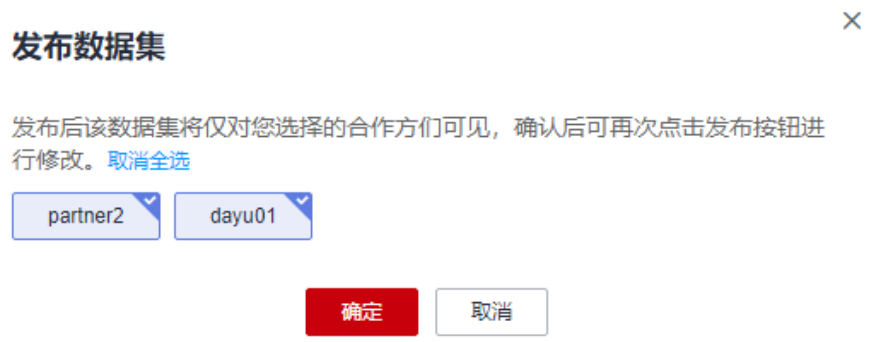
步骤5 在“数据管理”页签找到待发布的数据名称，单击“发布”，弹出发布数据集选择框。

图 4-63 发布数据



步骤6 在发布数据集选择框中选择需要发布的合作方，单击“发布”，数据就会被同步到对应合作方作业管理的数据集中。数据集创建者默认拥有数据集权限。

图 4-64 发布数据集



步骤7 如果需要取消合作方的访问权限，需要重新发布数据集，单击“发布”并去勾选该合作方，单击“确认”。

图 4-65 取消数据集权限

----结束

4.6.5 数据预处理

4.6.5.1 创建数据预处理作业

数据预处理是训练机器学习模型的一个重要前置步骤，其主要是通过转换函数将特征数据转换成更加适合算法模型的特征数据过程。TICS特征预处理功能能够实现对数据的探索、分析、规整以及转换，以达到数据在训练模型中可使用、可实用，在TICS平台内完成数据处理到建模的闭环。

假设您有如下数据集（只展示部分数据），由于数据不够完整，如job、gender等字段均存在一定程度的缺失。为了不让机器理解形成偏差、以达到机器学习的使用标准，需要基于对数据的理解，对数据进行特征预处理。例如：

- job字段是多类别的变量，其值0、1、2实际没有大小之分，一般会将该特征转换成向量，如值为0用向量[1, 0, 0]表示，1用向量[0,1,0]表示，2用向量[0, 0, 1]表示，此即为onehot编码。
- gender字段先填补缺失值，再将其映射成算法可以理解的数值型，比如将woman映射成0，man映射成1，此即为离散特征编码。

图 4-66 数据集样例

id	hour	job	apartment	gender
1	3.5		1	
2			1	woman
3	3.8	2	1	man
4	3.4	1	1	woman
5	3.7	1	1	woman
6	3.6	1	1	man
7	3.3	1	0	woman
8	3.4	1	0	woman
9	3	1	0	woman
10	3.4	2	0	woman
11	3.5	2	0	woman
12	3.4	2	0	woman
13	3.2	0	0	woman
...	...	...	...	...

数据预处理通常被用于评估和预测场景。本文以使用训练数据训练预处理作业，然后再将预处理方法应用于评估/预测数据为例进行说明。

前提条件

- 已提前准备好训练数据，和评估/预测数据。
- 存在未参与其他预处理作业的结构化数据集，且在创建数据集时已定义字段的分布类型。注意预处理作业对数据集的发布状态无要求。

创建数据预处理作业

步骤1 用户登录TICS控制台。

步骤2 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3 在“计算节点管理”页面，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 4-67 选择计算节点

步骤4 在“计算节点详情”页，单击“前往计算节点”，在登录页正确输入部署计算节点时设置的“登录用户名”和“密码”。

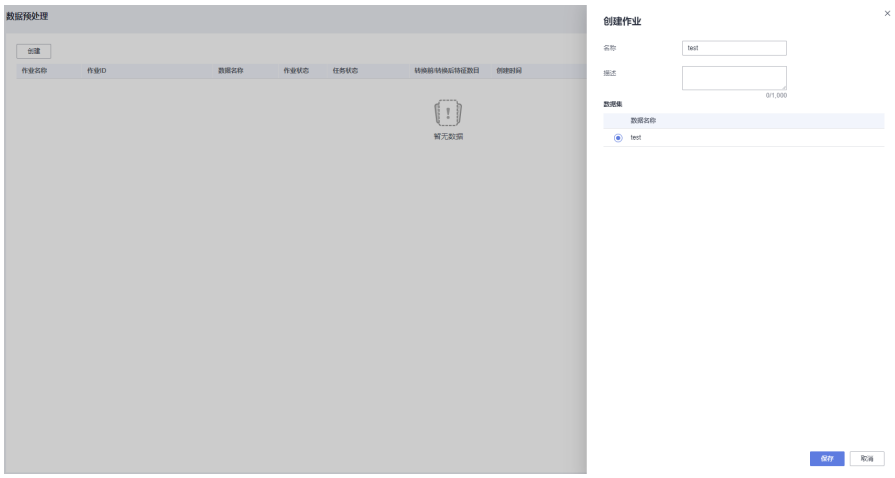
图 4-68 前往计算节点

步骤5 选择界面左侧“数据管理>数据预处理”，单击“创建”，可输入作业名称、描述及数据集，单击保存。若当前选不到目标数据集，可查看该数据集是否已参与其他的预处理作业。

说明

目标数据集需要对所选字段的分布类型进行严格定义。处理评估/预测数据前建议先使用训练数据进行预处理，以确保当数据处理达到目标需求。

图 4-69 创建数据预处理作业



步骤6 单击“保存”后，可查看数据预处理作业。

图 4-70 查看数据预处理作业

----结束

4.6.5.2 开发数据预处理作业

数据预处理通常被用于评估/训练作业场景。本文以使用训练数据训练预处理作业，然后再将预处理方法应用于评估/预测数据为例进行说明。

- **训练数据预处理作业**
- **评估/预测数据预处理**

前提条件

- 已提前准备好训练数据，和评估/预测数据。
- 数据预处理作业选择的结构化数据集（包括CSV文件或目录数据集），需要在创建数据集时定义字段的分布类型。

训练数据预处理作业

步骤1 用户登录TICS控制台。

步骤2 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3 在“计算节点管理”页面，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 4-71 选择计算节点

步骤4 在“计算节点详情”页，单击“前往计算节点”，在登录页正确输入部署计算节点时设置的“登录用户名”和“密码”。

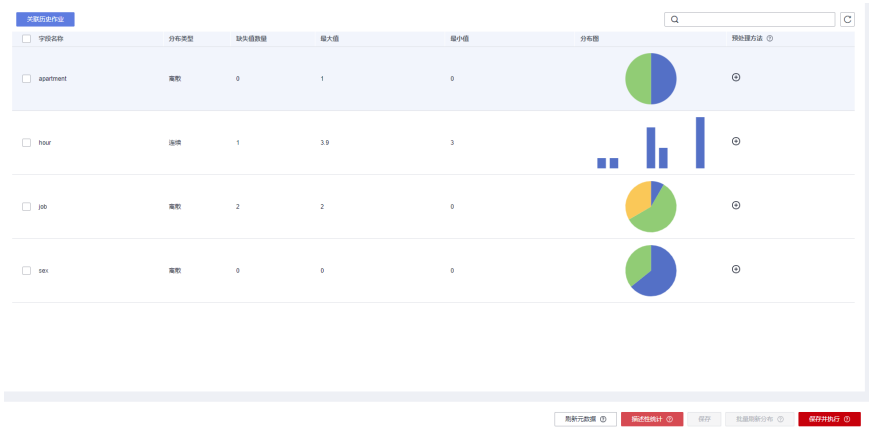
图 4-72 前往计算节点

步骤5 选择界面左侧“数据管理>数据预处理”，单击已创建的数据预处理作业后的开发按钮，进入作业开发页面。该页面描述了字段的属性，如字段名称和分布类型。另外可以通过列表下方的“描述性统计”按键来统计字段的统计量，包括缺失值数量、最大值、最小值及数据分布图。还可以通过⊕为字段添加预处理方法。

图 4-73 作业开发页面

步骤6 进行字段描述性统计。单击列表下方的“描述性统计”按键，会对该数据集的选定字段（即数据创建处筛选的字段）进行原数据的描述性统计，包括缺失值数量、最大值、最小值以及分布图。

图 4-74 描述性统计



步骤7 执行预处理。单击列表字段后的⊕添加预处理方法，系统将利用所选的预处理方法（转换函数）将特征数据转换成更加适合算法模型的特征数据。当前TICS支持的特征预处理方法如表4-3所示。对于一个字段，可以添加多种预处理方法，并且建议按照如下处理顺序进行编排：

- 连续型字段：缺失值处理>特征缩放、缺失值处理>标准化、异常值处理>标准化、缺失值处理>异常值处理>Log变换等
- 离散型字段：缺失值处理>离散特征编码、缺失值处理>OneHot编码等

表 4-3 预处理方法

预处理方法名称	使用范围	功能介绍
缺失值处理	连续型/离散型	针对连续特征有均值、中位数2种填充策略，针对离散特征有众数的填充策略。
离散特征编码	离散型	将字符串形式存储的特征，映射为[0, n_classes-1]范围内的整数

预处理方法名称	使用范围	功能介绍
Onehot编码	离散型	将[0, n_classes-1]范围内整数，映射为大小为n-classes的向量，仅对应索引的元素为1，其余为0
特征放缩	连续型	适合连续特征。将特征的取值范围缩放到[min，max]的范围，推荐min=0,max=1
标准化	连续型	将特征的取值标准化为均值=0，标准差=1的高斯分布
异常值处理	连续型	对特征数据进行异常值定义和处理。对连续特征的数值范围定义合理区间，低于或超过该范围的数值进行修正。支持均值、中位数以及边界值进行修正。
Log变换	连续型	适合连续特征。将特征进行sign(x)log(|x|+1)非线性变换，主要作用是稳定数值方差，使得右偏分布变换后接近正态分布。

添加预处理方法后，勾选添加预处理方法的字段，然后单击列表下方的“批量刷新分布”按键预览预处理结果，查看是否符合预期并进行预处理方法调试。直到预处理结果符合预期结果，则单击列表下方的“保存并执行”按键执行预处理。

图 4-75 添加预处理方法

步骤8 执行预处理结束后，页面跳转到作业列表。单击预处理作业列表中的开发按钮，再次进入作业开发页面，页面展示数据转换后的各项统计结果。例如缺失值数量处理为0，特征放缩的字段最大值与最小值发生变化，离散特征编码的字段字符串已编码为数值，OneHot编码的字段已转为多列特征。

图 4-76 查看预处理执行结果

步骤9 保存预处理作业。经过一系列数据探索和分析，当数据集达到目标需求后，单击页面下方的“保存并执行”按键即可将所选取的预处理方法及其参数进行保存。然后页面跳转到作业列表，此处可以查看预处理作业的任务状态和作业状态。

图 4-77 查看预处理作业

步骤10 发布预处理后的训练数据集。在预处理作业列表，单击“发布”可以将作业生成的训练数据集发布到空间。发布时可查看生成数据集的各项属性，包括数据名称（预处理生成的数据集前缀为preprocessed，后缀为train）、数据文件位置、数据结构等。确认无误后，单击确定即可发布数据集。

发布后可在“数据管理>数据创建”页面查看生成的数据集。

图 4-78 查看生成的数据集

步骤11 （可选）单击作业列表中对应作业的“更多>下载参数配置”，下载本地文件。文件包含字段在作业开发页面使用预处理方法及参数，便于后期线下处理数据。

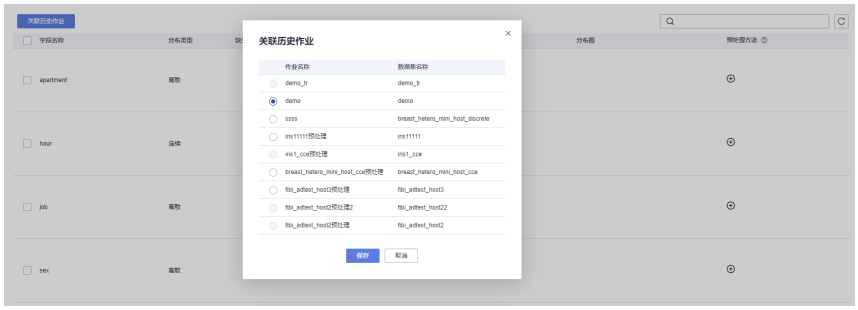
----结束

评估/预测数据预处理

步骤1 参考创建数据预处理作业，在“数据管理>数据预处理”界面创建用于处理评估/预测数据的数据预处理作业。注意，作业中所选的数据集应为评估/预测数据集，且字段定义、尤其是分布类型的定义与之前的训练数据集相同。

步骤2 单击创建的数据预处理作业后的开发按钮，进入作业开发页面。然后单击左上角的“关联历史作业”，在弹窗中选择训练数据的预处理作业后，单击“保存”。

图 4-79 关联历史作业



步骤3 系统提示关联成功，则说明这两个数据集的字段及属性一致、完成校验，并已将训练数据预处理作业的预处理方法成功关联应用。

说明

注意，此时的预处理方法已冻结，与训练数据预处理作业保持一致，不可再修改。

步骤4 依次单击“描述性统计”、“批量刷新分布”，评估预处理方法效果是否符合预期。评估通过后，单击“保存并执行”，完成对评估/预测数据的处理和生成。

图 4-80 生成处理后的评估/预测数据

步骤5 发布预处理后的评估/预测数据集。在预处理作业列表，单击“发布”可以将作业生成的评估/预测数据集发布到空间。生成后的评估/预测数据集即可用于纵向联邦作业及其他作业（不建议用于横向联邦作业，因为单方的横向数据分布并不保证其具备总体样本的分布特点）。

----结束

4.7 审计日志

审计日志页面是可信智能计算服务提供的一项审计数据流动的功能。通过计算节点侧审计页面信息，用户可以清晰地获知空间中的参与方通过该计算节点运行的任务详情。同时，部署计算节点时若开启BCS功能，审计数据会同步至区块链上。

计算节点侧查看审计日志

步骤1 用户登录TICS控制台。

步骤2 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3 在“计算节点管理”页面，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 4-81 选择计算节点

步骤4 在“计算节点详情”页，单击“前往计算节点”，在登录页正确输入部署计算节点时设置的“登录用户名”和“密码”。

图 4-82 前往计算节点

步骤5 在界面左侧选择“审计日志”，在弹出的界面查看详细信息。

图 4-83 审计日志

说明

- 事件信息内容主要有：参与方[参与方别名]创建[作业类型]作业[作业名称:作业实例id]，使用数据集[数据集名称]，耗费[时间]，输出[条数]。
- 多方安全计算作业中的作业详情信息，即SQL语句也会参与审计，但该信息属于敏感信息不会上链。

----结束

4.8 对接 AOM 日志服务

对接AOM日志服务后，AOM服务将支持收集可信计算节点日志，推荐开启。

- 计算节点为云租户部署时，在购买时打开“开启AOM日志监控”功能，即可对接AOM。
- 计算节点为边缘节点部署时，需要手动在IEF平台对接AOM。

约束限制

- 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**。
- 计算节点为边缘节点部署时，仅支持1.20.0及以上版本对接AOM，低版本可参考**空间升级**将空间升级至最新版本。

云租户部署对接 AOM

若购买可信计算节点时，打开“开启AOM日志监控”功能，则已完成对接AOM。

对接完成后，可参考**AOM服务查看可信节点日志**，前往AOM服务管理查看可信计算节点日志。

边缘节点部署对接 AOM

计算节点为边缘节点部署时，仅支持1.20.0及以上版本对接AOM，对接步骤如下。

步骤1 进入IEF服务控制台，找到对应部署计算节点的边缘节点。

图 4-84 找到边缘节点

步骤2 单击边缘节点名，进入节点详情，然后切换到配置页签。

步骤3 在配置页签找到日志配置，在系统日志下单击”编辑”按钮，参考图4-85进行配置。

图 4-85 系统日志配置样例

步骤4 系统日志配置完成并保存后，切换到应用日志，参考图4-86进行配置。

图 4-86 应用日志配置样例

步骤5 应用日志配置完成并保存后，此节点配置完成，成功对接AOM。

----结束

AOM 服务查看可信节点日志

步骤1 用户登录华为云。

步骤2 搜索AOM服务，进入AOM服务控制台。

步骤3 在AOM左侧功能列表选择日志文件，右侧集群下拉列表选择可信计算节点，即可查看对应日志文件。

图 4-87 AOM 日志文件

----结束

4.9 管理密钥

密钥用于对加密的数据文件进行AES加解密。在多方安全计算作业场景，当SQL语句使用系统函数进行AES加解密时需要使用密钥。

约束限制

- 上传密钥文件需要以.key为后缀结尾。
- 上传密钥文件大小不超过256B。
- 上传密钥文本为base64编码之后的密钥，长度小于1000。

上传密钥

步骤1 用户登录进入计算节点页面。

步骤2 在左侧导航树上单击“基本信息”，打开“基本信息”页面，找到“密钥管理”部分。

图 4-88 密钥管理

步骤3 单击“上传”，打开“创建密钥”页面，选择文本或文件模式上传密钥。

图 4-89 创建密钥

步骤4 如果已经上传过密钥，再次上传密钥会更新当前已有密钥。

----结束

删除密钥

单击“删除”按钮，会删除当前已上传密钥。

5 多方安全计算作业

5.1 创建作业

多方安全计算是可信智能计算提供的关系型数据安全共享和分析功能。您可以创建多方安全计算作业，根据合作方已提供的数据，编写相关SQL作业并获取您所需要的分析结果，同时能够在作业运行保护数据使用方的数据查询和搜索条件，避免因查询和搜索请求造成的数据泄露。

前提条件

- 空间组建完成，参考**组建空间**。
- 空间成员完成计算节点部署，参考**部署计算节点**。
- 空间成员完成数据发布，参考**发布数据**。

约束限制

1. SQL语法支持
   - **关键词**：select 、from 、where 、inner join/join/left outer join/right outer join、group by 、order by、limit、on 、as、union all；
   - **逻辑表达式**： <、 >、 = 、<= 、>=、 <>、 between and、 in、 like、 exists；
   - **运算符**：+、-、*、/ 和 case when；
   - **数据类型**：字符串、 整型、 浮点型、 decimal、日期(date)、 时间(timestamp)；
   - **聚合函数**：max、min、sum、avg、count、median、variance；
   - **系统函数：**包含时间日期函数、字符串函数、数学函数。使用介绍如**表5-1**所示。
   - **通配符**：%；--与like配合使用；
2. 注意事项：
   - 不识别的数据类型被认为是字符串类型。
   - “隐私保护等级”设置为高级别后，参与多方计算的字段会进行秘密分享加密。

- “隐私保护等级”设置为高级别后，参与2方计算的join字段会使用psi算法输出碰撞的密文数据。
- 由于本地数据集不支持统计信息上报，因此本地数据集不支持差分隐私功能。

创建多方安全计算作业

步骤1 用户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”，打开多方安全计算页面。

步骤3 在“多方安全计算”页面，在页面上方选择作业创建的空间后，单击“创建”。

图 5-1 创建作业

步骤4 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 5-2 新建作业

步骤5 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。

- 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集。数据集第一级是合作方名称，第二级是数据集名称。SQL语句中用“合作方名.数据集名”表示一张表。
- SQL语法支持

  - **关键词**：select 、from 、where 、inner join/join/left outer join/right outer join、group by 、order by、limit、on 、as、union all；
  - **逻辑表达式**： <、 >、 = 、<= 、>=、 <>、 between and、 in、 like、 exists；
  - **运算符**：+、-、*、/ 和 case when；
  - **数据类型**：字符串、 整型、 浮点型、 decimal、日期(date)、 时间(timestamp)；
  - **聚合函数**：max、min、sum、avg、count、median、variance；
  - **系统函数**：包含时间日期函数、字符串函数、数学函数。使用介绍如**表5-1**所示。
  - **通配符**：%；--与like配合使用；
- 编写SQL语句时，您可以使用作业变量定义需要在执行中替换的过滤条件值
  - 作业变量名仅可使用字母、数字、下划线，否则不会被识别，格式为${变量名}，如：${USER_NAME}
  - 作业变量值为字符串类型时，需要在定义时左右加单引号，如：'${USER_NAME}'
  - 作业变量命名长度限制0-20个字符，可支持40个变量
- 编写SQL语句时，您可以参考编辑器右侧的“系统函数”，在SQL语句中输入并使用系统函数。

表 5-1 系统函数介绍

系统函数类型	函数	命令格式	命令说明	参数说明	返回值说明
数学函数	ABS	abs(number)	计算number的绝对值。	number：必填。参数类型支持INT、BIGINT、FLOAT、DOUBLE、DECIMAL、STRING。 如果输入为STRING类型，则隐式转换为DECIMAL类型后参与运算。	- 输入为INT、BIGINT、FLOAT、DOUBLE、DECIMAL、STRING，则返回对应输入参数的数据类型。 - 当输入非INT、BIGINT、FLOAT、DOUBLE、DECIMAL、STRING六种类型，返回报错。

系统函数类型	函数	命令格式	命令说明	参数说明	返回值说明
	LN	ln(number)	计算number的自然对数。	number：必填。参数类型支持INT、BIGINT、FLOAT、DOUBLE、DECIMAL、STRING。 如果输入为STRING类型，则隐式转换为DECIMAL类型后参与运算。	– 当number为INT、BIGINT、FLOAT、DOUBLE、DECIMAL、STRING类型时返回DOUBLE类型。 – 当number为负数或0时，返回报错。
	RAND	rand(seed)	返回随机数，返回值区间是0~1。	seed：选填。参数类型支持INT、BIGINT、FLOAT、DOUBLE、DECIMAL、STRING。 如果输入为STRING类型，则隐式转换为DECIMAL类型后参与运算。	返回DOUBLE类型。
	ROW_NUMBER	row_number()	返回记录行数	long：必填。参数类型为LONG类型。	返回LONG类型。
	MEDIAN	median(number)	聚合运算，返回一列数的中位数	number：必填。参数类型支持INT、BIGINT、FLOAT、DOUBLE、DECIMAL。	– 当number为INT、BIGINT类型时返回DOUBLE类型。 – 当number类型为FLOAT、DOUBLE、DECIMAL时返回DECIMAL类型。

系统函数类型	函数	命令格式	命令说明	参数说明	返回值说明
	VARIANCE	variance(number)	聚合运算，返回一列数的方差	number：必填。参数类型支持INT、BIGINT、FLOAT、DOUBLE、DECIMAL。	– 当number为INT、BIGINT类型时返回DOUBLE类型。 – 当number类型为FLOAT、DOUBLE、DECIMAL时返回DECIMAL类型。
字符串操作函数	CHAR_LENGTH	char_length(string)	计算字符串string的长度。	string：必填。参数类型为STRING类型。 如果输入为非STRING类型，则隐式转换为STRING类型后参与运算。	返回INT类型。
	CHARACTER_LENGTH	character_length(string)	计算字符串string的长度。同CHAR_LENGTH。	string：必填。参数类型为STRING类型。 如果输入为非STRING类型，则隐式转换为STRING类型后参与运算。	返回INT类型。
	LOWER	lower(string)	将字符串string中的大写字符转换为对应的小写字符。	string：必填。参数类型为STRING类型。 如果输入为非STRING类型，则隐式转换为STRING类型后参与运算。	返回STRING类型。
	UPPER	upper(string)	将字符串string中的小写字符转换为对应的大写字符。	string：必填。参数类型为STRING类型。 如果输入为非STRING类型，则隐式转换为STRING类型后参与运算。	返回STRING类型。

系统函数类型	函数	命令格式	命令说明	参数说明	返回值说明
	SUBSTRING	substring(string from start[for length])	返回字符串string从start开始，长度为length的子串。	– string：必填。参数类型为STRING类型。 如果输入为非STRING类型，则隐式转换为STRING类型后参与运算。 – start: 必填。参数类型为INT类型。起始位置为1（起始位置0作1处理）。当start为负数时，表示开始位置是从字符串的尾部向前倒数。推荐start从1开始，负数及0在不同数据库中表现不同。 – length：选填。参数类型为INT类型。表示子串的长度。值必须大于0。	返回STRING类型。
	BASE64_ENCODE	BASE64_ENCODE(binary)	将二进制的字节内容用base64编码并输出成utf8编码的字符串。	binary：必填。参数类型为字节数组byte[]类型。	返回utf8格式的STRING字符串。
	BASE64_ENCODE	BASE64_ENCODE(string)	将字符串用base64编码并输出成utf8编码的字符串。	string：必填。参数类型为utf8格式的STRING类型。	返回utf8格式的STRING字符串。

系统函数类型	函数	命令格式	命令说明	参数说明	返回值说明
	BASE64_DECODE	BASE64_DECODE(string)	将base64编码后的字符串解码为明文的字符串。	string：必填。参数类型为base64编码后的STRING类型。	返回utf8格式的STRING字符串。
	HEX_ENCODE	HEX_ENCODE(binary)	将二进制的字节内容用hex编码并输出成utf8编码的字符串	binary：必填。参数类型为字节数组byte[]类型。	返回utf8格式的STRING字符串。
	HEX_ENCODE	HEX_ENCODE(string)	将字符串用hex编码并输出成utf8编码的字符串。	string：必填。参数类型为utf8格式的STRING类型。	返回utf8格式的STRING字符串。
	HEX_DECODE	HEX_DECODE(string)	将hex编码后的字符串解码为明文的字符串。	string：必填。参数类型为hex编码后的STRING类型。	返回解码所得到的STRING字符串的ASCII码值。
	STR_UTF8	STR_UTF8(binary)	将二进制的字节内容直接转换为utf8格式的字符串。	binary：必填。参数类型为字节数组byte[]类型。	返回utf8格式的STRING字符串。

系统函数类型	函数	命令格式	命令说明	参数说明	返回值说明
	AES_DECRYPT	AES_DECRYPT(binary, binary)	将加密的二进制字节内容使用用户上传的密钥和数据的iv字节解密。	用户上传的密钥是指在**上传密钥**上传的AES密钥。 binary：必填。加密的数据，参数类型为字节数组byte[]类型。 binary：必填。加密时使用的iv信息，参数类型为字节数组byte[]类型。	返回解密后的字节数组。 可以再使用STR_UTF8和BASE64_ENCODE函数将其转为字符串STRING格式。
	AES_ENCRYPT	AES_ENCRYPT(binary, binary)	将二进制字节内容使用用户上传的密钥和数据的iv字节加密。	用户上传的密钥是指在**上传密钥**上传的AES密钥。 binary：必填。需要加密的明文数据，参数类型为字节数组byte[]类型。 binary：必填。加密时使用的iv信息，参数类型为字节数组byte[]类型。	返回加密后的字节数组。 可以再使用STR_UTF8和BASE64_ENCODE函数将其转为字符串STRING格式。
时间日期函数	YEAR	year(date)	返回日期date的年。	date：必填。DATE或TIMESTAMP类型，格式为yyyy-mm-dd或yyyy-MM-dd HH:mm:ss。	返回INT类型。 date为非DATE或TIMESTAMP类型，返回报错。
	QUARTER	quarter(date)	返回日期date的季度	date：必填。DATE或TIMESTAMP类型，格式为yyyy-mm-dd或yyyy-MM-dd HH:mm:ss。	返回INT类型。 date为非DATE或TIMESTAMP类型，返回报错。
	MONTH	month(date)	返回日期date的月。	date：必填。DATE或TIMESTAMP类型，格式为yyyy-mm-dd或yyyy-MM-dd HH:mm:ss。	返回INT类型。 date为非DATE或TIMESTAMP类型，返回报错。
	WEEK	week(date)	返回日期date位于当年的第几周。	date：必填。DATE或TIMESTAMP类型，格式为yyyy-mm-dd或yyyy-MM-dd HH:mm:ss。	返回INT类型。 date为非DATE或TIMESTAMP类型，返回报错。

系统函数类型	函数	命令格式	命令说明	参数说明	返回值说明
	DAYOFYEAR	dayofyear(date)	返回日期date位于当年的第几天。	date：必填。DATE或TIMESTAMP类型，格式为yyyy-mm-dd或yyyy-MM-dd HH:mm:ss。	返回INT类型。 date为非DATE或TIMESTAMP类型，返回报错。
	DAYOFMONTH	dayofweek(date)	返回日期date位于当月的第几天。	date：必填。DATE或TIMESTAMP类型，格式为yyyy-mm-dd或yyyy-MM-dd HH:mm:ss。	返回INT类型。 date为非DATE或TIMESTAMP类型，返回报错。
	DAYOFWEEK	dayofmonth(date)	返回日期date位于当周的第几天。	date：必填。DATE或TIMESTAMP类型，格式为yyyy-mm-dd或yyyy-MM-dd HH:mm:ss。	返回INT类型。 date为非DATE或TIMESTAMP类型，返回报错。
	HOUR	hour(date)	返回日期date的小时部分的值。	date：必填。DATE或TIMESTAMP类型，格式为yyyy-mm-dd或yyyy-MM-dd HH:mm:ss。	返回INT类型。 date为非DATE或TIMESTAMP类型，返回报错。
	MINUTE	minute(date)	返回日期date的分钟部分的值。	date：必填。DATE或TIMESTAMP类型，格式为yyyy-mm-dd或yyyy-MM-dd HH:mm:ss。	返回INT类型。 date为非DATE或TIMESTAMP类型，返回报错。
	SECOND	second(date)	返回日期date的秒数部分的值。	date：必填。DATE或TIMESTAMP类型，格式为yyyy-mm-dd或yyyy-MM-dd HH:mm:ss。	返回INT类型。 date为非DATE或TIMESTAMP类型，返回报错。
	EXTRACT	extract(unit FROM date)	返回日期date的时间或日期部分。	date：必填。DATE或TIMESTAMP类型，格式为yyyy-mm-dd或yyyy-MM-dd HH:mm:ss。 unit支持参数：YEAR、QUARTER、 MONTH、WEEK、DOY、DAY、DOW、HOUR、MINUTE、SECOND。	返回INT类型。 date为非DATE或TIMESTAMP类型，返回报错。

系统函数类型	函数	命令格式	命令说明	参数说明	返回值说明
	UNIX_TIMESTAMP	unix_timestamp(timestamp)	将日期转换为时间戳。	long：必填。参数类型为LONG类型。 支持日期格式：yyyy-MM-dd HH:mm:ss。	返回LONG类型。

- SQL语句示例：

  SELECT

  column_A--字段名是租户别名.数据集名.字段名

  column_B as alias--支持别名

  SUM(column_C) AS alias--支持针对列名的聚合函数

  column_A + column_B*2 as alias--支持select中加计算式

  FROM

  partner1.dataset1 table_A---表名是租户别名.数据集名, 后面可以加一个表别名tableA

  JOIN--支持的JOIN类型，详见**语法支持**。

  partner2.dataset2 table_B

  ON

  table_A.ID = table_B.ID

  WHERE

  table_A.uid = ${uid}

  and table_A.name = '${name}'

  and table_A.age = 16

  GROUP BY

  table_A.ID

  ORDER BY

  table_A.ID

  LIMIT

  10

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，完成后单击“保存”。

图 5-3 编写 SQL 语句

步骤6 单击编辑器右侧的“作业配置项”，进行作业配置。

重试：开关开启后，执行失败的作业会根据配置定时进行重试，仅对开启后的执行作业生效。开关关闭后，关闭前已触发重试的作业不受影响，仅对关闭后的执行作业生效。

执行参数：用于作业调优。当前可用执行参数介绍如下：

- job.ins.memory.size：本次作业在各执行节点分配的内存大小，默认200MB。如果作业中间结果过大，需要调高该参数。
- max.result.file.size：最大存储文件大小，默认10GB。如果最终结果存储超过这个大小，则会执行失败，需要调大该值。
- tics.task.concurrency：在TICS所属计算节点执行计算时的并行度，默认值为1。当需要提升作业性能时，可以修改该参数，参考配置为CCE集群中规格时建议配置范围为4~8，大规格部署时建议配置范围为8~16，具体根据实际需求和情况调整。
- user.task.concurrency：在用户所属计算节点计算时的并行度，默认值为1。当需要提升作业性能时，可以修改该参数，参考配置为CCE集群中规格时建议配置范围为4~8，大规格部署时建议配置范围为8~16，具体根据实际需求和情况调整。
- complex.sql.push.connector：ORACLE作业在开启差分隐私开关时，为避免rand语法在ORACLE执行报错，可配置该作业参数为“false”。其他场景下无需配置。
- join.runtime.filter：是否启用两表id初筛机制。配置为“true”后，在执行SQL join前会默认通过ID字段前8位明文来初筛过滤数据，提高join效率。对数据安全要求较高的场景下，建议配置为“false”。
- secret.share.decimal.precision.len：开启“隐私保护等级”高级别开关后，敏感数值比大小会采用秘密分享协议，此参数表示比较数值精确到小数点后位数，取值范围为0~10，最高可支持10位小数之间的比较。
- secret.share.bit.precision.len：开启“隐私保护等级”高级别开关后，敏感数值比大小会采用秘密分享协议，此参数表示秘密分享支持的比大小数值范围，取值范围为8~64之间整数，例如取值为60时，表示可以比较-2^59至2^59-1之间的整数；小数比大小场景下，会乘上10^secret.share.decimal.precision.len放大小数，转化为整数进行比较，如果数值超过比较范围会出现异常提示，并且给出推荐参数。

图 5-4 作业配置

步骤7 单击“保存”后，单击“提交审批”按钮，等完成审批再单击“执行”按钮，等待执行完成后在下方“执行结果”页签查看结果。

----结束

5.2 执行作业

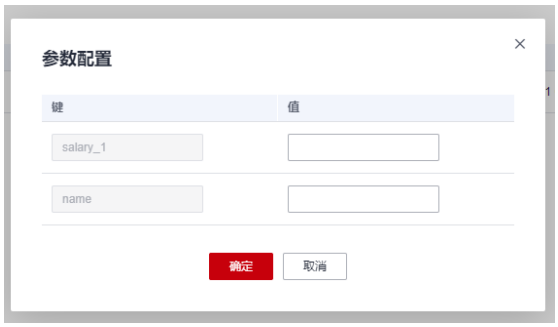
执行多方安全计算作业

步骤1 用户登录计算节点页面。

步骤2 在左侧导航树上依次选择“作业管理 > 多方安全计算”，打开多方安全计算页面。

步骤3 在多方安全计算页面查找待执行的作业，单击“执行”。如果SQL中存在作业变量，需要在执行时填入实际值。

图 5-5 执行作业



----结束

5.3 查看作业计算过程和作业报告

在空间侧查看作业计算过程和作业报告

步骤1 用户登录TICS控制台。

步骤2 在左侧导航树上单击“空间作业”，打开“空间作业”页面。

步骤3 在作业列表上，单击对应作业操作栏的“作业报告”。可在弹出的页面查看作业报告。

图 5-6 空间侧查看作业报告

说明

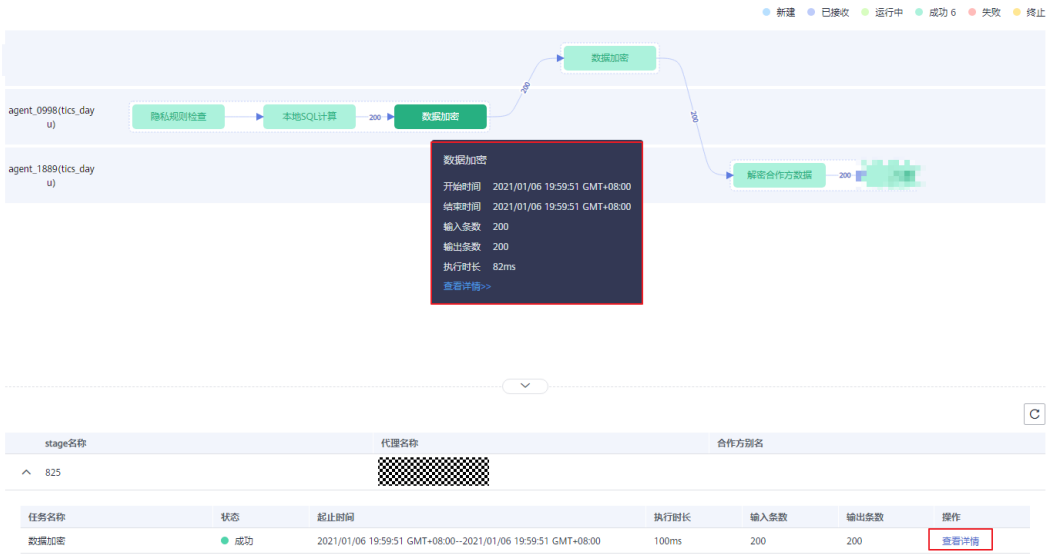
空间侧不支持查看作业执行结果，查看作业执行结果需要去对应的计算节点存储路径查看作业执行的实际结果。

步骤4 查找待查看计算过程的作业，单击作业名称展开，在操作栏单击“计算过程”。

图 5-7 空间侧查看作业计算过程

步骤5 计算过程页面可以单击任务节点，查看开始和结束时间等信息。在计算过程页面下方详情列表打开任务详情，可以查看更详细的计算过程信息。

图 5-8 作业计算过程信息详情（截图为多方安全计算作业示例，请以实际作业为准）



----结束

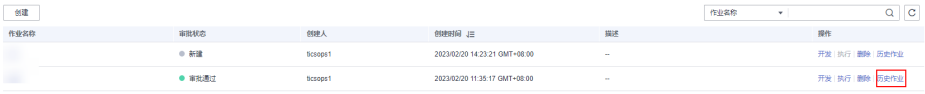
在计算节点侧查看作业计算过程和作业报告

步骤1 用户登录进入计算节点页面。

步骤2 在左侧导航树上单击“作业管理”，选择作业类型，打开作业列表页面。

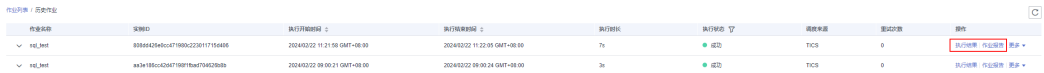
步骤3 查找待获取执行结果和作业报告的作业，单击操作栏的“历史作业”。

图 5-9 历史作业



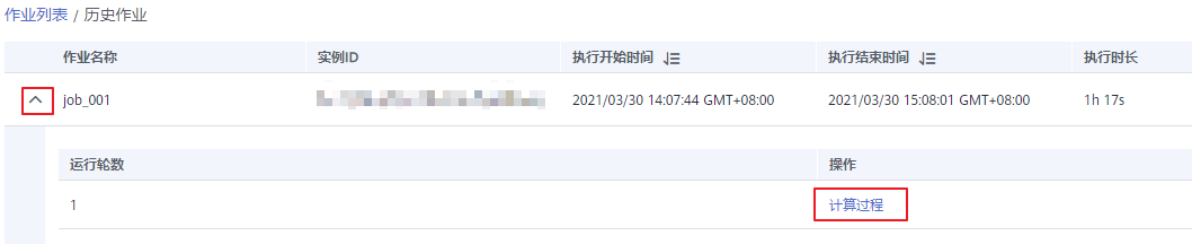
步骤4 在历史作业列表中，单击操作栏的“执行结果”或者“作业报告”。在弹出的页面查看执行结果和作业报告。

图 5-10 查看执行结果、作业报告



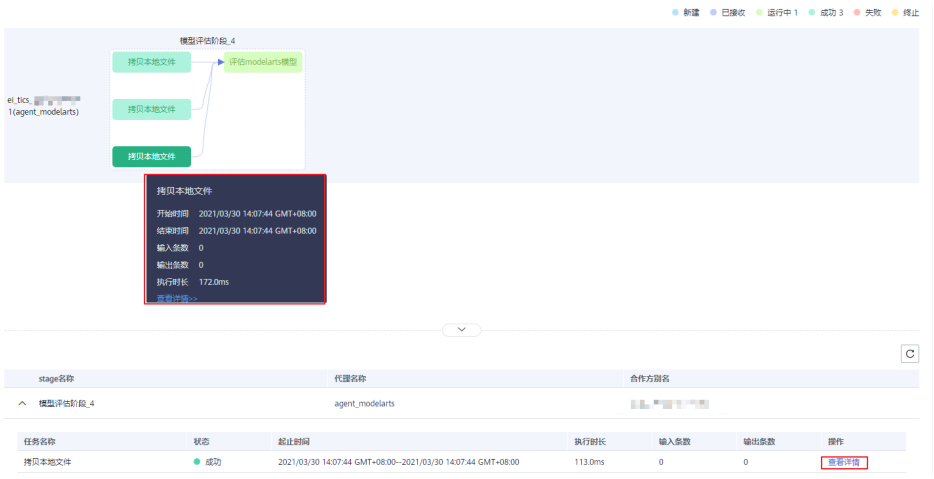
步骤5 在历史作业列表中，查找待查看计算过程的作业，单击作业名称展开，在操作栏单击“计算过程”。

图 5-11 在计算节点侧查看作业计算过程



步骤6 计算过程页面可以单击任务节点，查看开始和结束时间等信息。在计算过程页面下方详情列表打开任务详情，可以查看更详细的计算过程信息。

图 5-12 作业计算过程信息详情（截图为多方安全计算作业示例，请以实际作业为准）



----结束

5.4 删除作业

删除多方安全计算作业

步骤1 用户登录计算节点页面。

步骤2 在左侧导航树上依次选择“作业管理 > 多方安全计算”，打开多方安全计算页面。

步骤3 在多方安全计算页面查找待删除的作业，单击“删除”。

说明

删除操作无法撤销，请谨慎操作。

图 5-13 删除作业

----结束

5.5 审批模式作业

TICS基于安全隐私策略的数据安全防护会自动拒绝不合法的SQL语句执行，但当安全规则限制过强的时候，可能会影响正常业务的执行。

对此TICS 提供作业审批功能。配置生效后，所有的计算任务执行时，均会生成审批报告，提交到数据提供方侧，由提供方确认关联数据集的用途和风险。关联参与方都同意后，才能执行SQL作业。

具体操作步骤如下：

步骤1 作业发起方进入自己所属的计算节点，编写完作业之后，单击“提交审批”。在页面下方可查看审批方和审批进度。

图 5-14 提交审批

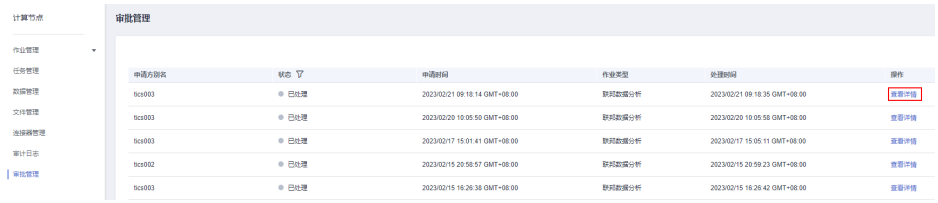
审批中或者审批通过后， 如果进行了修改SQL和保存操作，那么就需要重新提交审批。

提交完成后，在页面下方可查看审批方和审批进度。

图 5-15 审批进度

步骤2 数据提供方进入数据集所在计算节点，单击页面左侧的“审批管理”，查找待处理的审批项。单击“查看详情”。

图 5-16 审批管理



详情页可以看到审批报告，报告内容包括作业发起方、会在该计算节点连接器上执行的SQL语句、各字段作用描述、各字段加密类型、是否在结果中可见（即明文显示）等。

图 5-17 详情

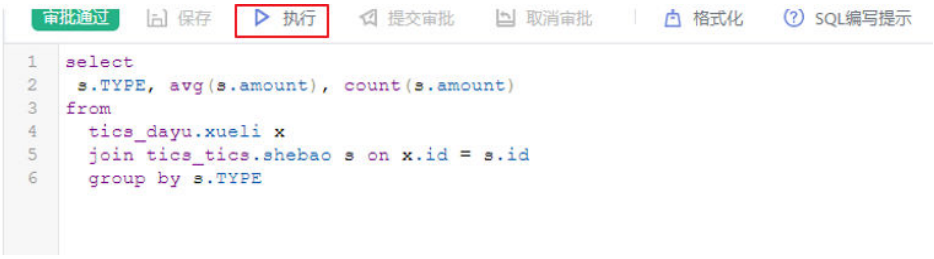
说明

- 处于保护作业发起方的业务机密性， 这里会屏蔽所有和该审批者无关的字段信息，例如ID字段的描述中，会屏蔽该字段具体和哪个字段做Join。
- 审批报告中的“是否在结果中可见”直接决定了该字段数值是否会明文显示，请根据字段业务类型慎重判断是否可见。

步骤3 数据提供方确认风险后，在详情页填写审批意见，单击“同意”。

步骤4 作业发起者执行作业，执行完成后，可在页面下方查看执行结果。

图 5-18 执行作业



----结束

6 可信联邦学习作业

6.1 概述

可信联邦学习作业是可信智能计算服务提供的在保障用户数据安全的前提下，利用多方数据实现的联合建模。

- 安全可信。
- 多种训练场景。
- 方便与已有服务对接。

使用场景

1. 横向联邦机器学习

   横向联邦机器学习，适用于参与者的数据特征重叠较多，而样本ID重叠较少的情况，联合多个参与者的具有相同特征的多行样本进行可信联邦学习，联合建模。

2. 模型评估

   评估训练得出的模型权重在某一数据集上的预测输出效果。

3. 纵向联邦机器学习

   纵向联邦机器学习，适用于参与者训练样本ID重叠较多，而数据特征重叠较少的情况，联合多个参与者的共同样本的不同数据特征进行可信联邦学习，联合建模。

概念术语

- 存储方式：是指计算节点部署时选择的存储方式，目前仅支持“主机存储”和“OBS存储”两种存储方式。前一种是指计算节点交互的数据存储在计算节点所在机器上，后一种是计算节点交互的数据存储在部署时选择的OBS桶中。
- 数据目录：计算节点部署时选择的存储路径，用于TICS服务的数据和外部交互。用户只有在目录中放置数据集等文件，服务才能读取到；服务运行作业生成的结果、日志文件也会输出到数据目录，供用户查看、获取。

文件管理

文件管理是可信智能计算服务提供的一项管理联邦学习模型文件的功能。参与方无需登录后台手动导入模型文件，通过该功能即可将模型文件上传到数据目录，并支持批

量删除。在创建联邦学习作业时可以选到上传的脚本模型等文件，提高了易用性及可维护性。

使用场景：管理联邦学习作业所需的脚本、模型、权重文件。

6.2 创建横向训练型作业

前提条件

- 空间组建完成，参考**组建空间**。
- 空间成员完成计算节点部署，配置参数时选择存储方式和数据目录，参考**部署计算节点**。
- 空间成员完成数据集准备工作，参考**准备本地横向联邦数据资源**。
- 空间成员在数据目录中完成数据发布，参考**发布数据**。
- 参与方的计算节点如果是采用云租户部署，并且使用子账号进行创建的，需要参考**配置CCE集群子账号权限**。

约束限制

参与方数据要求特征相同（字段格式相同）、样本不同。

创建可信联邦学习训练型作业

步骤1 用户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 > 可信联邦学习”，打开可信联邦学习作业页面。

步骤3 在“可信联邦学习”页面，单击“创建”。

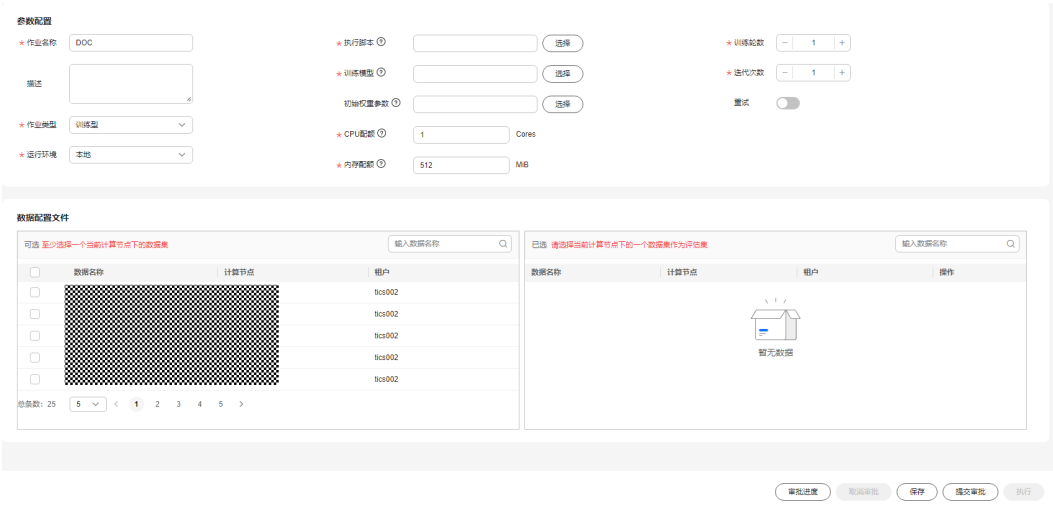
图 6-1 创建作业

步骤4 在弹出的对话框中配置作业名称相关参数，完成后单击“确定”。

图 6-2 新建作业

步骤5 在弹出的界面，继续配置联邦训练作业的参数，参数配置参考表6-1。

图 6-3 配置参数



“数据配置文件”的“可选数据列表”：

- LOCAL运行环境，展示的是通过本地连接器发布的本地数据。
- “训练型作业”同一个计算节点只能选一个数据集，但是一个作业必须要选两个及两个以上的数据集才能做训练。

表 6-1 作业参数说明

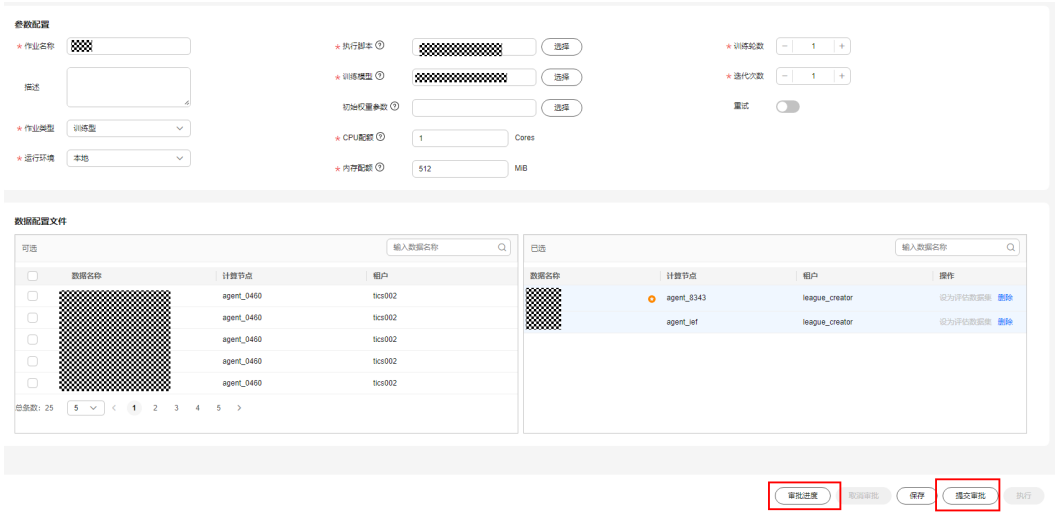
参数名	参数描述
作业名称	用户自定义作业的名称，只能包含英文字母、数字、中文、“-”、“_”、“.”，且长度为1～128个字符
描述	作业的详细描述信息。

参数名	参数描述
作业类型	用户下拉选择所需作业类型即可。
运行环境	用户下拉选择作业的运行位置： • LOCAL表示的是可信联邦学习作业在本地运行。 • ModelArts表示的是可信联邦学习作业在ModelArts Lite资源池内运行。 • PriorityModelArts表示的是可信联邦学习作业优先使用ModelArts Lite资源池运行，没有则在本地运行。 **说明** ModelArts和PriorityModelArts只有在CCE计算节点才能选择，IEF计算节点只能选择LOCAL。
执行脚本	用户本地的自定义执行脚本，样例请参考**准备本地横向联邦数据资源**中步骤4。
训练模型	用户自定义模型，样例请参考**准备本地横向联邦数据资源**中步骤3。
初始权重参数	评估时必填，训练时可选，样例请参考**准备本地横向联邦数据资源**中步骤3。
迭代次数	即epoch，数据迭代计算的次数。
训练轮数	训练的轮数，每一轮训练结束都会对各方训练出的权重进行一次安全聚合。
重试	开关开启后，执行失败的作业会根据配置定时进行重试，仅对开启后的执行作业生效。 开关关闭后，关闭前已触发重试的作业不受影响，仅对关闭后的执行作业生效。
CPU配额	执行作业使用容器的CPU核数。
内存配额	执行作业使用容器的内存大小。

步骤6 参数配置完成后，单击保存，完成可信联邦学习任务的创建。

步骤7 完成创建后，单击页面右下角的提交审批，待完成审批后，才可执行作业。审批进度可单击页面右上角的审批进度进行查询。

图 6-4 提交审批



----结束

6.3 横向联邦训练作业对接 MA

前提条件

- MA Lite资源池已创建完毕。
- 空间组建完成，参考**组建空间**。
- 空间成员完成计算节点部署，配置参数时选择存储方式和数据目录，参考**4.1 部署计算节点**。
- 空间成员完成数据集准备工作，参考**准备本地横向联邦数据资源**。
- 空间成员在数据目录中完成数据发布，参考**4.6.4 发布数据**。
- 对接MA的计算节点如果是使用子账号进行创建的，需要参考**配置CCE集群子账号权限**给子账号增加“管理员权限”配置。

约束限制

- 仅CCE计算节点支持横向训练作业对接MA。
- MA纳管的CCE集群要和TICS的CCE计算节点在同一个VPC下。

注册 MA 资源池

步骤1 用户登录进入计算节点页面。

步骤2 在左侧导航树上选择“基本信息”，打开基本信息页面。

步骤3 在“基本信息”页面，输入创建MA Lite资源池纳管的CCE集群ID，单击“注册”。

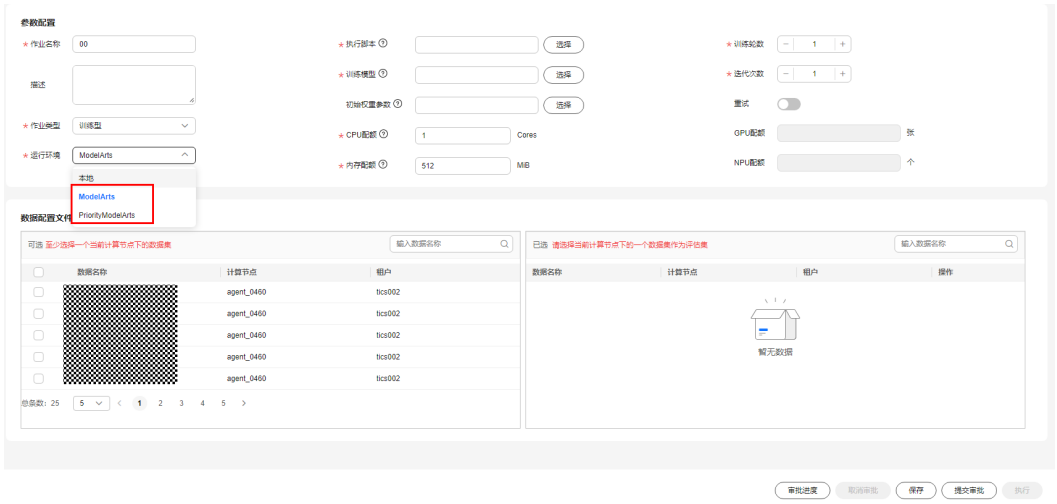
图 6-5 注册 ma 资源池

----结束

创建可信联邦学习训练型作业

参考步骤**创建横向训练型作业**创建可信联邦学习训练型作业，运行环境选择ModelArts和PriorityModelArts时，新增的资源配额是使用MA Lite资源池进行训练时，工作负载需要配置的资源参数。

图 6-6 配置参数



6.4 创建横向评估型作业

前提条件

- 空间组建完成，参考**组建空间**。
- 空间成员完成计算节点部署，配置参数时选择挂载方式和计算节点，参考**部署计算节点**。

- 空间成员完成数据集准备工作，参考**准备本地横向联邦数据资源**。
- 空间成员在计算节点中完成数据发布，参考**发布数据**。

约束限制

仅IEF计算节点支持创建横向评估型作业。

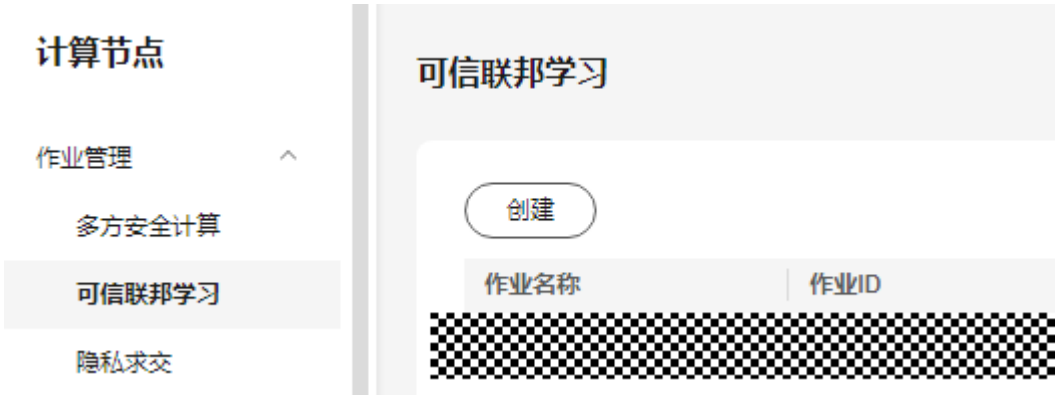
创建可信联邦学习评估型作业

步骤1 用户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 > 可信联邦学习”，打开可信联邦学习作业页面。

步骤3 在“可信联邦学习”页面，单击“创建”。

图 6-7 创建作业

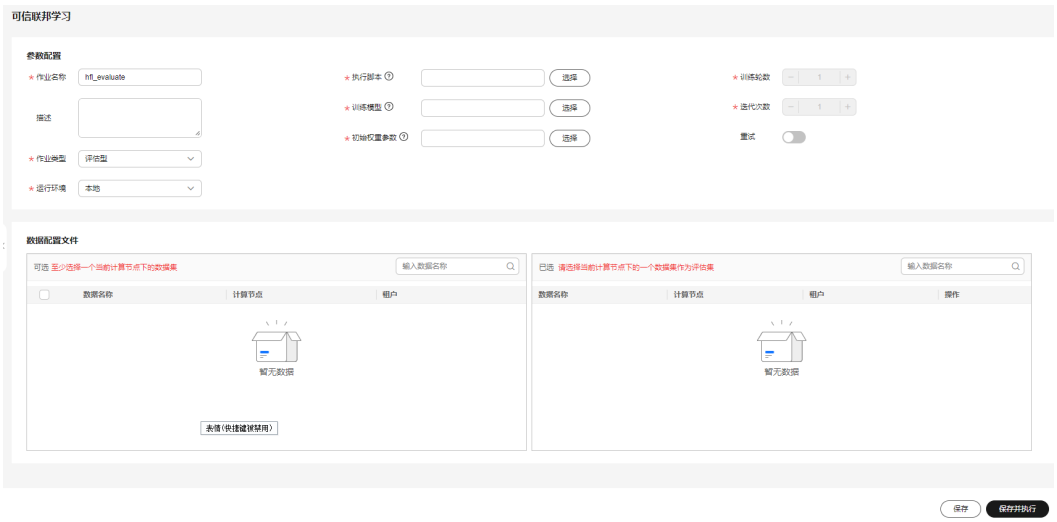


步骤4 在弹出的对话框中配置作业名称相关参数，完成后单击“确定”。

图 6-8 新建作业

步骤5 在弹出的界面，继续配置可信联邦学习作业的参数，参数配置参考**表6-2**。

图 6-9 配置参数



“数据集配置”的“可选数据列表”：

- 本地运行环境时，展示的是通过本地连接器发布的本地数据。
- “评估型作业”只能选择当前计算节点的一个数据集。

表 6-2 作业参数说明

参数名	参数描述
作业名称	用户自定义作业的名称，只能包含英文字母、数字、中文、“-”、“_”、“.”，且长度为1～128个字符
描述	作业的详细描述信息。
作业类型	用户下拉选择所需作业类型即可。
运行环境	表示可信联邦学习作业在本地运行。
执行脚本	用户本地的自定义执行脚本，样例请参考**准备本地横向联邦数据资源**中步骤4。
训练模型	用户自定义模型，样例请参考**准备本地横向联邦数据资源**中步骤3。
初始权重参数	模型的初始权重，样例请参考**准备本地横向联邦数据资源**中步骤3。
迭代次数	即epoch，数据将会被执行的次数。评估型作业的迭代次数固定为1。
训练轮数	训练的轮数，每一轮训练结束都会对各方训练出的权重进行一次安全聚合，评估型作业的轮数固定为1。

参数名	参数描述
重试	开关开启后，执行失败的作业会根据配置定时进行重试，仅对开启后的执行作业生效。 开关关闭后，关闭前已触发重试的作业不受影响，仅对关闭后的执行作业生效。
CPU配额	执行作业使用容器的CPU核数。
内存配额	执行作业使用容器的内存大小。

步骤6 参数配置完成后，单击保存，完成可信联邦学习任务的创建。

----结束

6.5 创建纵向联邦学习作业

前提条件

- 空间组建完成，参考**组建空间**。
- 空间成员完成计算节点部署，配置参数时选择挂载方式和数据目录，参考**部署计算节点**。
- 空间成员在计算节点中完成数据发布，参考**发布数据**。
- 参与方的计算节点如果是采用云租户部署，并且使用子账号进行创建的，需要参考**配置CCE集群子账号权限**给子账号增加权限配置。

约束限制

- 纵向联邦作业XGBoost算法只支持两方参与训练。
- 训练作业必须选择一个当前计算节点发布的数据集。
- 参与方数据要求样本相同、特征不同。
- 数据集在发布时可以指定一个字段为“唯一标识”，样本对齐时会使用唯一标识字段进行比对。
- 作业创建者的数据集必须含有特征。

  其中有一方需要提供标签和特征，另一方仅提供特征。

创建纵向联邦学习作业

纵向联邦学习作业在本地运行，目前支持XGBoost算法、逻辑回归LR算法和FiBiNET算法。

纵向联邦学习分为**五个步骤**：数据选择、样本对齐（可选）、特征选择（可选）、模型训练、模型评估。

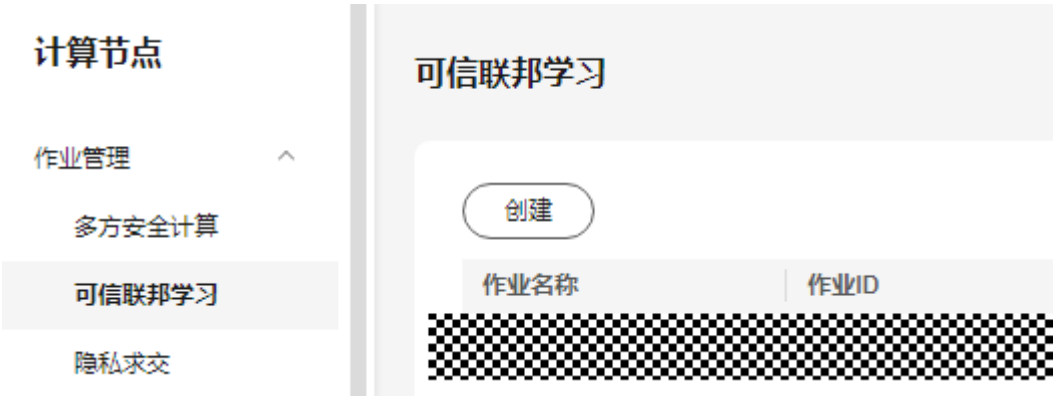
创建过程如下：

步骤1 用户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 > 可信联邦学习”，打开可信联邦学习作业页面。

步骤3 在“可信联邦学习”页面，单击“创建”。

图 6-10 创建作业



步骤4 在弹出的对话框中单击“纵向联邦”按钮，编辑“作业名称”等相关参数，完成后单击“确定”。

目前，纵向联邦学习支持“XGBoost”、“逻辑回归”、“FiBiNET”三种算法类型，XGBoost支持“分类”和“回归”两种任务类型。

图 6-11 新建作业

步骤5 在弹出的界面进行**数据选择**，选择两方数据集作为整个作业的数据集，必须选择一个当前代理的数据集，另一个数据集可以来自空间中的任意一方。两方的数据集中一方数据集只含有特征，另一方的数据集必须含有标签。

重试：开关开启后，执行失败的作业会根据配置定时进行重试，仅对开启后的执行作业生效。开关关闭后，关闭前已触发重试的作业不受影响，仅对关闭后的执行作业生效。

CPU配额：执行特征选择作业和训练作业时，会创建新容器来执行，该参数的值为创建新容器的CPU核数。

内存配额：执行特征选择作业和训练作业时，会创建新容器来执行，该参数的值为创建新容器的内存。

样本粗筛：当己方数据过大无法导出成文本文件时，可以使用样本粗筛获取合作方的明文id前缀，使用大数据组件筛选出id前缀相符的数据，达到减少数据量的目的。样本粗筛时还可以选择多个标记为“非敏感”的字段进行过滤，结果会按照“id前缀,过滤字段1,过滤字段2……”的格式保存成csv文本文件。

选择完成后单击“下一步”。

图 6-12 数据选择

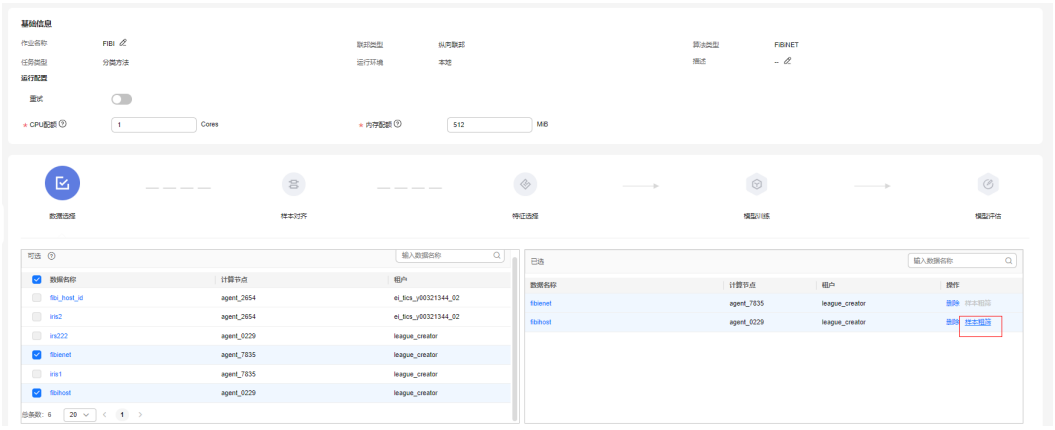


图 6-13 样本粗筛

步骤6 (可选步骤) 样本对齐，支持使用新对齐的结果，如图6-14所示；也支持复用隐私求交作业中通过这两个数据集计算得到的结果，如图6-15所示。

图 6-14 使用新对齐结果

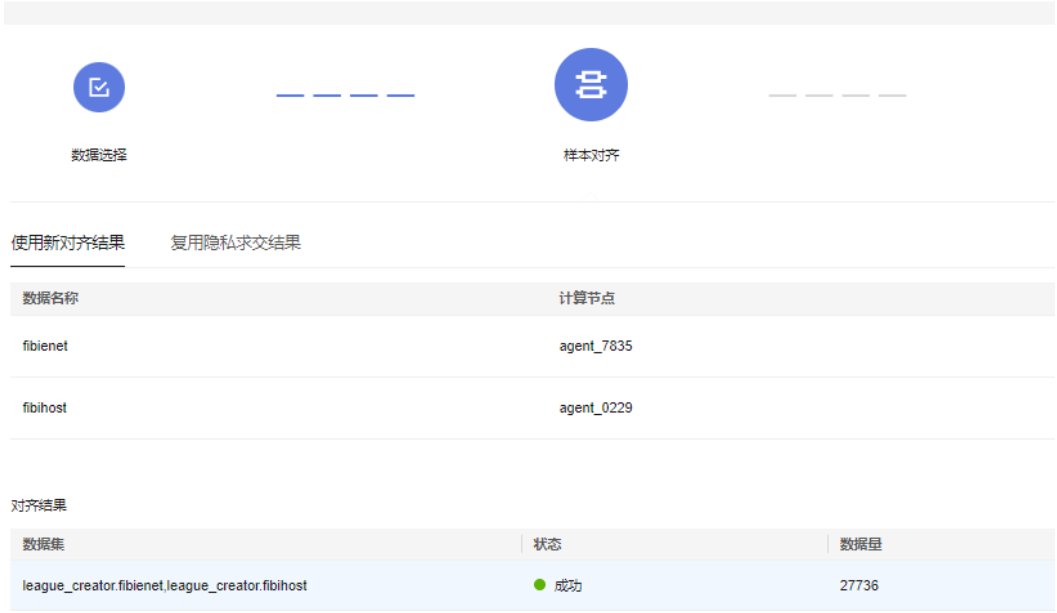


图 6-15 复用隐私求交作业中的结果

步骤7 （可选步骤）进行特征选择，此步骤要求数据已经对齐，即两方数据集每一行的数据都是一一对应的。

单击数据集按钮切换数据集，勾选特征作为模型训练的指定特征，选择分箱方式后单击“启动分箱和IV计算”，计算得到所选特征对标签的影响程度。计算完成后，单击特征行的 可以展开图表形式的分箱woe值。

“FiBiNET”算法新增限制：

1. 特征方必须要有两个及以上离散特征，连续特征可有可无。
2. 标签方可以不提供任何特征，如果标签方提供特征也要遵循1规则。

其他算法无限制

选择完成后单击“下一步”。

说明

- 在所选数据集中只能有一个字段是标签。
- 训练时需勾选使用的特征选项，勾选后可以跳过特征分箱，直接进行训练。
- 分箱方式包括等频分箱和等距分箱。等频分箱是指经过计算使得每个分箱区间包含大致相等的实例数量；等距分箱是指经过计算使得每个箱体的区间间隔保持一致。
- 需要至少勾选一个无标签数据集特征才能进行模型训练。如果不勾选任何特征，会提示“选择两个数据集，一个有标签，一个无标签，且至少选择一个无标签方特征，才可启动训练。”

图 6-16 特征选择

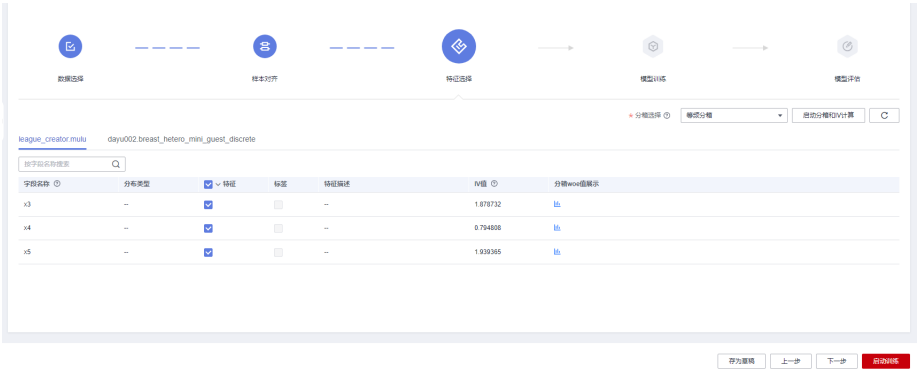


图 6-17 查看特征分箱 woe 值

步骤8 在页面右下角单击“启动训练”进行模型训练。

步骤9 在弹出的界面配置执行参数，配置执行参数可选择常规配置与自定义配置。

- 常规配置：通过界面点选算法使用的常规参数，具体支持的参数请参考表6-3。

表 6-3 常规配置参数

算法类型	参数名	参数描述
XGBoost	学习率	控制权重更新的幅度，以及训练的速度和精度。取值范围为0~1的小数。
	树数量	定义XGBoost算法中决策树的数量，一个样本的预测值是多棵树预测值的加权和。取值范围为1~50的整数。

算法类型	参数名	参数描述
	树深度	定义每棵决策树的深度，根节点为第一层。取值范围为1~10的整数。
	切分点数量	定义每个特征切分点的数量，数量越多，准确率越高，计算时间越长。取值范围为5~10的整数。
	分类阈值	区分正负例的得分阈值。
逻辑回归/FiBiNET	学习率	控制权重更新的幅度，影响训练收敛速度和模型精度，取值范围为0~1。
	迭代次数	完成全部样本训练的次数，取值为正整数。
	批大小	单次训练使用的样本数，取值为正整数。
	分类阈值	区分正负例的得分阈值

- 自定义配置： 通过json格式的文本配置更多高级参数，具体支持的参数请参考**表6-4**。

表 6-4 自定义配置参数

参数	是否必选	参数类型	描述
predict_threshold	否	Float	预测阈值，最小值0，最大值1
learning_rate	否	Float	学习率，最小值0，最大值1
batch_size	否	Integer	批大小，最小值1
epoch	否	Integer	迭代次数，最小值1
tree_num	否	Integer	树数量，最小值1
tree_depth	否	Integer	树深度，最小值1
split_num	否	Integer	切分点数量，最小值5
discrete_embedding_size	否	Integer	离散特征embedding的维度，最小值4
multihot_embedding_size	否	Integer	multihot特征embedding的维度，最小值4
mlp_dims	否	Array of integers	多层感知机每层的节点数
reduction_ratio	否	Integer	senet层压缩比例，最小值2
save_format	否	String	模型保存格式
loss_function	否	String	损失函数
loss_param	否	String	损失函数参数json字符串

图 6-18 常规参数配置（XGBoost）

图 6-19 常规参数配置（逻辑回归/FiBiNET）

图 6-20 自定义参数配置

填写完作业参数，单击“确定”即可开始训练作业。启动作业后会生成一条新的历史作业记录。模型训练页面展示了历史作业的执行情况、模型的评估指标和生成时间。模型的评估指标是使用训练数据集产生的。

单击“查看参数”可以查看该模型训练时指定的机器学习作业参数；逻辑回归作业可以单击“查看中间结果”实时查看每一次迭代的评估指标。

图 6-21 模型训练参数

步骤10 进行模型评估。在历史作业列表中，单击执行成功的记录操作列的“发起评估”，可对该模型发起一次评估作业，用于评估该模型在非训练数据集上的表现。

评估作业需要选择和训练数据集数据结构相同的两方数据集，以保证评估的正常进行。

模型评估指标包括**准确率/AUC/KS/F1/召回率/精确率**，取值范围均在0~1之间。AUC和F1作为综合评估指标，值越大说明训练出的模型越好。

图 6-22 发起评估

----结束

6.6 执行作业

执行横向作业

横向训练型作业在作业配置页面单击“保存”按钮后，单击“提交审批”按钮，审批完成后再单击“执行”按钮。

横向评估型作业在作业配置页面单击“保存”按钮后，可以直接单击“执行”按钮。

步骤1 用户登录进入计算节点页面。

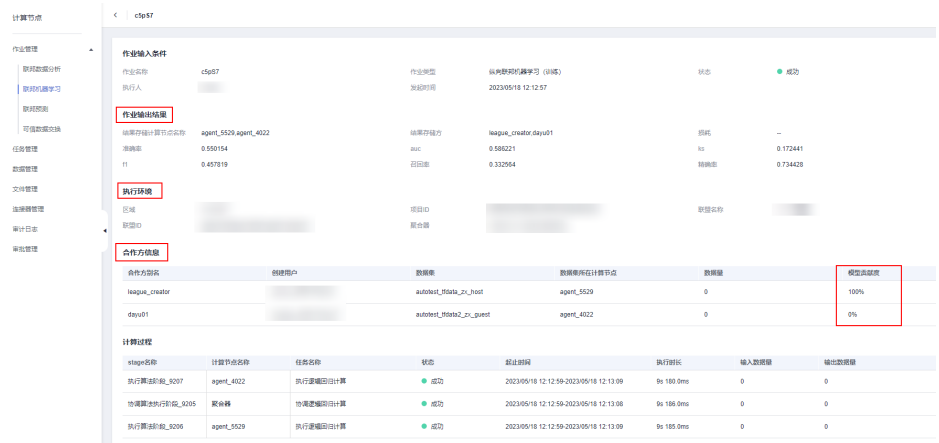
步骤2 在左侧导航树上依次选择“作业管理 > 可信联邦学习”，打开可信联邦学习作业页面。

步骤3 在“可信联邦学习”页面，查找待执行的作业，单击“执行”，系统自动跳转到“历史作业”页面。

图 6-23 执行作业

步骤4 等待执行完成，在“历史作业”页面查看对应的执行结果、作业报告。作业报告展示作业详细信息，包括作业输入条件、输出结果、执行环境、合作方信息和模型贡献度等。

图 6-24 展示作业报告



说明

TICS通过沙普利值衡量每个参与方对于模型的贡献度。贡献度体现了参与方在一个评估模型中的重要程度。参与方模型贡献度越大，表示参与方所提供的数据对于模型的影响越大。

----结束

执行纵向作业

步骤1 用户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 > 可信联邦学习”，打开可信联邦学习作业页面。

步骤3 在“可信联邦学习”页面，查找待执行的纵向作业，单击“执行”。

图 6-25 执行作业

步骤4 在弹出的界面配置执行参数，配置执行参数可选择常规配置与自定义配置。填写完作业参数，单击“确定”即可开始训练作业。

- 常规配置：通过界面点选算法使用的常规参数，具体支持的参数请参考表6-5。

表 6-5 常规配置参数

算法类型	参数名	参数描述
XGBoost	学习率	控制权重更新的幅度，以及训练的速度和精度。取值范围为0~1的小数。
	树数量	定义XGBoost算法中决策树的数量，一个样本的预测值是多棵树预测值的加权和。取值范围为1~50的整数。
	树深度	定义每棵决策树的深度，根节点为第一层。取值范围为1~10的整数。
	切分点数量	定义每个特征切分点的数量，数量越多，准确率越高，计算时间越长。取值范围为5~10的整数。
	分类阈值	区分正负例的得分阈值。
逻辑回归/ FiBiNET	学习率	控制权重更新的幅度，影响训练收敛速度和模型精度，取值范围为0~1。
	迭代次数	完成全部样本训练的次数，取值为正整数。
	批大小	单次训练使用的样本数，取值为正整数。
	分类阈值	区分正负例的得分阈值

- 自定义配置： 通过json格式的文本配置更多高级参数，具体支持的参数请参考表6-6。

表 6-6 自定义配置参数

参数	是否必选	参数类型	描述
predict_threshold	否	Float	预测阈值，最小值0，最大值1
learning_rate	否	Float	学习率，最小值0，最大值1
batch_size	否	Integer	批大小，最小值1
epoch	否	Integer	迭代次数，最小值1
tree_num	否	Integer	树数量，最小值1
tree_depth	否	Integer	树深度，最小值1
split_num	否	Integer	切分点数量，最小值5
discrete_embedding_size	否	Integer	离散特征embedding的维度，最小值4
multihot_embedding_size	否	Integer	multihot特征embedding的维度，最小值4
mlp_dims	否	Array of integers	多层感知机每层的节点数
reduction_ratio	否	Integer	senet层压缩比例，最小值2
save_format	否	String	模型保存格式
loss_function	否	String	损失函数
loss_param	否	String	损失函数参数json字符串

启动作业后会生成一条新的历史作业记录。

步骤5 等待执行完成，在“历史作业”页面查看更详细的作业运行信息，包括执行结果、作业报告。

----结束

6.7 查看作业计算过程和作业报告

在空间侧查看作业计算过程和作业报告

步骤1 用户登录TICS控制台。

步骤2 在左侧导航树上单击“空间作业”，打开“空间作业”页面。

步骤3 在作业列表上，单击对应作业操作栏的“作业报告”。可在弹出的页面查看作业报告。

图 6-26 空间侧查看作业报告

说明

空间侧不支持查看作业执行结果，查看作业执行结果需要去对应的计算节点存储路径查看作业执行的实际结果。

步骤4 查找待查看计算过程的作业，单击作业名称展开，在操作栏单击“计算过程”。

图 6-27 空间侧查看作业计算过程

步骤5 计算过程页面可以单击任务节点，查看开始和结束时间等信息。在计算过程页面下方详情列表打开任务详情，可以查看更详细的计算过程信息。

图 6-28 作业计算过程信息详情（截图为多方安全计算作业示例，请以实际作业为准）

----结束

在计算节点侧查看作业计算过程和作业报告

步骤1 用户登录进入计算节点页面。

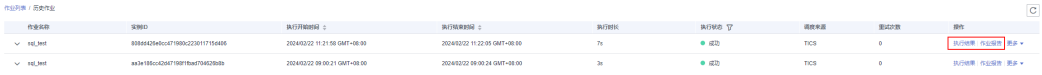
步骤2 在左侧导航树上单击“作业管理”，选择作业类型，打开作业列表页面。

步骤3 查找待获取执行结果和作业报告的作业，单击操作栏的“历史作业”。

图 6-29 历史作业

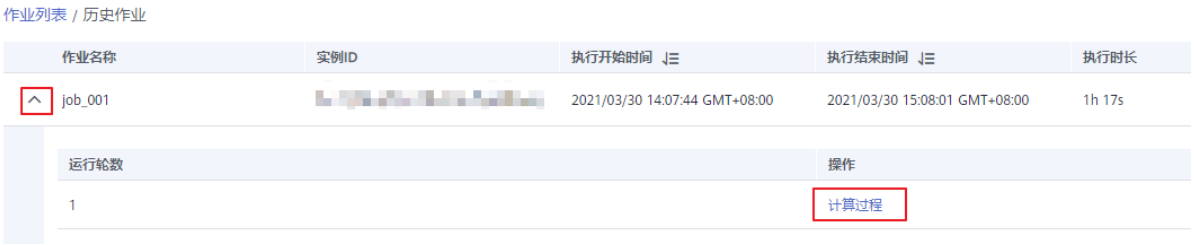
步骤4 在历史作业列表中，单击操作栏的“执行结果”或者“作业报告”。在弹出的页面查看执行结果和作业报告。

图 6-30 查看执行结果、作业报告



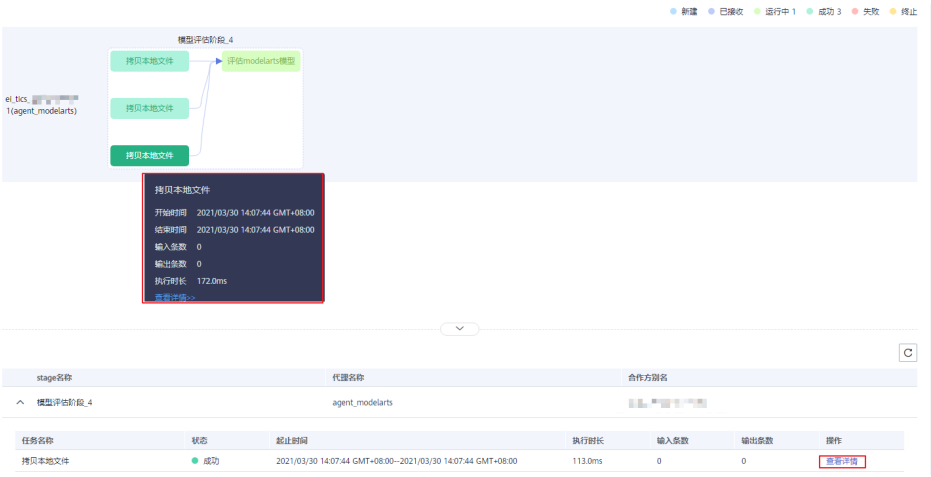
步骤5 在历史作业列表中，查找待查看计算过程的作业，单击作业名称展开，在操作栏单击“计算过程”。

图 6-31 在计算节点侧查看作业计算过程



步骤6 计算过程页面可以单击任务节点，查看开始和结束时间等信息。在计算过程页面下方详情列表打开任务详情，可以查看更详细的计算过程信息。

图 6-32 作业计算过程信息详情（截图为多方安全计算作业示例，请以实际作业为准）



----结束

6.8 删除作业

删除可信联邦学习作业

步骤1 用户登录进入计算节点页面。

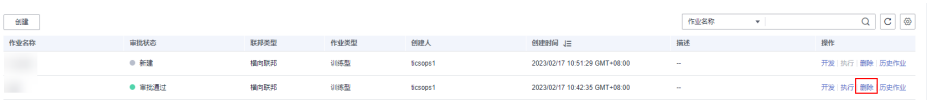
步骤2 在左侧导航树上依次选择“作业管理 > 可信联邦学习”，打开可信联邦学习作业页面。

步骤3 在“可信联邦学习”页面，查找待删除的作业，单击“删除”。

说明

删除操作无法撤销，请谨慎操作。

图 6-33 删除作业



----结束

6.9 安全沙箱机制

TICS支持沙箱能力，TICS计算节点容器属于沙箱，整体架构为数据加工处理提供优于传统沙箱的数据安全保障。

背景

当计算节点执行横向联邦训练型作业时，若执行脚本中包含恶意行为，包含但不限于非授权访问其他作业数据、篡改文件和配置、恶意消耗容器资源等场景时，会影响到数据提供方的计算环境安全以及其他学习作业的正常执行。

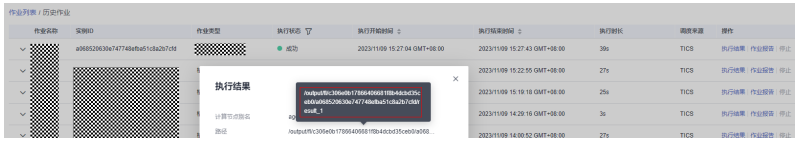
针对该问题，在边缘节点部署场景中，TICS通过构建Python安全沙箱来单独运行横向联邦作业，做到作业运行的安全隔离。

验证安全沙箱防护能力

接下来模拟篡改文件的恶意行为，来验证安全沙箱防护能力。

步骤1 发起方获取某个横向联邦训练作业的训练结果路径。

图 6-34 获取作业结果路径



步骤2 发起方执行恶意脚本，试图篡改所获取的路径中的作业训练结果。

图 6-35 执行恶意脚本

步骤3 发起方执行恶意脚本后，由于安全沙箱确保每个横向联邦作业都是隔离的，当某个作业想去访问或篡改其他作业相关的文件时，无法找到作业执行结果文件，因此脚本执行失败、无法篡改，从而实现安全防护。

图 6-36 恶意脚本执行结果

----结束

7 隐私求交

7.1 概述

隐私求交是可信智能计算服务提供的安全获取参与双方所持数据交集的功能。它允许参与计算的双方，在不获取对方任何额外信息（除交集外的其它信息）的基础上，得到双方持有数据的交集。

约束限制

TICS隐私求交功能支持粗筛和精筛两个步骤。在粗筛环节，会基于求交id的哈希前缀进行前置过滤操作，支持数据规模达到十亿级别。在精筛环节，大规格节点支持的小表数据规模为千万级别。

单独使用场景

数据持有双方为获取己方与对方数据的交集，在不暴露其它数据的情况下，将需要获取交集的那一部分数据与对方的数据，通过创建并执行可信智能计算服务提供的隐私求交作业，可以得到最终交集数据并保存下来，用于后续的数据分析以及使用。

联合使用场景

用于纵向联邦学习中数据对齐。

7.2 创建隐私求交作业

前提条件

参与计算的双方需要在其代理节点上创建好各自的数据集，并需要确保数据集含有非敏感的唯一标识字段。

创建作业

步骤1 用户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 > 隐私求交”，打开隐私求交作业列表页面。

步骤3 在隐私求交作业列表页面，单击“创建”。

图 7-1 创建隐私求交作业

步骤4 在创建页面填写如下信息：

- 作业名称。
- 作业描述可按需填写。
- 勾选参与双方的数据集，同时单击右侧已选数据集的对齐列框选择需要求交集的字段信息。

  说明

  对齐列只能选择非敏感的唯一标识。
- 选择求交算法。
- 选择椭圆曲线。
- 选择大数据量节点。
- 配置重试参数。开关开启后，执行失败的作业会根据配置定时进行重试，仅对开启后的执行作业生效。开关关闭后，关闭前已触发重试的作业不受影响，仅对关闭后的执行作业生效。
- 配置运行参数。运行参数说明：
  - user.task.memory.size：本次作业在用户代理节点中分配的内存大小。
  - stream.count：本次作业的每批流数量，最大值2的32次方-1。
  - user.task.concurrency：用户端数据节点的并发度，默认值为1，当需要提升作业性能时，可以修改该参数，参考配置为CCE集群中规格时建议配置范围4~8，大规格部署时建议配置范围为8~16，具体根据实际需求和情况调整。

步骤5 配置完成后，单击右下角的保存按钮即可新建一个隐私求交作业。

----结束

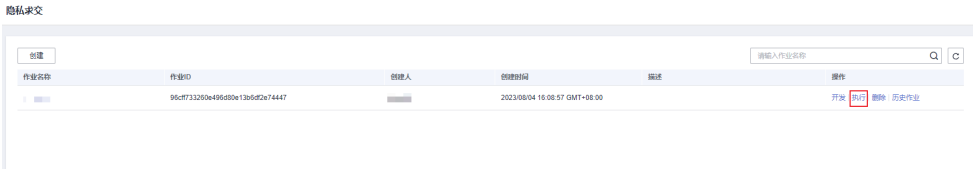
7.3 执行隐私求交作业

步骤1 用户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 > 隐私求交”，打开隐私求交作业列表页面。

步骤3 在已存在的作业项右侧，单击“执行”按钮即可启动执行该作业。

图 7-2 执行隐私求交作业



----结束

7.4 查看作业计算过程和作业报告

在空间侧查看作业计算过程和作业报告

步骤1 用户登录TICS控制台。

步骤2 在左侧导航树上单击“空间作业”，打开“空间作业”页面。

步骤3 在作业列表上，单击对应作业操作栏的“作业报告”。可在弹出的页面查看作业报告。

图 7-3 空间侧查看作业报告

说明

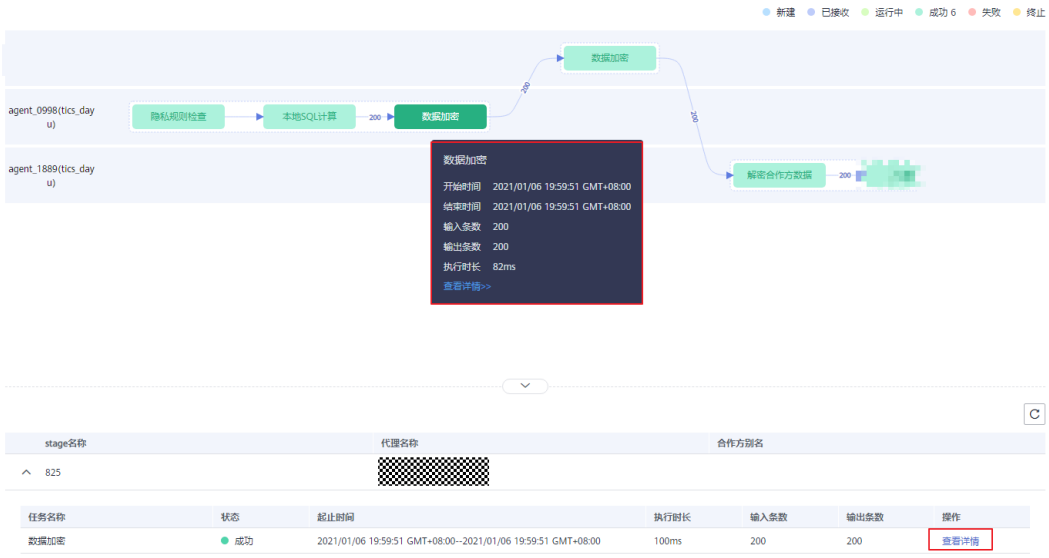
空间侧不支持查看作业执行结果，查看作业执行结果需要去对应的计算节点存储路径查看作业执行的实际结果。

步骤4 查找待查看计算过程的作业，单击作业名称展开，在操作栏单击“计算过程”。

图 7-4 空间侧查看作业计算过程

步骤5 计算过程页面可以单击任务节点，查看开始和结束时间等信息。在计算过程页面下方详情列表打开任务详情，可以查看更详细的计算过程信息。

图 7-5 作业计算过程信息详情（截图为多方安全计算作业示例，请以实际作业为准）



----结束

在计算节点侧查看作业计算过程和作业报告

步骤1 用户登录进入计算节点页面。

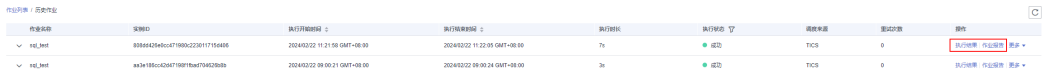
步骤2 在左侧导航树上单击“作业管理”，选择作业类型，打开作业列表页面。

步骤3 查找待获取执行结果和作业报告的作业，单击操作栏的“历史作业”。

图 7-6 历史作业

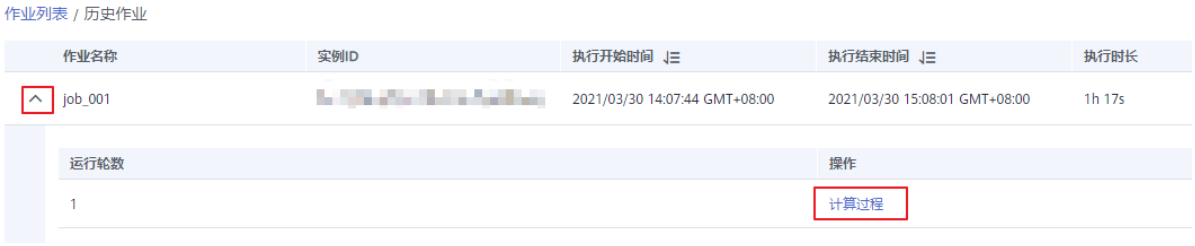
步骤4 在历史作业列表中，单击操作栏的“执行结果”或者“作业报告”。在弹出的页面查看执行结果和作业报告。

图 7-7 查看执行结果、作业报告



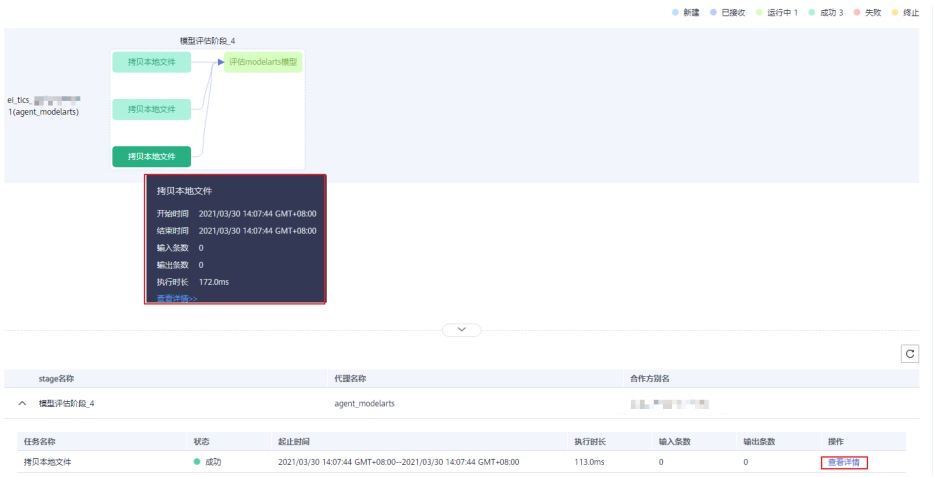
步骤5 在历史作业列表中，查找待查看计算过程的作业，单击作业名称展开，在操作栏单击“计算过程”。

图 7-8 在计算节点侧查看作业计算过程



步骤6 计算过程页面可以单击任务节点，查看开始和结束时间等信息。在计算过程页面下方详情列表打开任务详情，可以查看更详细的计算过程信息。

图 7-9 作业计算过程信息详情（截图为多方安全计算作业示例，请以实际作业为准）



----结束

7.5 删除隐私求交作业

步骤1 用户登录进入计算节点页面。

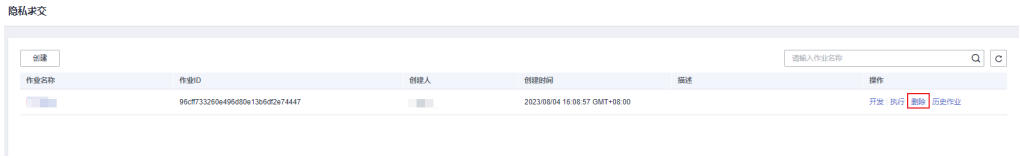
步骤2 在左侧导航树上依次选择“作业管理 > 隐私求交”，打开隐私求交作业列表页面。

步骤3 在隐私求交作业列表页面查找待删除的作业，单击“删除”。

说明

删除操作无法撤销，请谨慎操作。

图 7-10 删除作业



----结束

8 隐匿查询

8.1 概述

目前TICS支持两种隐匿查询方式：

- 批量隐匿查询：支持SQL语言查询，适用大数据量批量查询场景。
- 实时隐匿查询：适用高性能、实时性要求高的查询场景，应用程序可以通过提供的标准API使用。

8.2 批量隐匿查询

隐匿查询，也称隐私信息检索，是指查询方隐藏被查询对象关键词或客户id信息，数据服务方提供匹配的查询结果却无法获知具体对应哪个查询对象。数据不出门且能计算，杜绝数据缓存的可能性。

例如查询方希望查询身份证id为“张三”的人信贷公式数据，发起了一个类似于SELECT salary * 16 + age*10 FROM t WHERE id = ‘张三’的单数据集查询。t表存储在数据提供方计算节点中。查询方不希望有人知道自己查询的是“张三”这个人，也不希望知道查出的这条信贷公式结果具体值。

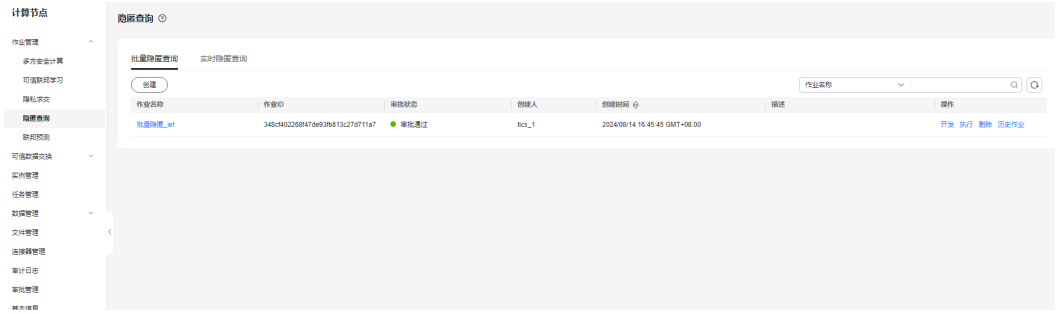
具体操作步骤如下：

步骤1 空间管理员登录TICS控制台。

步骤2 作业发起方进入自己所属的计算节点，进入作业管理->隐匿查询->批量隐匿查询作业，单击创建。

步骤3 编写完作业之后。单击保存，提交审批。

图 8-1 编写批量隐匿查询作业



步骤4 隐匿查询过滤条件出现多个字段时，需要使用.pir或.PIR标识隐匿查询字段。

图 8-2 pir 或.PIR 标识隐匿查询字段

步骤5 单击编辑器右侧的“作业配置项”，进行作业配置。

重试：开关开启后，执行失败的作业会根据配置定时进行重试，仅对开启后的执行作业生效。开关关闭后，关闭前已触发重试的作业不受影响，仅对关闭后的执行作业生效。

执行参数：用于作业调优。当前可用执行参数介绍如下：

- job.ins.memory.size：本次作业在各执行节点分配的内存大小，默认200MB。如果作业中间结果过大，需要调高该参数。
- max.result.file.size：最大存储文件大小，默认10GB。如果最终结果存储超过这个大小，则会执行失败，需要调大该值。
- tics.task.concurrency：在TICS所属计算节点执行计算时的并行度，默认值为1。当需要提升作业性能时，可以修改该参数，参考配置为CCE集群中规格时建议配置范围为4~8，大规格部署时建议配置范围为8~16，具体根据实际需求和情况调整。
- user.task.concurrency：在用户所属计算节点计算时的并行度，默认值为1。当需要提升作业性能时，可以修改该参数，参考配置为CCE集群中规格时建议配置范围为4~8，大规格部署时建议配置范围为8~16，具体根据实际需求和情况调整。
- apsi.num.threads：数据提供方处理查询并发线程数，默认1，取值正整数，并发线程数越大，性能越优。
- id.byte.length：查询id序列化字节长度，默认20，需要根据实际情况调整。
- query.fields.byte.length：查询字段序列化字节长度，默认20，需要根据实际情况调整。

图 8-3 作业配置

步骤6 合作方进入自己所属的计算节点，进入审批管理页面，单击审批详情，查看查询方的sql请求的id为“？？？？”，无法获取查询具体查询数据。

图 8-4 审批详情

说明

- 仅限单表查询，不支持多表查询。
- Sql中必须包含where条件。不支持join操作，即使是单方内的join操作。
- where条件后必须包含隐匿查询字段，隐匿查询字段只能是非敏感唯一标识，且字段数值类型只能是字符串或整数。
- where条件后出现多个字段时必须使用.pir或.PIR标识隐匿查询字段。
- where条件后不支持or语句，多个条件必须使用and进行拼接。
- 隐匿查询字段只能用于where id='xxx'或where id in ('xxx' 'xxx')或where id in (select xx from table)语句。
- 隐匿查询条件为in+子查询时，子查询中数据集只能是发起方数据集。

----结束

8.3 实时隐匿查询

8.3.1 创建作业

前提条件

- 空间组建完成，参考**组建空间**。
- 空间成员完成计算节点部署，配置参数时选择挂载方式和数据目录，参考**部署计算节点**。
- 空间成员在计算节点中完成数据发布，参考**发布数据**。

约束限制

- 避免作业名重复。
- 支持本地连接器配置的CSV类型数据集。
- 支持DWS连接器配置的DWS数据集。
- 支持API连接器配置的API数据集。

创建实时隐匿查询作业

步骤1 用户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 > 隐匿查询 > 实时隐匿查询”，打开实时隐匿查询作业页面。

步骤3 在“实时隐匿查询”作业页面中，单击“创建”。

图 8-5 创建作业

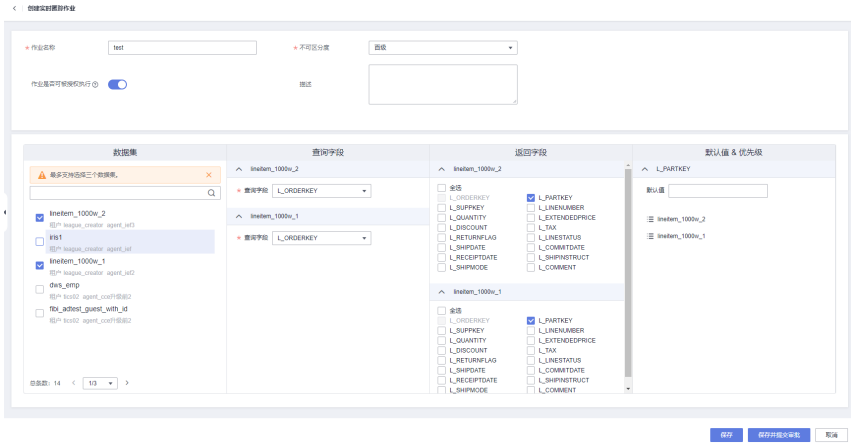
步骤4 在作业创建页面中输入作业名称，选择不可区分度，根据个人需求选择作业是否可被授权执行开关，并填写描述信息。

说明

- 不可区分度是指数据方无法从该数量级中区分出具体的查询值，例如百级不可区分度说明数据方不知道查询方具体查询了百级数量级中哪一条数据。
- 作业是否可被授权执行是指作业是否可被授权给空间内其他节点执行，被授权节点可以直接执行作业并获取作业结果，无编辑、查看、删除、初始化等权限。

然后选择数据集及其对应的查询字段和返回字段。当前支持最多选择3个数据集，同时返回字段支持配置默认值，针对相同的返回字段支持配置优先级。

图 8-6 选择数据文件



步骤5 单击“保存并提交审批”。

----结束

8.3.2 审批实时隐匿查询作业

前提条件

发起方已创建待审批的作业，参考**创建作业**。

约束限制

作业审批通过后，才能单击“启动数据初始化”。

审批实时隐匿查询作业

步骤1 审批方登录进入计算节点页面。

步骤2 在左侧导航树上选择“审批管理”，打开审批页面。

步骤3 选择待处理的审批记录，单击“查看详情”。

步骤4 填写审批意见，单击“同意”。

图 8-7 填写审批意见

----结束

启动数据初始化

审批通过后，发起方可以在实时隐匿查询页面作业列表中单击“启动数据初始化”。

8.3.3 作业授权

前提条件

仅当实时隐匿查询作业开启“作业是否可被授权执行”开关并审批通过后，发起方可以进行作业授权，参考**创建作业**和**审批实时隐匿查询作业**。

作业授权

步骤1 在实时隐匿查询作业列表页面，查找待授权的作业，单击“更多>授权”。

图 8-8 授权作业

步骤2 在弹出的窗口中，选择需要授权的执行节点。授权成功后，被授权节点可以直接执行作业并获取作业结果。

图 8-9 选择授权对象

----结束

取消作业授权

需要取消授权时，可以在作业列表中单击“更多>授权”，在授权窗口中去勾选对应的执行节点，即可取消对此节点的授权。

8.3.4 执行作业

前提条件

已完成作业的审批和数据初始化，参考**审批实时隐匿查询作业**。

执行实时隐匿查询作业

步骤1 作业审批以及数据初始化完成后，单击“执行”按钮。

步骤2 在右侧弹出窗口的ID框中输入查询值，单击“查询”按钮进行实时隐匿查询，实时返回查询结果在下侧方框中。

图 8-10 输入自定义属性

----结束

8.3.5 删除作业

步骤1 用户登录进入计算节点页面。

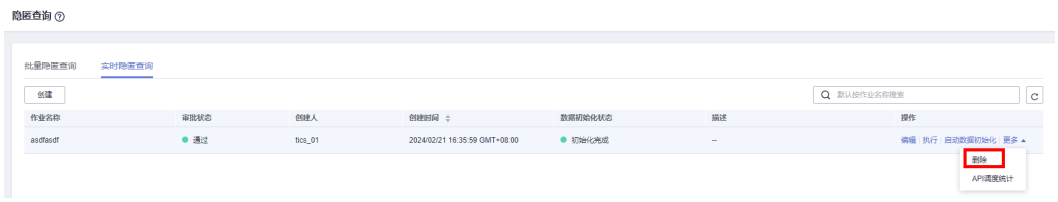
步骤2 在左侧导航树上依次选择“作业管理 > 隐匿查询 > 实时隐匿查询”，打开实时隐匿查询作业页面。

步骤3 在实时隐匿查询作业列表页面查找待删除的作业，单击“更多>删除”，即可删除作业。

说明

删除操作无法撤销，请谨慎操作。

图 8-11 删除作业



----结束

9 联邦预测作业

9.1 概述

联邦预测作业在保障用户数据安全、模型资产安全的前提下，利用多方数据和模型实现样本联合预测。

目前TICS支持两种类型的预测方式：

- 批量预测：

  批量预测通过在计算节点后台发起离线预测任务的方式，在任务完成后可以获得指定数据集中所有样本的预测结果。
- 实时预测：

  实时预测通过在计算节点部署在线预测服务的方式，允许用户利用POST请求，在毫秒级时延内获取单个样本的预测结果。

9.2 批量预测

批量预测通过在计算节点后台发起离线预测任务的方式，在任务完成后可以获得指定数据集中所有样本的预测结果。

9.2.1 创建批量预测作业

前提条件

- 空间组建完成，参考**组建空间**。
- 空间成员完成计算节点部署，配置参数时选择挂载方式和数据目录，参考**部署计算节点**。
- 空间成员在计算节点中完成数据发布，参考**发布数据**。
- 参与方的计算节点如果是采用云租户部署，并且使用子账号进行创建的，需要参考**配置CCE集群子账号权限**。

约束限制

- 避免作业名重复。

- 必须选择一个已有模型才能创建批量预测作业。
- 批量预测作业必须选择一个当前计算节点发布的数据集。

创建联邦预测作业

批量预测作业在本地运行，目前支持XGBoost算法、逻辑回归LR算法、深度神经网络FiBiNet算法。

步骤1 用户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 > 联邦预测”，打开联邦预测作业页面。

步骤3 在“联邦预测”页面，选择批量预测的Tab页，单击创建。

图 9-1 创建作业

步骤4 在弹出的对话框中编辑“作业名称”，选择“算法类型”。

选择“算法类型”之后，配置是否开启作业重试：开关开启后，执行失败的作业会根据配置定时进行重试，仅对开启后的执行作业生效。开关关闭后，关闭前已触发重试的作业不受影响，仅对关闭后的执行作业生效。

对重试操作配置后，配置CPU配额和内存配额。执行批量预测作业时，会创建新容器来执行，这两个配额参数的值为创建新容器的CPU核数和内存大小，默认CPU核数为1，内存大小512M。

然后勾选“选择训练作业”列表中的某一训练作业，然后勾选“选择模型”列表中对应模型，最后单击“确定”按钮完成作业创建。

步骤5 参数配置完成后，单击确认，完成批量预测任务的创建。

----结束

9.2.2 编辑批量预测作业

步骤1 用户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 > 可信联邦学习”，打开可信联邦学习作业页面。

步骤3 在“联邦预测”页面，选择批量预测的Tab页，找到待开发的作业，单击“开发”。

图 9-2 开发作业

步骤4 在弹出的对话框中编辑“选择模型”。只允许选择模型，其它作业参数暂时不支持修改。

单击保存。

----结束

9.2.3 执行批量预测作业

前提条件

参与方的计算节点如果是采用云租户部署，并且使用子账号进行创建的，需要参考**配置CCE集群子账号权限**给子账号增加权限配置。

执行批量预测作业

步骤1 用户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 > 联邦预测”，打开联邦预测作业页面。

步骤3 在“联邦预测”页面批量预测Tab页，查找待执行的作业，单击“发起预测”，在系统弹窗中填写“分类阈值”，勾选数据集发起联邦预测。

如果在**创建联邦预测作业 步骤4**中勾选的模型不包含标签方特征，联邦预测支持只勾选己方数据集发起单方预测。

图 9-3 发起预测

图 9-4 勾选数据集

步骤4 在“联邦预测”页面批量预测Tab页单击“历史预测”，可以“查看结果”和“作业报告”。

- “查看结果”为预测结果存储相对路径。分类作业的预测结果为0/1标签以及正负样本概率，0表示负样本，1表示正样本；回归作业的预测结果为最后的样本得分。
- “作业报告”为作业的详细信息，如作业输入条件、作业输出结果、执行环境、合作方信息、计算过程等。

图 9-5 历史预测

----结束

9.2.4 删除批量预测作业

删除批量预测作业

步骤1 用户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 > 联邦预测”，打开联邦预测作业页面。

步骤3 在“联邦预测”页面批量预测，查找待删除的作业，单击“删除”。

说明

删除操作无法撤销，请谨慎操作。

图 9-6 删除作业

----结束

9.3 实时预测

实时预测通过在计算节点部署在线预测服务的方式，允许用户利用POST请求，在毫秒级时延内获取单个样本的预测结果。

9.3.1 创建实时预测作业

前提条件

- 空间组建完成，参考**组建空间**。
- 空间成员完成计算节点部署，配置参数时选择挂载方式和数据目录，参考**部署计算节点**。
- 空间成员在计算节点中完成数据发布，参考**发布数据**。

约束限制

- 避免作业名重复。
- 必须选择一个已有的FiBiNet模型才能创建实时预测作业。
- 实时预测作业必须选择训练FiBiNet模型的参与方计算节点发布的数据集。
- 创建训练模型时参数必须有"save_format": "SAVED_MODEL"。

创建联邦预测作业

实时预测作业在本地运行，目前仅支持深度神经网络FiBiNet算法。

步骤1 用户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 > 联邦预测”，打开联邦预测作业页面。

步骤3 在“联邦预测”页面，选择实时预测的Tab页，单击创建。

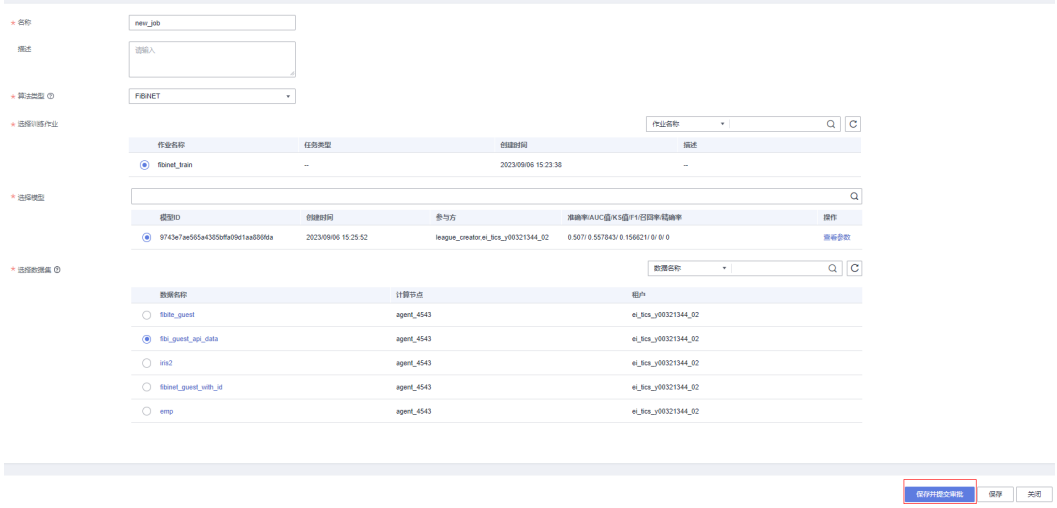
图 9-7 创建作业

步骤4 在弹出的对话框中编辑“作业名称”，选择“算法类型”。

选择“算法类型”之后，勾选“选择训练作业”列表中的某一训练作业，然后勾选“选择模型”列表中对应模型，再勾选”选择数据集”列表中参与方预测要用的某一数据集，最后单击“保存并提交审批”按钮完成作业创建。等审批方审批完后，就可以执行任务。

注意：选择的数据集中需要有样本id列，后面预测需要使用。

图 9-8 新建作业



步骤5 等待参与方审批，当参与方单击“同意”后，就可以执行任务了。

图 9-9 审批详情

----结束

9.3.2 执行实时预测作业

执行实时预测作业

步骤1 用户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 > 联邦预测”，打开联邦预测作业页面。

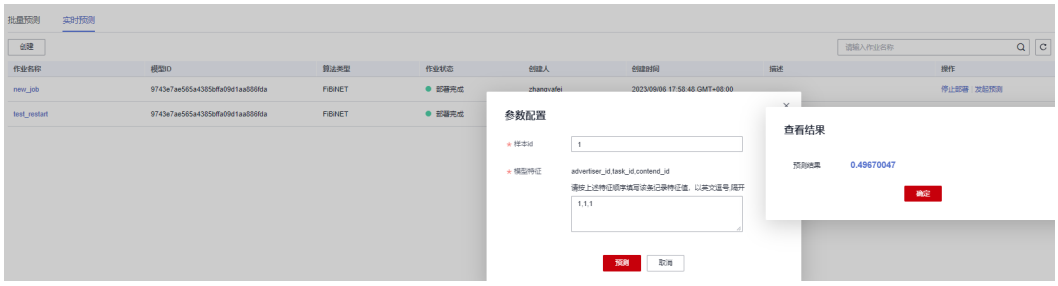
步骤3 在“联邦预测”页面实时预测Tab页，单击“模型部署”，开始部署模型。

图 9-10 模型部署

步骤4 模型部署完成后，单击“发起预测”，在系统弹窗中填写要预测的“样本id”和“模型特征”对应的数值，然后单击“预测”，就会有系统弹窗弹出，显示预测结果。

注意：样本id从创建作业选择数据集的样本id列获取。

图 9-11 发起预测



----结束

9.3.3 删除实时预测作业

删除实时预测作业

步骤1 用户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 > 联邦预测”，打开联邦预测作业页面。

步骤3 在“联邦预测”页面实时预测tab页，查找待删除的作业，单击“删除”。如果作业处于“部署完成“状态，需要单击“停止部署”后，方可删除。

说明

删除操作无法撤销，请谨慎操作。

图 9-12 删除作业

----结束

9.4 查看作业计算过程和作业报告

在空间侧查看作业计算过程和作业报告

步骤1 用户登录TICS控制台。

步骤2 在左侧导航树上单击“空间作业”，打开“空间作业”页面。

步骤3 在作业列表上，单击对应作业操作栏的“作业报告”。可在弹出的页面查看作业报告。

图 9-13 空间侧查看作业报告

说明

空间侧不支持查看作业执行结果，查看作业执行结果需要去对应的计算节点存储路径查看作业执行的实际结果。

步骤4 查找待查看计算过程的作业，单击作业名称展开，在操作栏单击“计算过程”。

图 9-14 空间侧查看作业计算过程

步骤5 计算过程页面可以单击任务节点，查看开始和结束时间等信息。在计算过程页面下方详情列表打开任务详情，可以查看更详细的计算过程信息。

图 9-15 作业计算过程信息详情（截图为多方安全计算作业示例，请以实际作业为准）

----结束

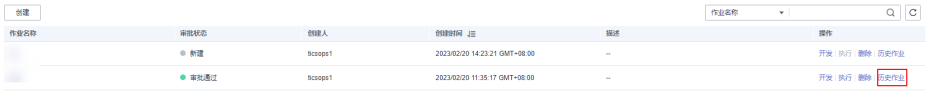
在计算节点侧查看作业计算过程和作业报告

步骤1 用户登录进入计算节点页面。

步骤2 在左侧导航树上单击“作业管理”，选择作业类型，打开作业列表页面。

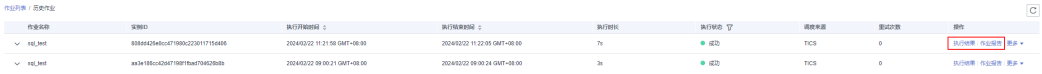
步骤3 查找待获取执行结果和作业报告的作业，单击操作栏的“历史作业”。

图 9-16 历史作业



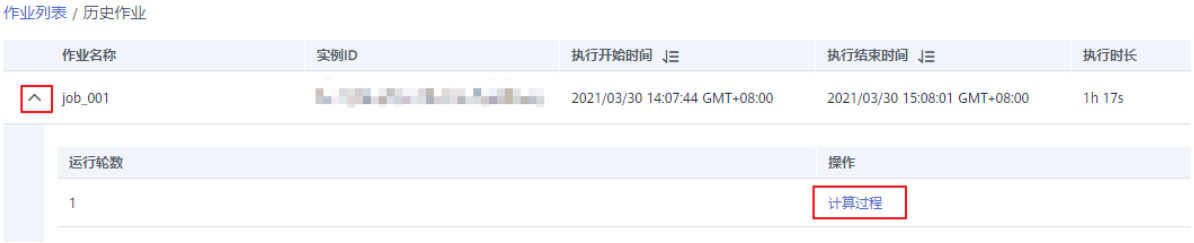
步骤4 在历史作业列表中，单击操作栏的“执行结果”或者“作业报告”。在弹出的页面查看执行结果和作业报告。

图 9-17 查看执行结果、作业报告



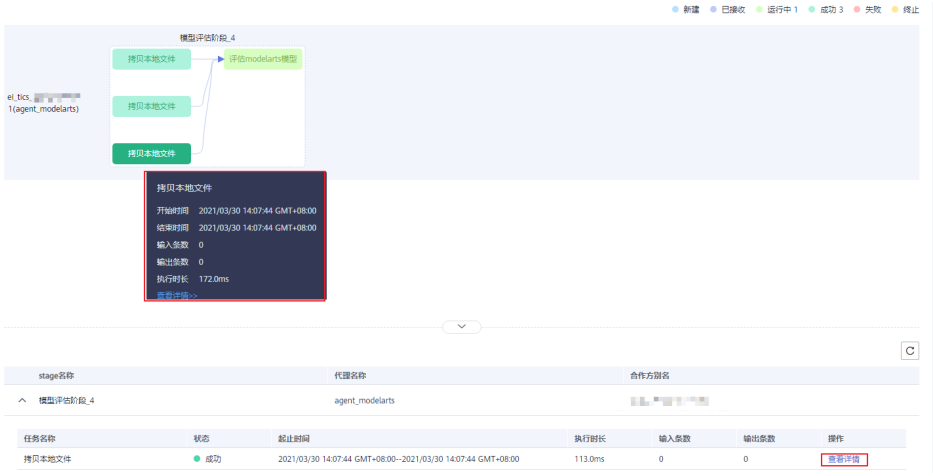
步骤5 在历史作业列表中，查找待查看计算过程的作业，单击作业名称展开，在操作栏单击“计算过程”。

图 9-18 在计算节点侧查看作业计算过程



步骤6 计算过程页面可以单击任务节点，查看开始和结束时间等信息。在计算过程页面下方详情列表打开任务详情，可以查看更详细的计算过程信息。

图 9-19 作业计算过程信息详情（截图为多方安全计算作业示例，请以实际作业为准）



----结束

10 可信数据交换

10.1 概述

基于数据胶囊技术，将用户配置属性嵌入到数据加密策略中，只有匹配属性的用户才能打开文件，达到数据出域后仍然主权可控的目的。

进行数据交换的角色分为用数方和供数方，用数方通过发送申请传递数据使用需求；供数方确认使用需求后，创建合约发送到供数方进行签署，一旦合约生效，数据交换作业就可以执行。

10.2 创建申请

用数方可以在数据目录选取需要的数据集，创建数据申请并描述需求，发送至供数方审视需求。

支持的数据源类型：CSV或者二进制的本地文件、MySQL、Hive，其中MySQL和Hive的数据集配置可参照**管理数据**章节。

前提条件

- 空间组建完成，参考**组建空间**。
- 空间成员完成计算节点部署，配置参数时选择挂载方式和数据目录，参考**部署计算节点**。
- 空间成员在计算节点中完成数据发布，参考**发布数据**。

约束限制

- 避免作业名重复。
- 支持本地连接器配置的数据交换类型文件。
- 只可以申请使用非己方的数据。

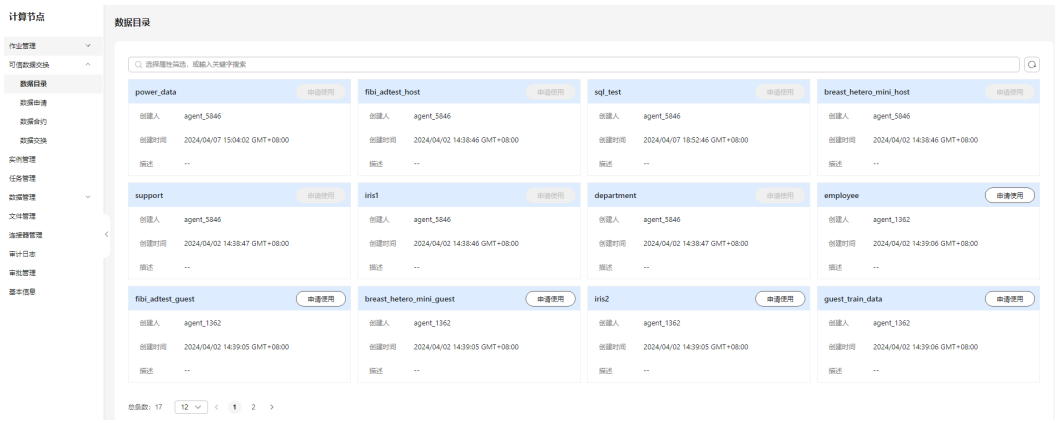
创建数据交换作业

步骤1 用户登录进入计算节点页面。

步骤2 在左侧导航树上依次选择“可信数据交换 > 数据目录”，打开“数据目录”页面。

步骤3 在“数据目录”页面，对数据集单击“申请使用”。

图 10-1 创建数据申请



步骤4 在申请使用界面配置使用字段及用数方的访问需求。

图 10-2 设置使用的字段及访问的需求

- 支持选择访问截止时间、访问方式、访问次数。
- 不设置访问次数时，则不限制访问次数。

步骤5 单击保存或者保存并提交审批。

在“可信数据交换 > 数据申请 > 我创建的”的页签下可以查看、编辑、删除已创建的申请。

----结束

10.3 确认申请

供数方接受用数方的数据使用需求，审视是否符合用数方需求或与前期的约定一致，若不符合，可拒绝申请；若符合，则确认申请，接下来便拟定合约，发送给用数方签署。

前提条件

存在已创建的申请。

约束限制

仅供数方操作，即该数据集的提供方去确认申请。

用数方提交申请后未撤回的申请，一旦供数方确认申请，申请内容无法修改。

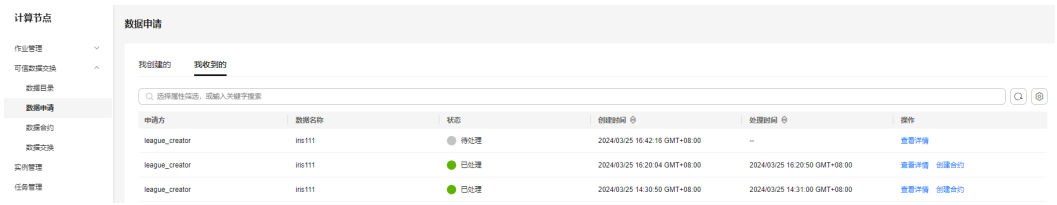
创建数据交换作业

步骤1 用户登录进入计算节点页面。

步骤2 在左侧导航树上选择“可信数据交换 > 数据申请”，打开数据申请页面。

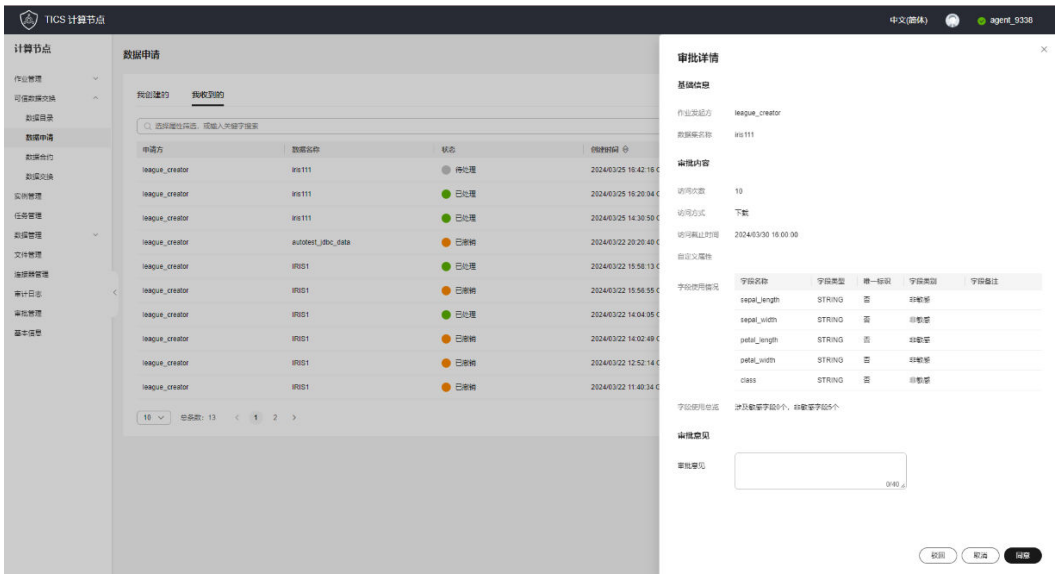
步骤3 在数据申请页面单击“我收到的”，查看供数方节点收到的申请列表。

图 10-3 我收到的数据申请



步骤4 在申请列表中选择申请状态为“待处理”，单击“查看详情”了解用数方需求。根据实际情况同意或者驳回申请。

图 10-4 查看详情



步骤5 （可选）如果同意申请，则可以创建合约，继续后续的合约流程，即用数方达成数据交换的合约。

----结束

10.4 创建合约

供数方可以在TICS 可信数据交换数据合约页面编辑、查看、发送合约给用数方，确认数据使用的合约详情，还可以撤回、中止合约。

前提条件

- 空间组建完成，参考**组建空间**。
- 空间成员完成计算节点部署，配置参数时选择挂载方式和数据目录，参考**部署计算节点**。
- 空间成员在计算节点中完成数据发布，参考**发布数据**。

约束限制

存在已创建的用数申请。

操作步骤

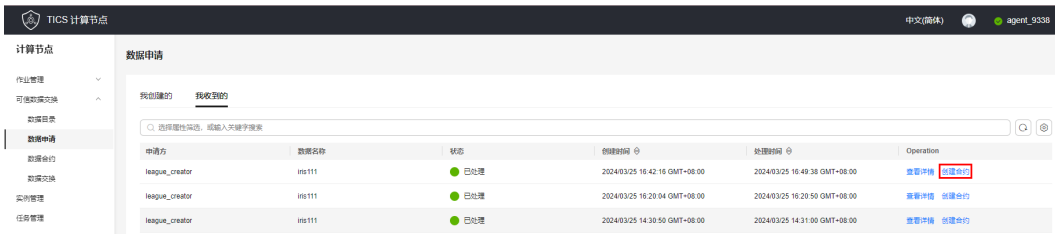
步骤1 用户登录进入计算节点页面。

步骤2 在左侧导航树上选择“可信数据交换 > 数据申请”，打开数据申请页面。

步骤3 在数据申请页面单击“我收到的”。

步骤4 在“我收到的”数据申请页签中，选择已经确认的申请，单击“创建合约”。

图 10-5 创建合约



步骤5 在创建合约对话框填写合约信息。

数据合约的内容有五个部分，包括：

1、合约内容：合约名称、合约描述。

2、数据信息：主要描述结构化数据的列信息，包含数据名称、创建人、创建时间描述等信息。

3、访问需求：主要描述数据用方的需求，包含访问截止时间、访问方式、访问次数。

4、访问限制：暂不支持。

5、自定义限制：自定义策略支持“<”、“>”和“=”。

供数方可以设置自定义属性来进一步强化数据访问控制。

图 10-6 填写参数

步骤6 单击“保存并提交审批”。

在“可信数据交换 > 数据合约 > 我创建的”的页签下可以查看、编辑、撤回已创建的合约。

----结束

10.5 签署合约

用数方在接受到供数方发送的数据合约，若满足需求或与前期约定一致，可签署合约，若不一致，可选择拒绝合约。

前提条件

- 空间组建完成，参考**组建空间**。
- 空间成员完成计算节点部署，配置参数时选择挂载方式和数据目录，参考**部署计算节点**。
- 空间成员在计算节点中完成数据发布，参考**发布数据**。
- 存在已创建的合约。

约束限制

- 仅用数方操作。

  如果用数方一直未审批签署合约，供数方可以撤回合约，重新编辑。一旦用数方确认，则合约内容无法修改。但供数方可中止合约。
- 对审批中的合约才可以进行签署。

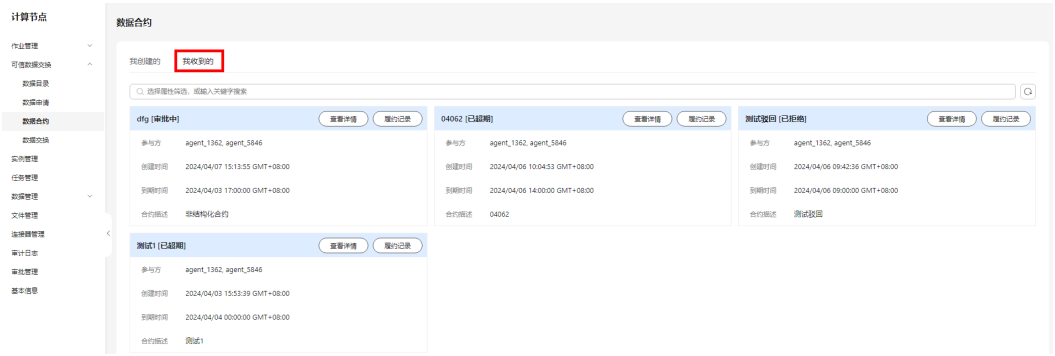
操作步骤

步骤1 用户登录进入计算节点页面。

步骤2 在左侧导航树上选择“可信数据交换 > 数据合约”，打开数据合约页面。

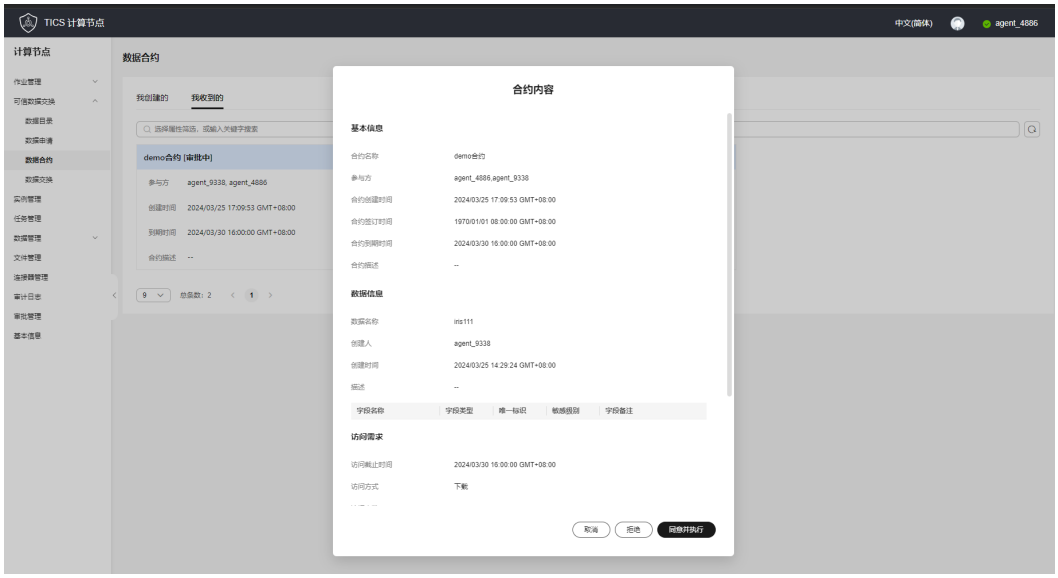
步骤3 在数据合约页面单击“我收到的”。

图 10-7 我收到的数据合约



步骤4 单击“查看详情”，查看合约内容。

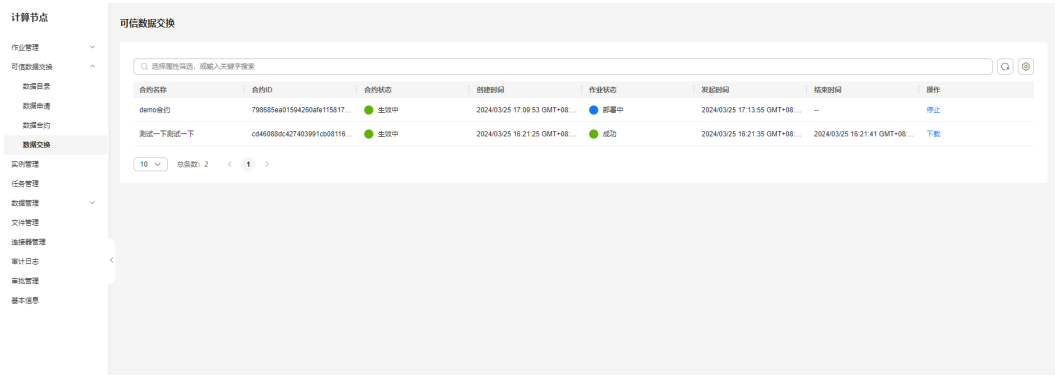
图 10-8 查看合约内容



步骤5 单击“同意并执行”，签署合约，合约开始履行。或者拒绝合约。

步骤6 在左侧导航树上选择“可信数据交换 > 数据交换”，在可信数据交换页面，查看交换作业的执行情况。

图 10-9 查看交换作业的执行情况



步骤7 单击“下载”，即可使用数据。

----结束

10.6 查看履约记录

查看供数方和用数方在合约界面的履约记录，包括关于合约的创建、提交、撤回、拒绝、确认、中止、到期、作业执行、文件解密等关键事件。

前提条件

已创建合约，参考**创建合约**。

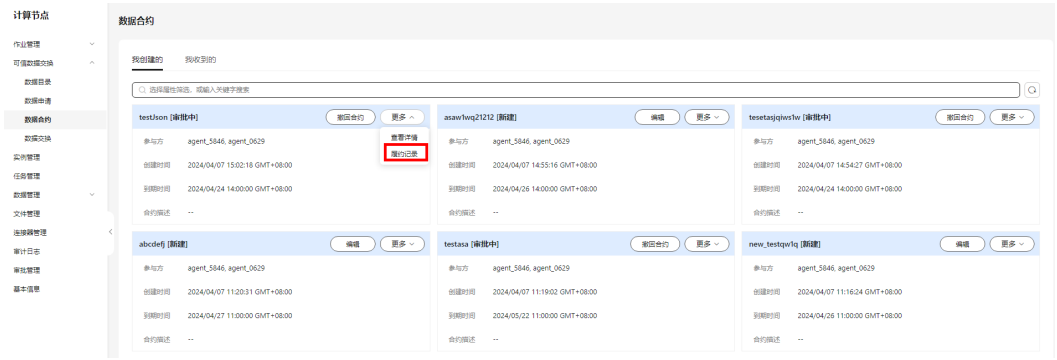
创建数据交换作业

步骤1 用户登录进入计算节点页面。

步骤2 在左侧导航树上选择“可信数据交换 > 数据合约”，打开数据合约页面。

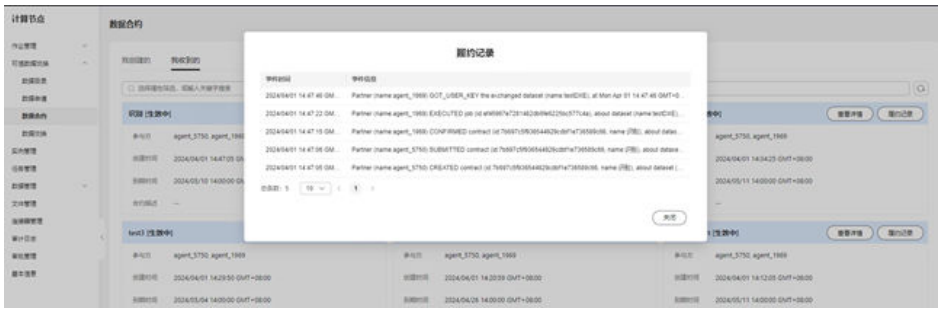
步骤3 在数据合约页面单击“我创建的”，单击“更多 > 履约记录”。

图 10-10 履约记录



步骤4 在弹出的对话框展示履约记录的内容。

图 10-11 查看履约记录详情



作为合约的参与一方，可以查看合约从创建、签署以及合约执行（文件交换），以及文件解密的整个过程。

合约双方都可以查看整个合约的履约过程。

----结束

10.7 查看作业计算过程和作业报告

在空间侧查看作业计算过程和作业报告

步骤1 用户登录TICS控制台。

步骤2 在左侧导航树上单击“空间作业”，打开“空间作业”页面。

步骤3 在作业列表上，单击对应作业操作栏的“作业报告”。可在弹出的页面查看作业报告。

图 10-12 空间侧查看作业报告

说明

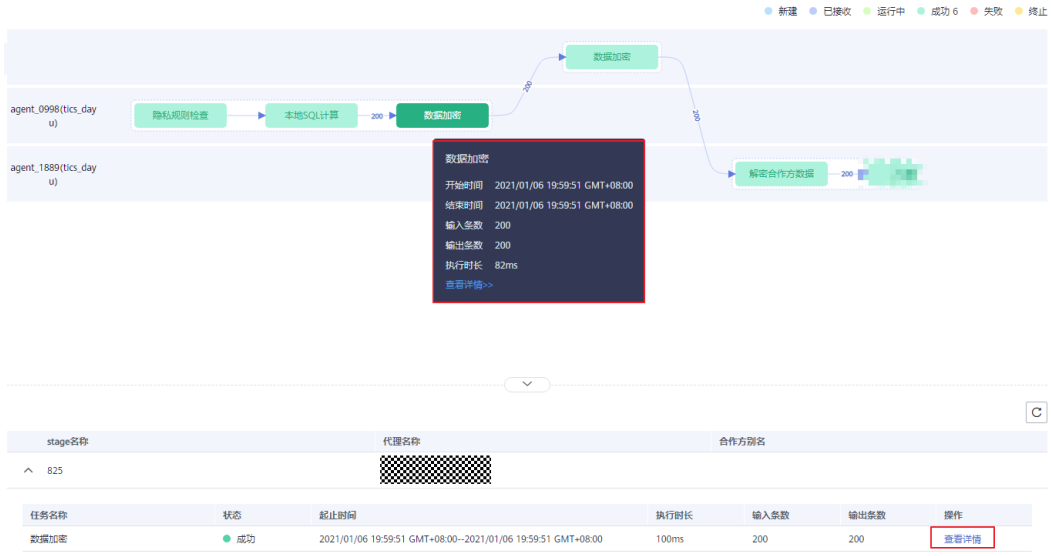
空间侧不支持查看作业执行结果，查看作业执行结果需要去对应的计算节点存储路径查看作业执行的实际结果。

步骤4 查找待查看计算过程的作业，单击作业名称展开，在操作栏单击“计算过程”。

图 10-13 空间侧查看作业计算过程

步骤5 计算过程页面可以单击任务节点，查看开始和结束时间等信息。在计算过程页面下方详情列表打开任务详情，可以查看更详细的计算过程信息。

图 10-14 作业计算过程信息详情（截图为多方安全计算作业示例，请以实际作业为准）



----结束

在计算节点侧查看作业计算过程和作业报告

步骤1 用户登录进入计算节点页面。

步骤2 在左侧导航树上单击“作业管理”，选择作业类型，打开作业列表页面。

步骤3 查找待获取执行结果和作业报告的作业，单击操作栏的“历史作业”。

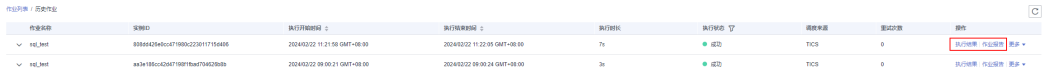
图 10-15 历史作业

步骤4 在历史作业列表中，单击“下载结果”。若作业提示已过期，则表明权限已过期，无法下载结果，需重新提交审批。

弹窗中输入自定义属性，没有则不填，单击确定即可通过浏览器下载文件。

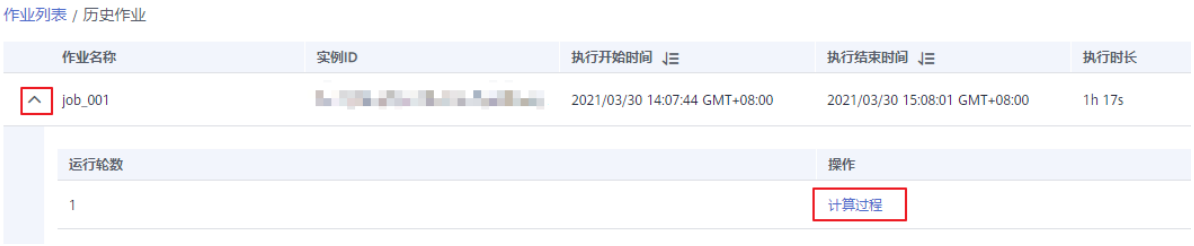
步骤5 在历史作业列表中，单击操作栏的“执行结果”或者“作业报告”。在弹出的页面查看执行结果和作业报告。

图 10-16 查看执行结果、作业报告



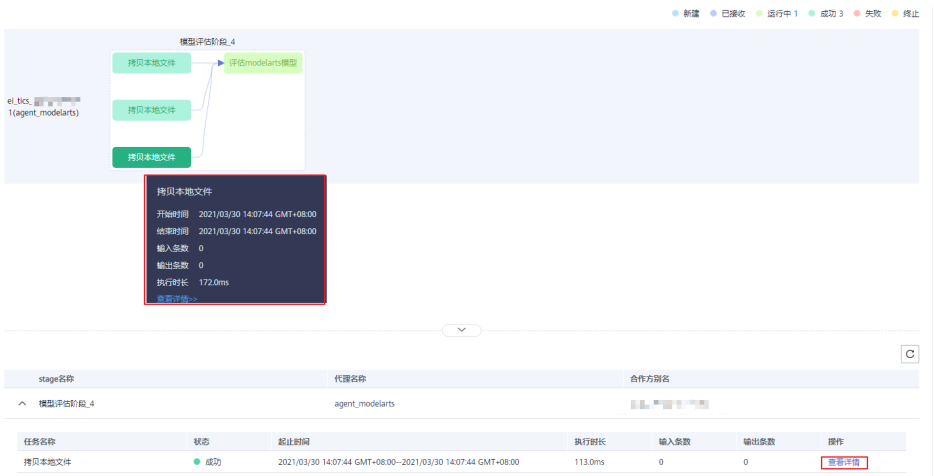
步骤6 在历史作业列表中，查找待查看计算过程的作业，单击作业名称展开，在操作栏单击“计算过程”。

图 10-17 在计算节点侧查看作业计算过程



步骤7 计算过程页面可以单击任务节点，查看开始和结束时间等信息。在计算过程页面下方详情列表打开任务详情，可以查看更详细的计算过程信息。

图 10-18 作业计算过程信息详情（截图为多方安全计算作业示例，请以实际作业为准）



----结束

