

跨节点计算及价值挖掘平台-用户手册

1. 平台介绍

1.1. 平台简介

跨节点计算及价值挖掘平台是一个隐私计算平台，专注于隐私计算技术，实现跨节点数据价值分析和挖掘，同时保护隐私信息。

平台提供轻量级部署解决方案，使数据开发人员可以在几小时内开始使用隐私计算技术。DSF 模块包括全生命周期的隐私计算能力，如联邦学习和多方安全学习，以及资源管理能力，如节点管理、数据集管理、计算场景管理、任务管理和模型管理。

通过全面的安全机制，该平台确保数据可用且不可见，满足用户在数据协作中对安全、合规和隐私保护的强烈需求，为数据协作中涉及的所有方建立一个可信和公平的处理和应用环境，促进业务发展和创新应用。

1.2. 平台亮点

轻量级部署

DSF 使用轻量级部署架构。在完成部署资源准备后，部署过程大幅简化至数个命令行即可完成，将整个部署过程从数周或数月缩短到数天内甚至数小时完成。

通过场景机制确保数据“最小可用”的授权原则

隐私保护不仅仅是隐私计算技术就能解决的简单问题（当然，DSF 提供了全套先进的隐私计算技术），而是一个完整的生命周期的工程问题。

DSF 采用了计算场景的授权机制——场景由参与者、数据集、应用程序和算力的组合编排定义，即：通过 DSF 进行的数据协作都需要定义谁（与谁协作）、什么（使用哪些数据集）、如何（使用哪些应用程序）和何处（计算发生在哪里）。

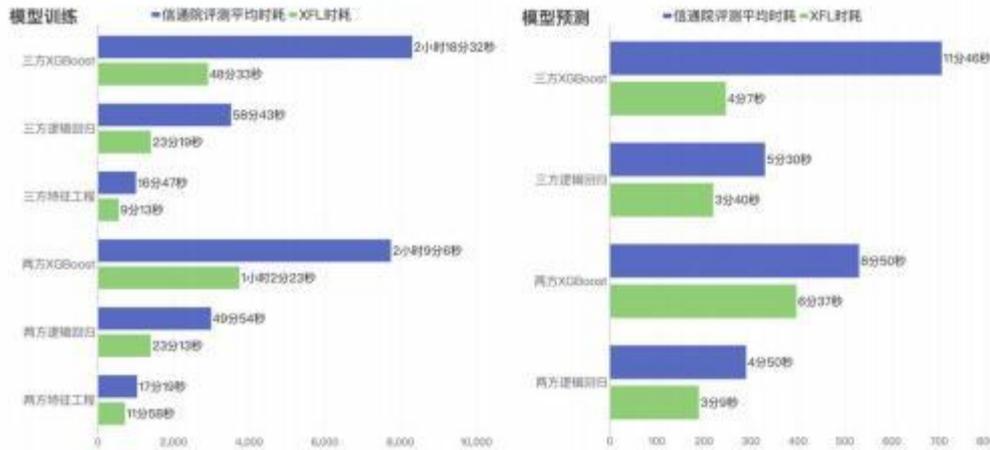
领先的联邦学习技术，可视化建模工具

XFL（由 Basebit 开发的联邦学习框架）是一个高性能、高灵活性、高适用性、轻量级、开放且易于使用的联邦学习框架。它支持横向和纵向联邦场景下的各种联邦模型。为了让用户合法、合规地共同训练模型，挖掘数据的价值，XFL 采用同态加密、差分隐私、安全多方计算等安全技术来保护用户的本地数据不被泄露，并应用安全通信协议来确保通信安全。

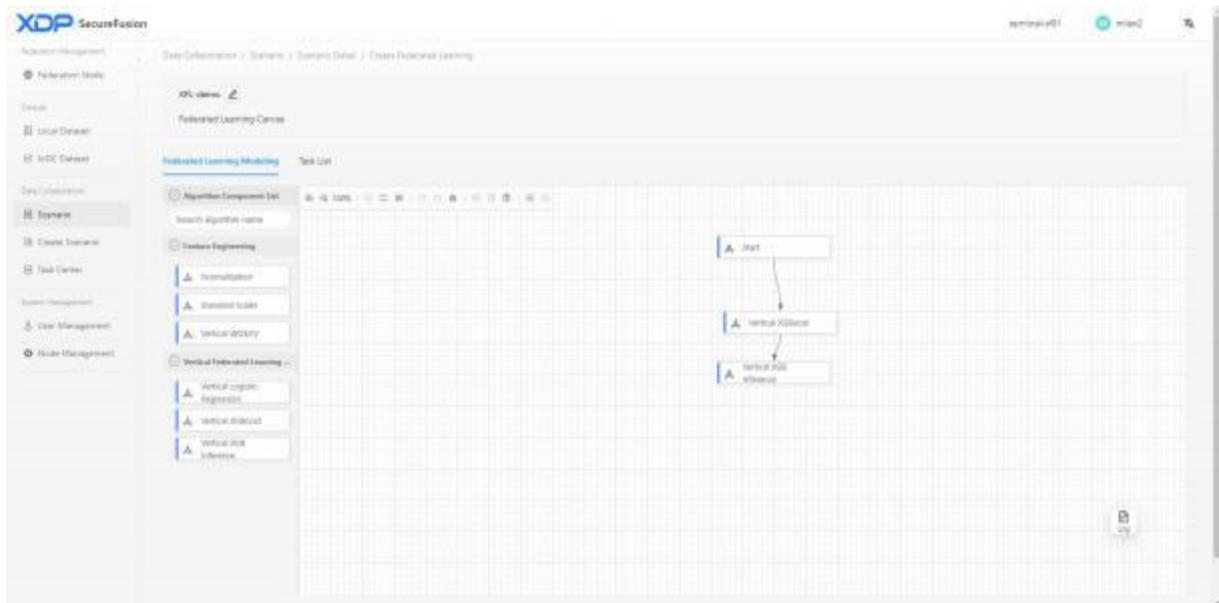
XFL 性能 - 信通院性能评测

BaseBit.ai 翼方健数®

设备信息: 6台服务器, 2*Intel至强5218 (2.3GHz/16-Core)、256G内存和1.6T SSD, 带宽: 1000Mbit/s
数据概况: 样本数: 训练集40w样本; 验证集10w样本
特征数: 两方联邦: 每方450维; 三方联邦: 每方300维



平台提供可视化建模画布, 非代码开发人员的使用者也可轻松上手, 快速使用联邦学习组件训练联邦学习模型。



XFL 算法目前已开源, 可前往查看更多信息: [Welcome to XFL's documentation! — XFL 1.2.0 documentation](#)

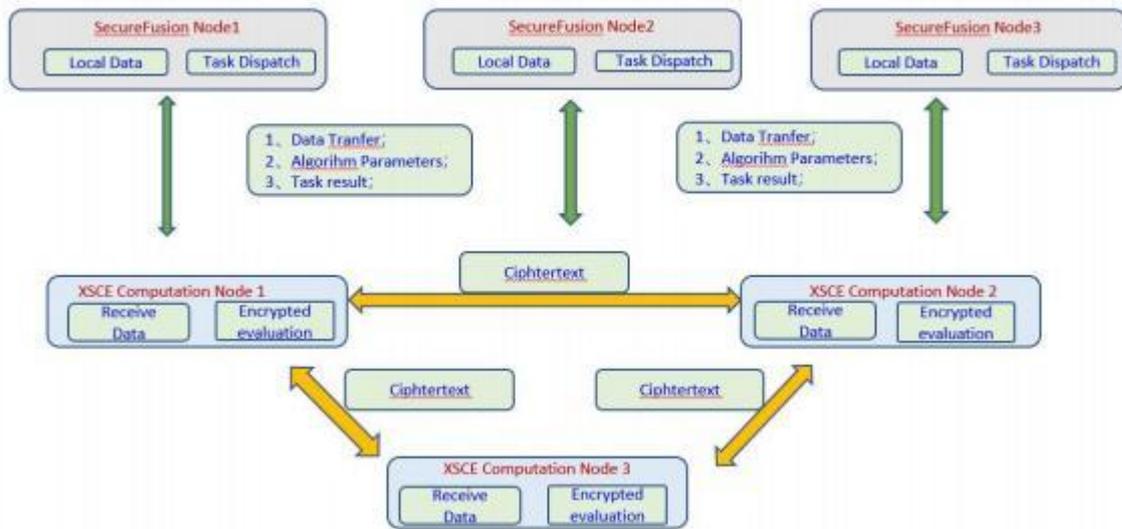
领先的多方安全计算技术 - XSCE

XSCE (XDP 安全计算引擎) 是一个高性能、功能丰富、灵活、集成的基于密码学的隐私计算引擎。

👉 已通过信通院评测, 且所有算法的性能都优于评测平均水平

👉 PSI 的性能比大多数供应商都要好: 100M 样本的 PSI 时间成本在 1000Mb 网络上不到 10 分钟;

👉 PIR: 在 100 万数据中进行 1 条数据查询的时间成本在 1000Mb 网络上不到 3 分钟。



2. 更多信息

2.1. 行业解决方案

营销

通过 DSF，您可以在广告商、渠道和数据源之间建立分布式的联盟网络，进行数据协作。例如，在营销行业中可以应用联邦学习，实现跨多个设备进行用户数据的隐私保护协作建模，无需与中央服务器共享数据。这可以帮助提高广告定向的效率和准确性，因为它允许在建模和分析过程中使用更多样化和全面的数据集。

金融

金融是广泛采用隐私计算的行业之一。典型的应用案例包括：

👉 反欺诈：

金融机构往往只能看到其客户财务活动的一部分。使用隐私安全技术可以帮助机构协作隐私保护信息共享，例如，通过多方安全计算技术，金融机构可利用 DSF 构建的分布式联盟网络获取其客户在各银行的贷款金额总额，从而对客户的风脸程度进行判断，使其能够更有效地打击网络犯罪和欺诈，同时保证客户的数据安全。

👉 营销：

银行和其他金融机构可以使用联邦学习来训练客户交易数据的模型，而不必将该数据发送到中央服务器。通过 DSF，每个客户的设备或本地服务器可以在其自己的数据上训练模型，然后将更新的模型参数发送回银行的服务器，以与其他客户的模型进行聚合。这样，机构可以

在不访问个别客户交易数据的情况下提高其营销效果。

医疗

在医疗行业中，联邦学习被用于各种应用，例如预测患者再入院、识别疾病早期迹象和检测医疗欺诈。

医疗模型构建：

通过 DSF 构建分布式的联盟网络，同一个模型能够在来自多个医院或诊所的分布式患者数据上进行训练，而无需将数据集中在一个位置。这确保了患者数据的隐私和安全，同时仍允许协作和准确的分析。

2.2. 基本概念

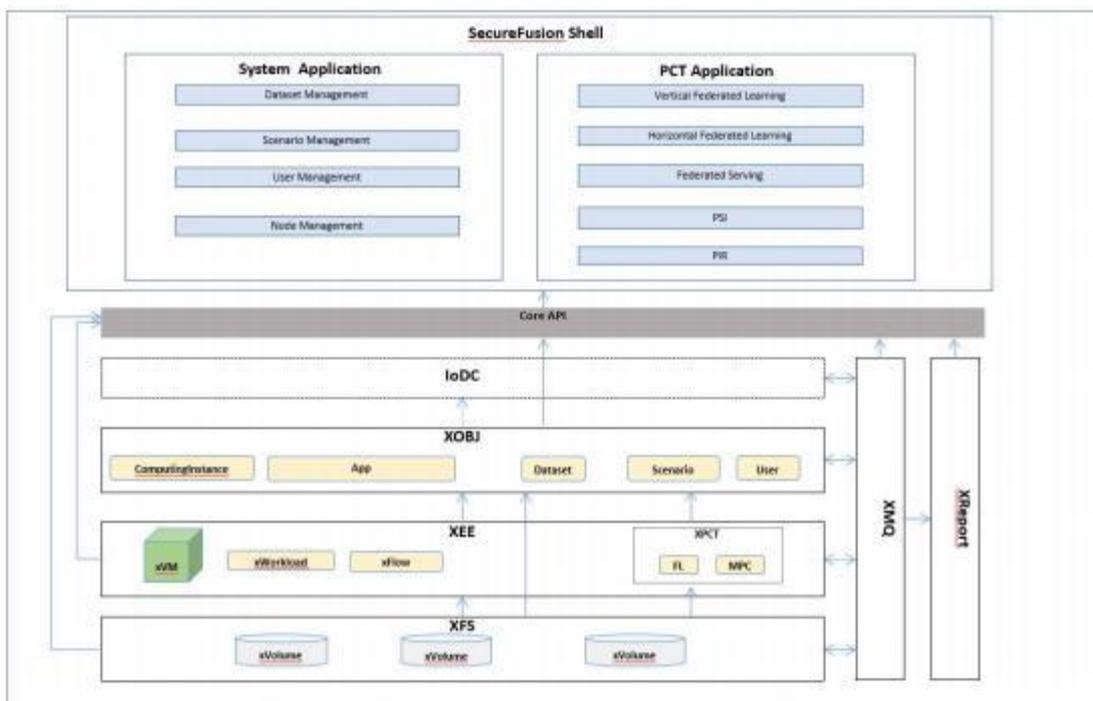
为了让您更好地理解和使用 Secure Fusion 平台，这里介绍了一些基础概念：

概念	解释
PCT	PCT(Privacy computing techniques, 隐私计算技术) 是用于在数据处理或共享过程中保护个人可识别信息 (PII) 并确保隐私的方法。在当前以数据为驱动的世界中，数据必须被共享和分析以改善生活的不同领域，但隐私必须得到保护，因此这些技术非常重要。典型的技术包括联邦学习 (FL)、多方安全计算 (MPC)、可信执行环境 (TEE) 等。
FL	FL(Federated learning, 联邦学习)是一种机器学习技术，它通过在持有本地数据样本的多个分散的边缘设备或服务器中训练算法，而不需要进行数据交换。
XFL	XFL (XDP Federated Learning) 是由 Basebit 开发的联邦学习框架。
MPC	MPC (Multi-Party Computation, 多方安全计算) 是一种增强隐私保护的技术，它允许多个参与方基于他们私有的输入共同计算一个函数，而不向彼此或任何外部方透露有关其输入的任何信息。
XSCE	XSCE(XDP Secure Computing Engine) 是由 Basebit 开发的多方安全计算框架。
TEE	TEE(Trusted Execution Environment, 可信执行环境) 是计算机硬件中的安全区域，确保敏感数据和进程受到未经授权的访问或篡改的保护。
Broker	联盟代理是一种工具，它在联盟体系结构中促进分布式系统之间的通信。它位于不同组织的系统之间，并管理它们之间数据的交换。
节点	节点是指联盟中的一个实体，它可以是 SecureFusion 或其他遵循 IoDC 协议的

	平台。
联盟	联盟一般指一组或多个单独实体（节点），它们以某种方式协同工作。
IoDC	IoDC (Internet of Data and Computing, 数据和计算互联网) 是由 Basebit 运营的联盟，旨在释放数据价值。
场景	场景是节点与其他联盟节点合作的授权基础。它是由发起方/参与方、数据集、应用程序和算力资源组合而成的一组集合。
发起方	发起方是创建场景的人。
参与方	参与方是参与某个发起方创建的场景的节点。

2.3. 平台架构

DSF 采用 Basebit Core&Shell 架构。XCore 是一组松散耦合的云原生服务和组件，旨在为开发人员提供基本的、可定制的隐私计算能力。Core 可以使用 IoDC 协议和实现在 IoDC 网络中不同节点和用户之间进行通信，实现网络范围内的安全数据协作和计算。



3. 功能介绍

3.1. 注册

目前，Secure Fusion 不允许用户随机注册。您需要联系公司/组织管理员以获得注册的邀请码。平台管理员将在开始部署平台时进行设置。



The screenshot shows the registration interface for XDP SecureFusion. At the top, it displays the logo and the text 'SecureFusion 隐私计算平台'. Below this, there is a section titled '注册账号' (Register Account). The form includes several input fields: '用户名' (Username), '邮箱地址' (Email Address), '8-20位密码, 区分大小写' (8-20 character password, case-sensitive), and '请再次输入密码' (Please re-enter password). There is also a field for '输入邀请码' (Enter invitation code). A checkbox labeled '我已阅读并同意' (I have read and agree) is present, with a link '使用条款' (Terms of Use) next to it. A large blue button labeled '注册' (Register) is at the bottom, with a link '使用已有账号登录' (Use existing account to log in) below it.

3.2. 登陆

一旦您成功在平台注册，您可以使用您的用户名和密码登录。如果您忘记了密码，您需要联系平台管理员帮助您重置密码。



The screenshot shows the login interface for XDP SecureFusion. At the top, it displays the logo and the text 'SecureFusion 隐私计算平台'. Below this, there is a section titled '账户密码登录' (Account Password Login). The form includes two input fields: '用户名' (Username) and '密码' (Password). There is a link '忘记密码?' (Forgot password?) next to the password field. A large blue button labeled '登录' (Login) is at the bottom, with a link '注册账号' (Register account) below it.

3.3. 首页

平台首页展示了关于场景、任务、数据集、服务等统计信息，您可以直观地了解到您在平台上的使用概况。

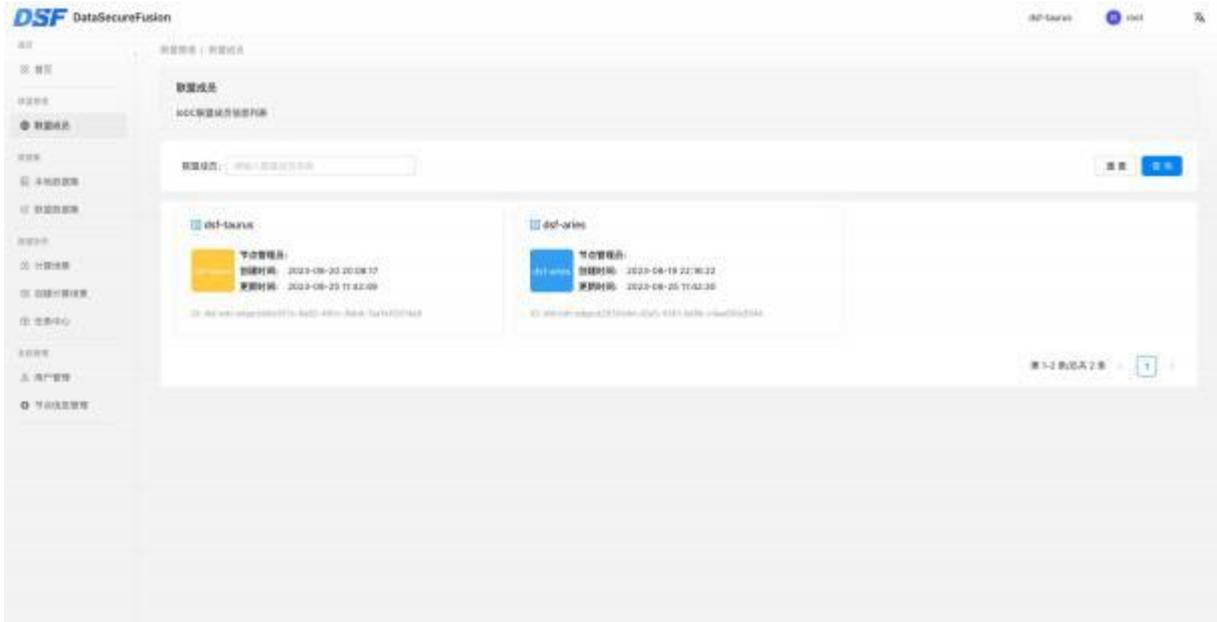


3.4. 联盟管理

Secure Fusion (SF) 最强大的功能之一是在不传输原始数据的情况下执行数据协作。这是由我们自己开发的多方计算 (MPC) 和联邦学习 (FL) 算法保障的。要与其他 SF 节点进行 MPC 或 FL，第一步是参与的 SF 节点需要加入同一个 SF 联盟。

联盟成员

要查看联盟中的节点，请前往导航栏上“联盟管理”下的“联盟成员”。在这里，您可以看到与您在同一联盟中的其他 SF 节点。

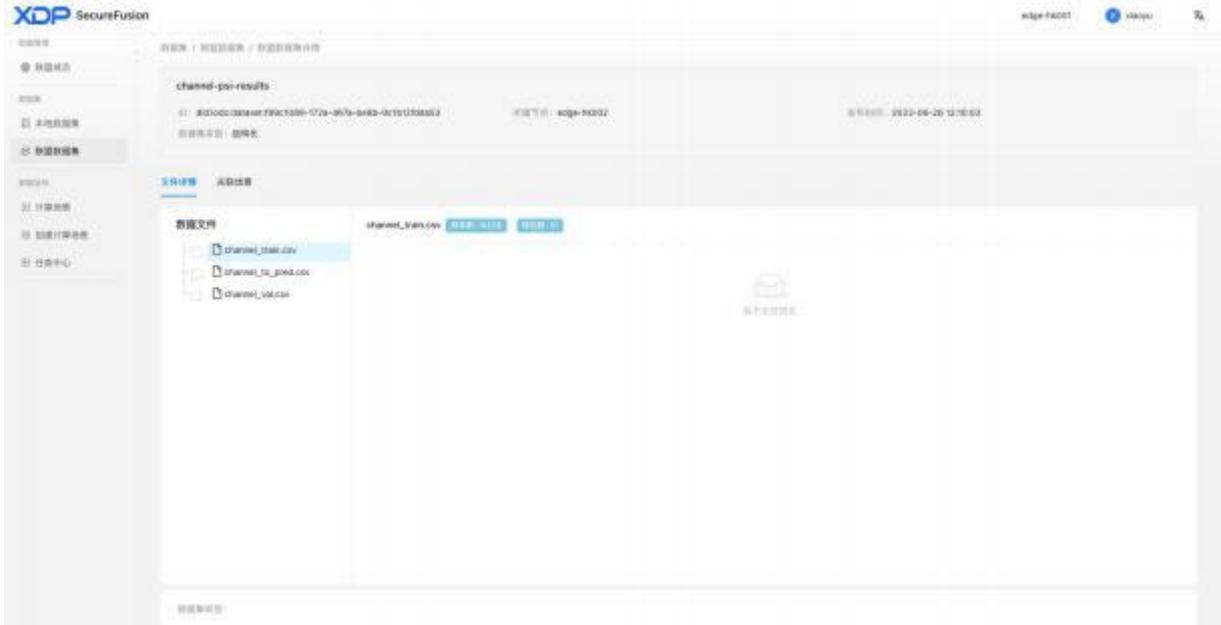


数据集

如果单击联盟中的任何 SF 节点，就可以看到他们向联盟发布了哪些数据集。如果需要使用这些数据集，需要创建计算场景并申请使用权限。请参考数据协作章节。



如果您点击“查看”进入数据集，您将注意到您无法预览该数据集的内容。请注意，SF 不允许您查看/预览任何其他 SF 节点的原始数据。

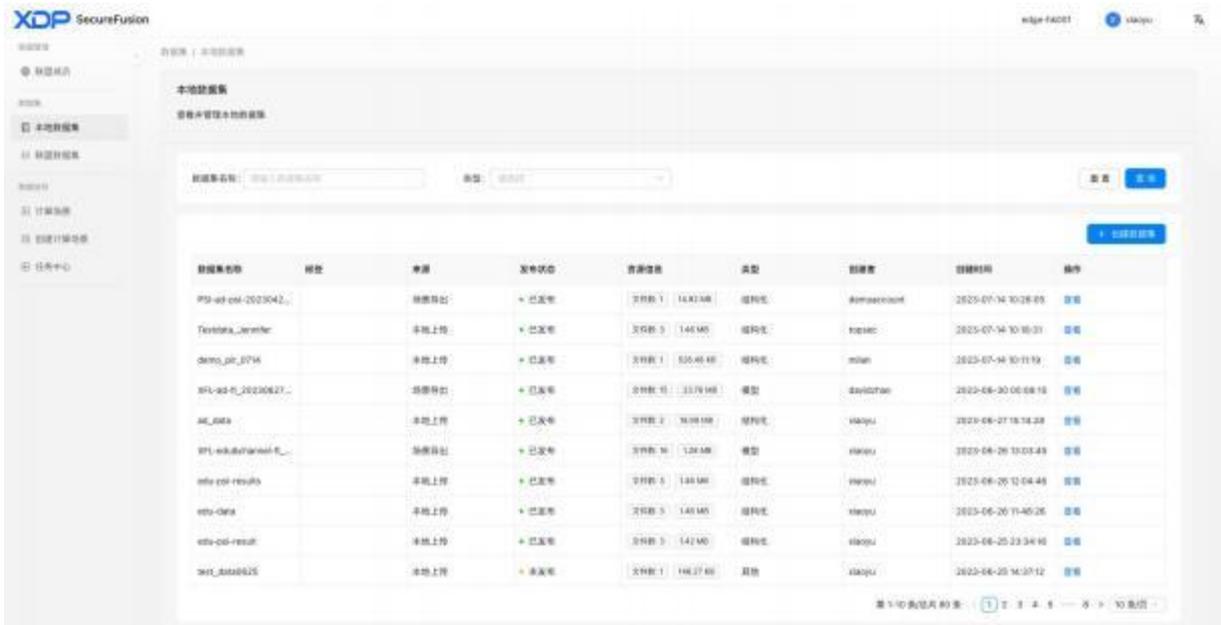


3.5. 数据集

3.5.1. 创建数据集

要与其他公司/组织进行数据协作，第一步是创建您的数据集。

在左侧导航栏上，点击“数据集”下的“本地数据集”。在这里，您可以看到您和您的公司/组织成员创建的所有数据集。数据集列表的每一行代表一个数据集及其基本信息。



数据集名称

标签：标签允许用户通过过滤器更容易地找到数据集。

来源：来源表明了数据集是来自用户上传还是来自计算场景的输出。

 发布状态：发布状态表明了数据集是否被发布到 IoDC，并且可以被来自联盟中其他 SF 节点的用户发现。

 资源信息：数据集的大小和文件的数量。

 类型：类型表明了数据集是模型、分层文件夹中的文件还是其他。

 创建者

 创建时间

 操作：您可以点击“查看”查看数据集的更多详细信息并对其进行修改。

创建数据集

要创建自己的数据集，请单击“+ 创建数据集”按钮。

您需要填写以下信息：

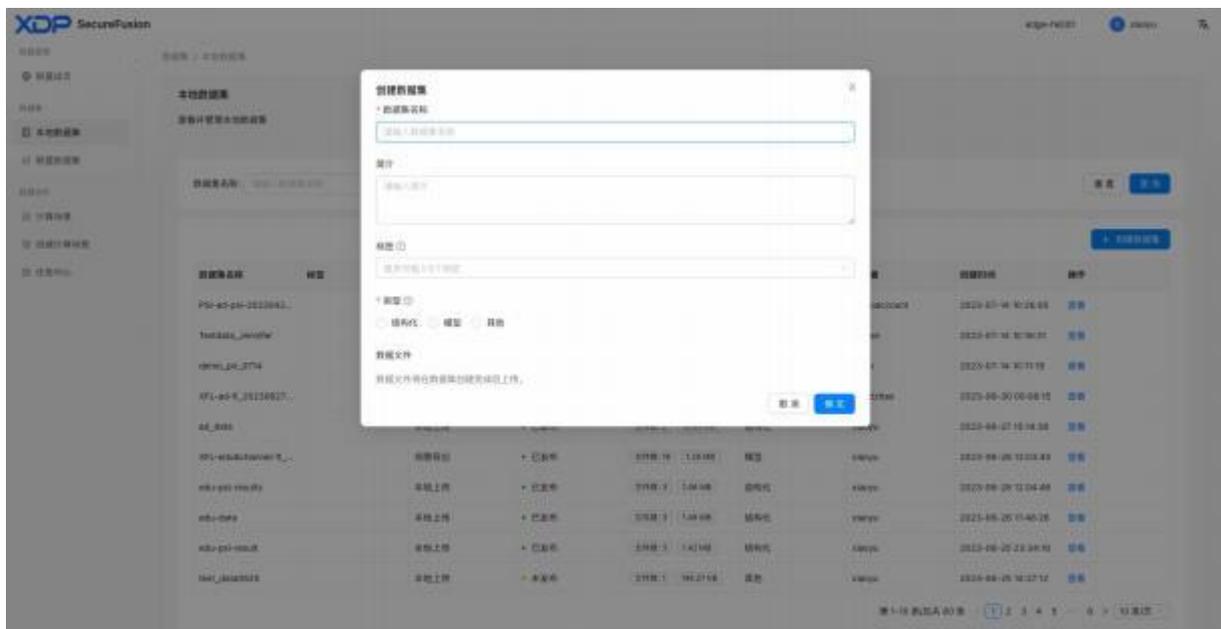
 数据集名称

 简介：数据集是用来干什么的？如何使用这个数据集？

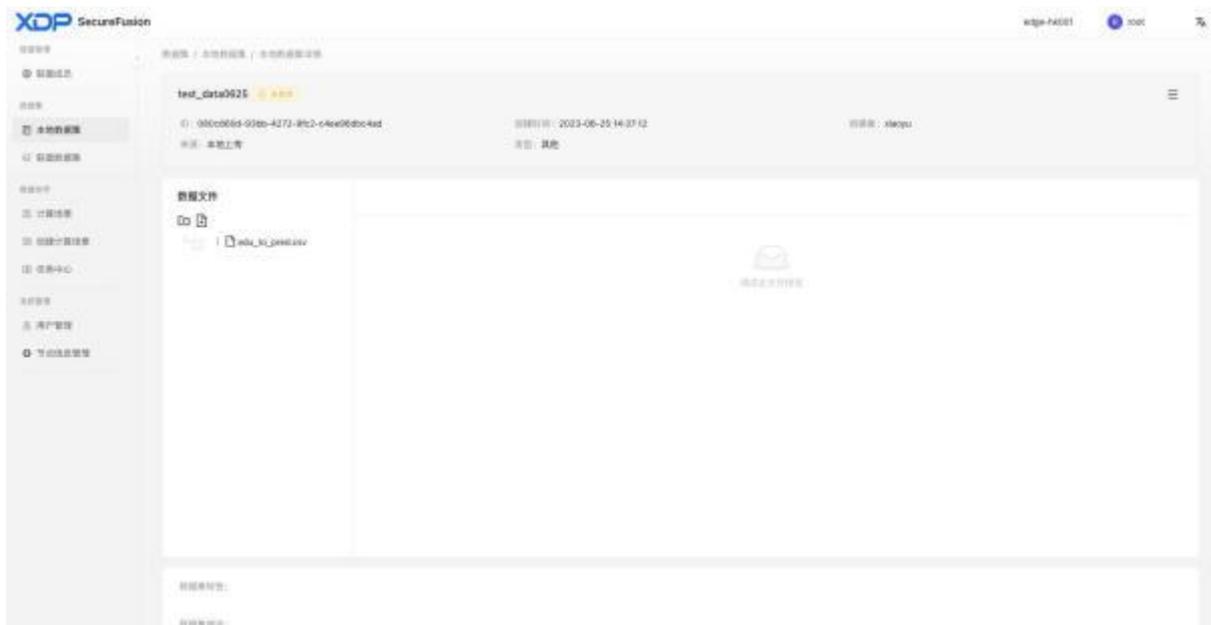
 标签

 类型

填写完这些信息后，单击“确定”按钮创建数据集。现在您可以看到刚才创建的数据集显示在列表中。下一步是向数据集中添加数据。单击“查看”进入数据集。



您可以通过单击文件夹图标在根目录下创建一个文件夹，也可以通过单击文件图标将文件上传到根目录。

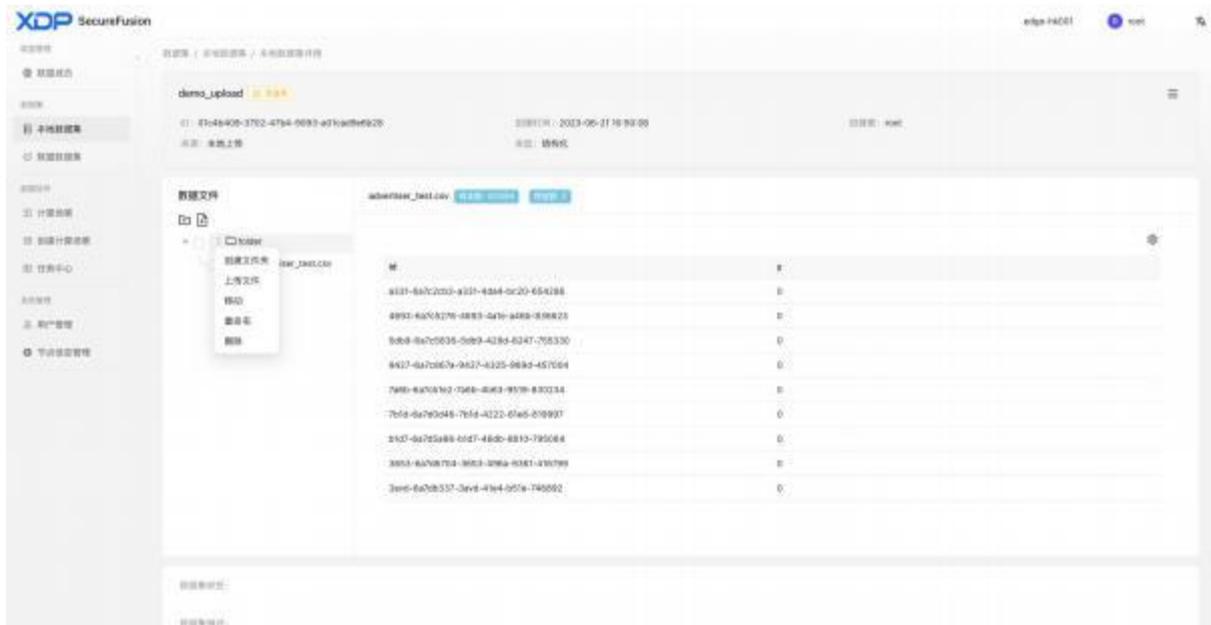


如果你想创建另一个文件夹或在文件夹下上传文件，点击旁边有“3点”的图标。您可以对它执行以下操作：

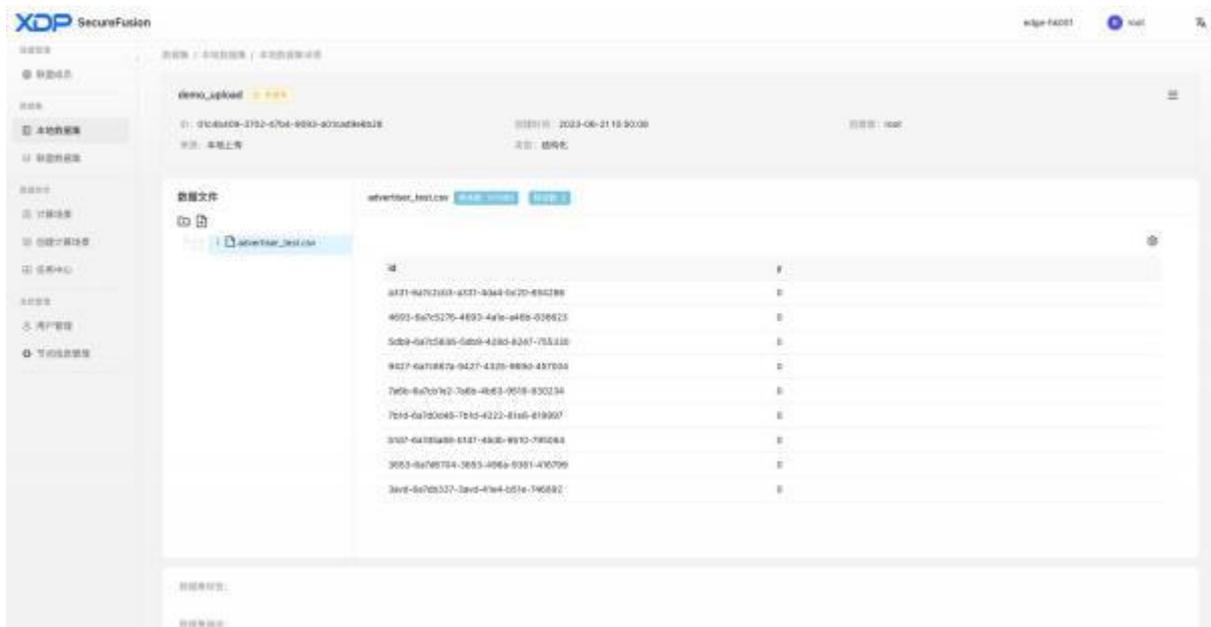
-  在当前文件夹下创建另一个文件夹
-  在文件夹下上传文件
-  将文件夹移动到其他目录
-  重命名文件夹
-  删除文件夹

点击文件的“3点”图标，可以执行以下操作：

-  将文件移动到其他目录
-  重命名文件
-  删除文件



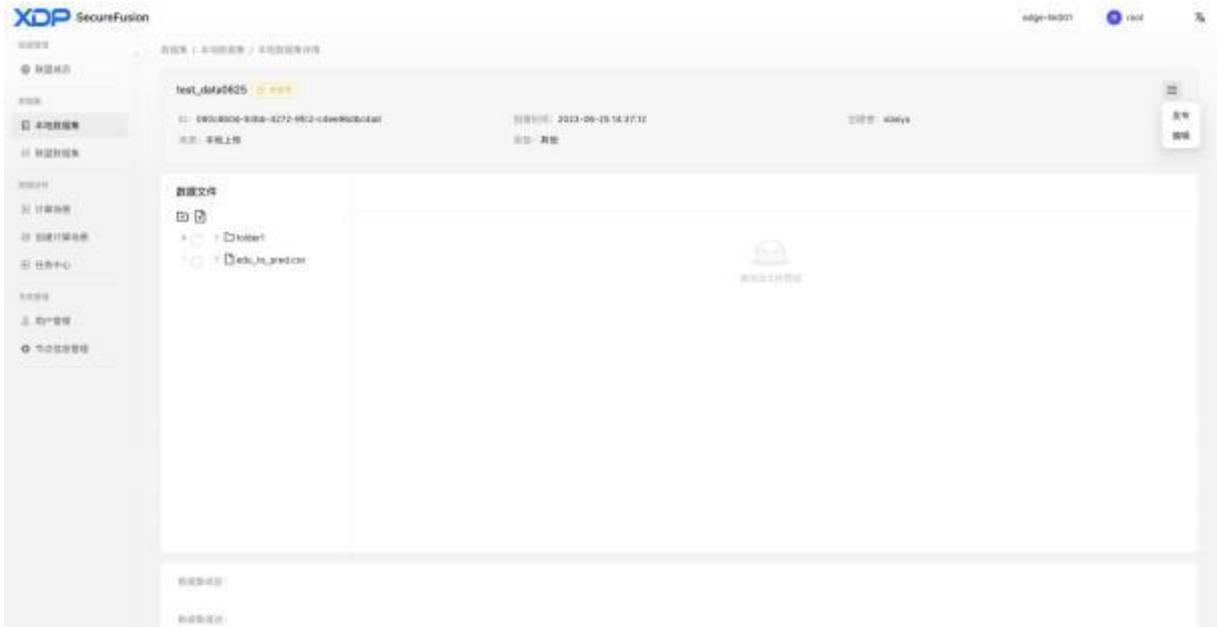
该平台支持预览 csv 文件，因此您不必只是为了查看文件内部的内容而下载文件。



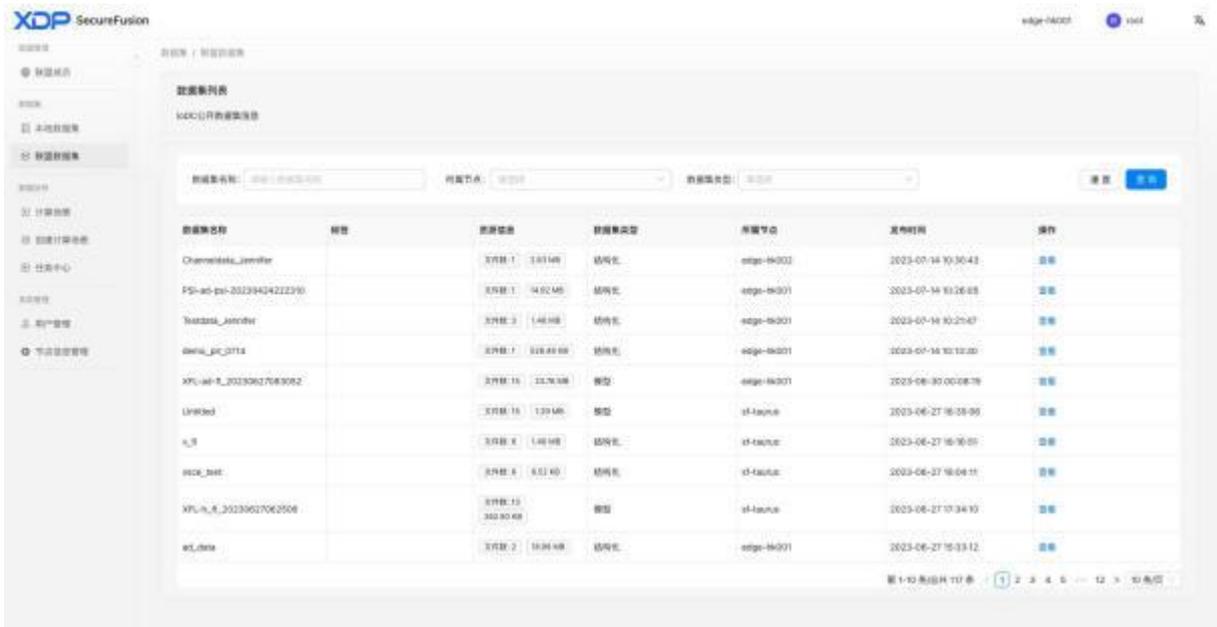
3.5.2.发布数据集

如果希望与联盟中的其他 Secure Fusion 节点进行数据协作，则需要将数据集发布到联盟，以便来自其他节点的用户可以发现您的数据集。

点击右上角的菜单，点击“发布”。注意，一旦数据集发布到联盟，就不能再修改它了。



数据集发布后，您可以前往左侧导航栏上的“联盟数据集”。在这里，您可以看到联盟中所有 Secure Fusion 节点发布的所有数据集，包括您刚刚发布的数据集。



如果您点击“查看”以查看来自联盟的任何数据集的更多详细信息，您将注意到所有文件都不可预览。如果希望使用来自联盟的数据集，则需要创建计算场景，并使用平台提供的多方安全计算或联邦学习技术处理数据。

3.6. 数据协作

3.6.1. 计算场景

为了与联盟的其他 Secure Fusion 节点进行数据协作，您需要创建一个计算场景。

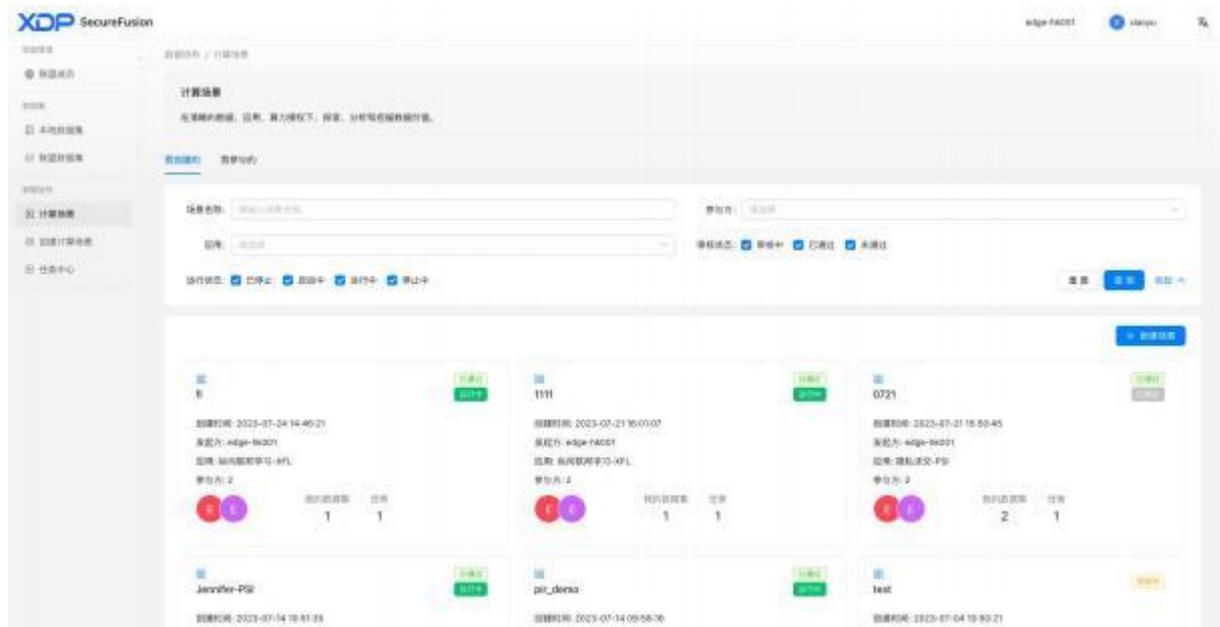
计算场景包括数据协作的以下信息：

- 👉 谁是参与者？
- 👉 使用什么应用程序/计算方法？
- 👉 MPC: PSI, PIR, 专家记分卡等
- 👉 FL: 纵向 FL, 横向 FL, XGBoost 等
- 👉 参与者的哪些数据集将被处理？
- 👉 此任务将使用哪些计算资源？

换句话说，计算场景指定谁将使用哪个数据集来做什么。一旦创建了计算场景，所有参与者将收到通知，并被要求审查该场景。只有当所有参与者都同意可以执行计算场景时，执行者才能运行应用程序并获得输出。

3.6.1.1. 创建场景

要创建计算场景，请在导航栏上选择“计算场景”。在这里，您将看到您公司/组织所有计算场景的列表。点击“新建场景”按钮创建一个新的计算场景。



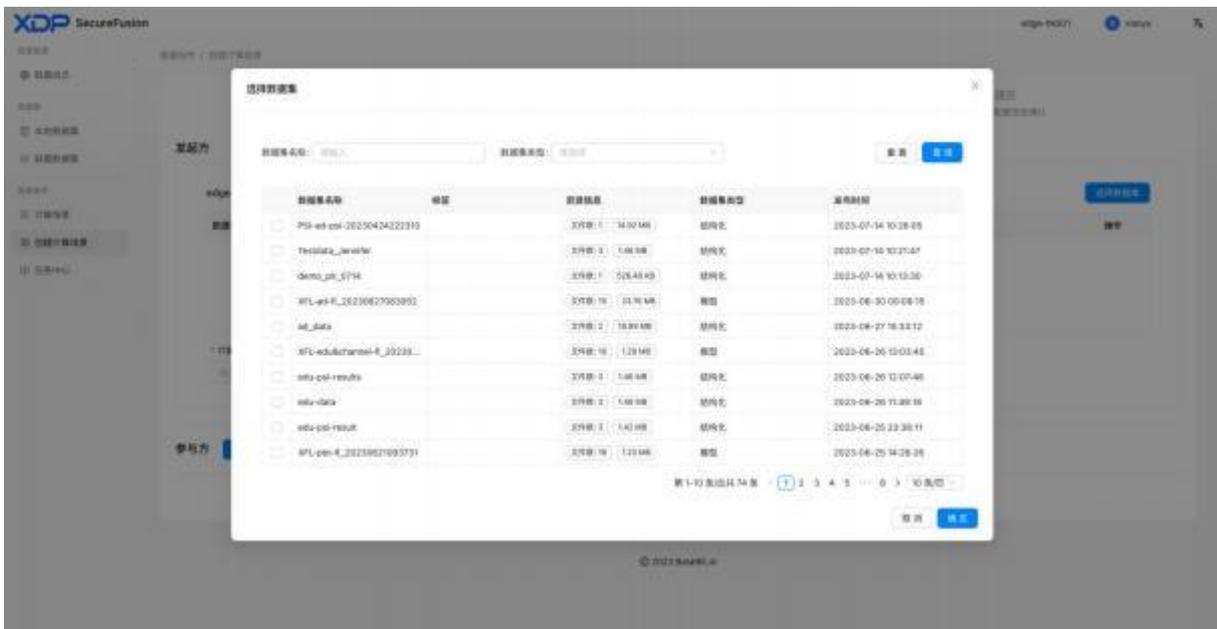
然后您需要为这个场景选择一种计算方法，即所谓的“应用”。这一步指定了您将如何处理数据以及您的计算目的。有关每个应用的更多详细信息，请参阅应用章节。



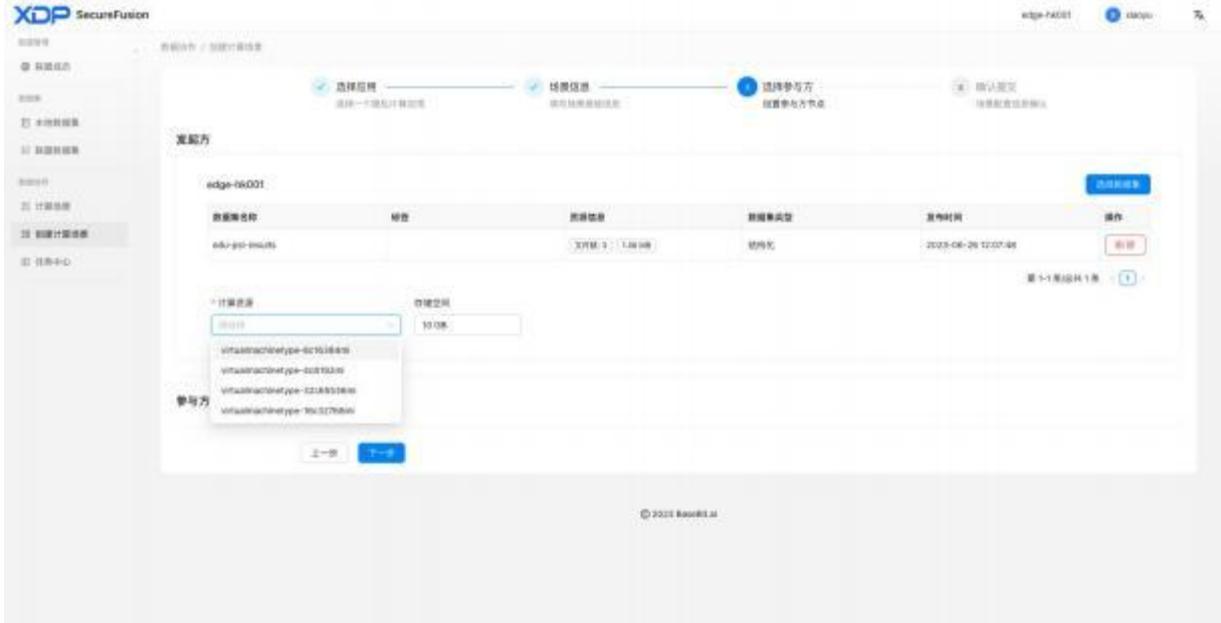
接下来，您必须为这个场景指定一个名称。您可以选择是否填写场景的描述，并根据需要为该场景添加一个标签。也就是说，你提供给参与者的信息越多，你的方案就越容易得到他们的认可。



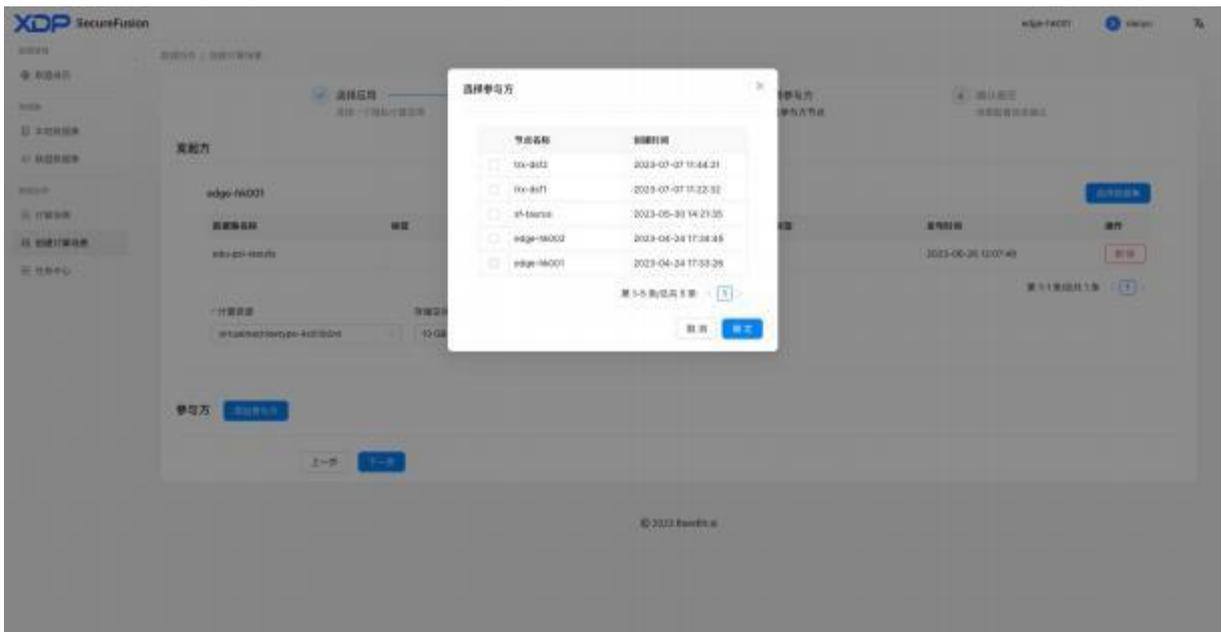
下一步是指定场景参与方和输入数据集。首先，您需要点击“选择数据集”按钮并从您的节点选择输入数据集。



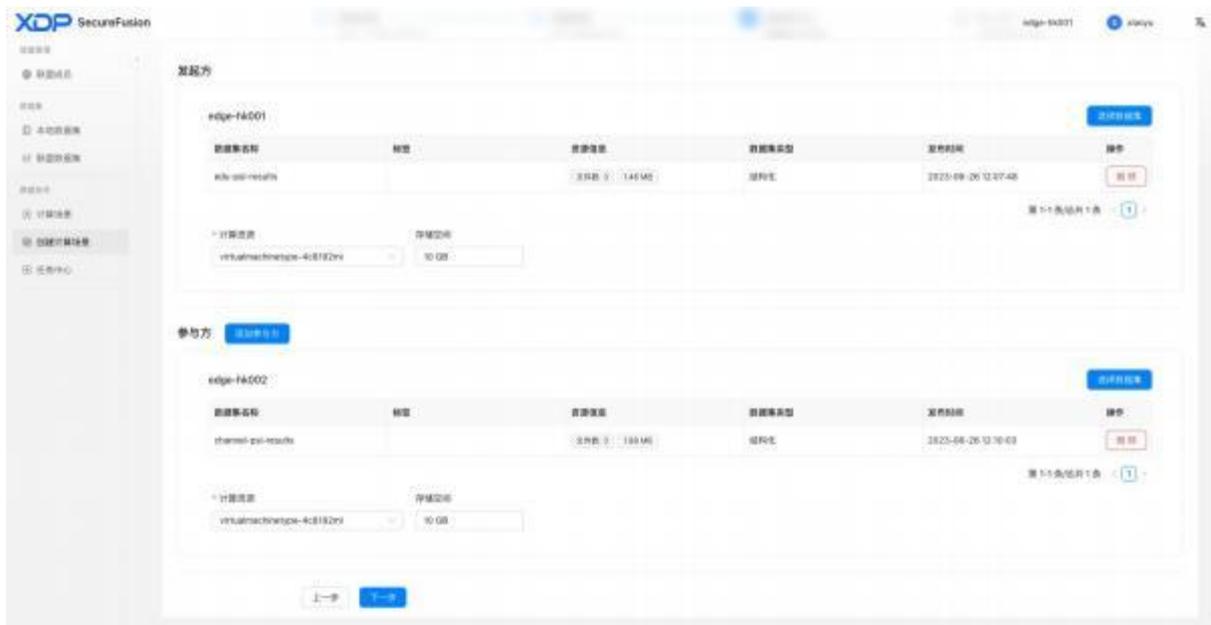
其次，您需要配置您的节点的计算资源。



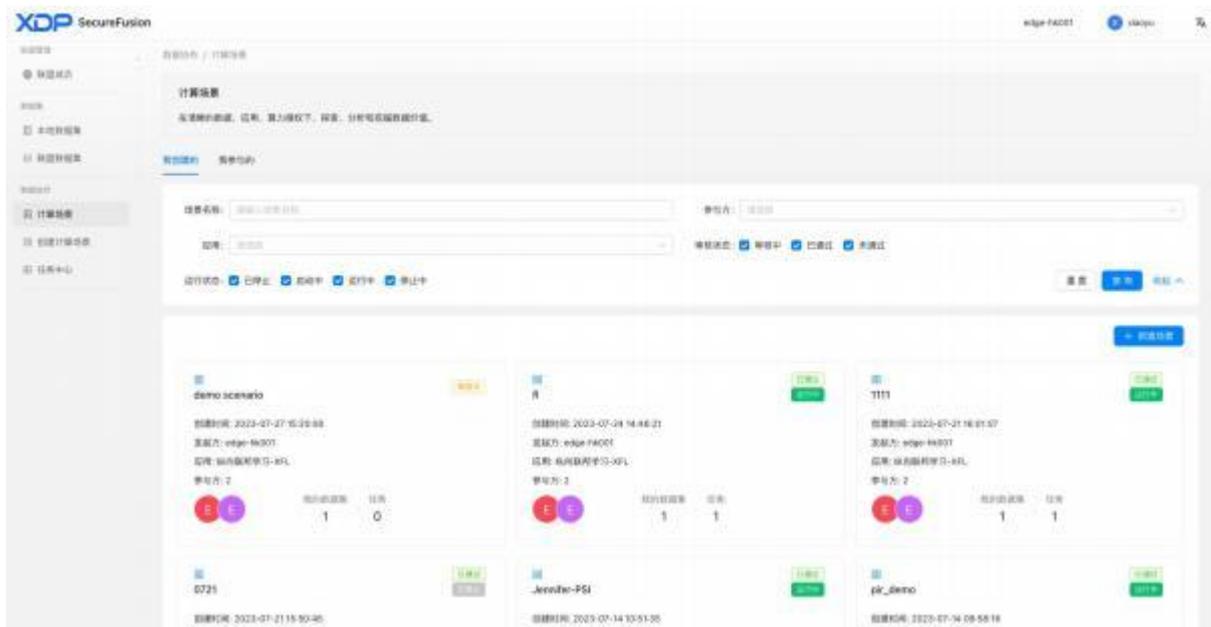
然后，您需要通过单击“添加参与方”按钮向此场景添加参与者。将有一个弹出窗口显示所有在您联盟中的 Secure Fusion 节点，请选择要与之协作的节点。请注意，如果您想从场景中删除参与者，您需要单击“添加参与方”按钮并从列表中取消选择该参与者。



最后，为每个参与节点选择输入数据集和计算资源。一旦一切都配置好了，单击“下一步”按钮继续并提交此场景以供审批。

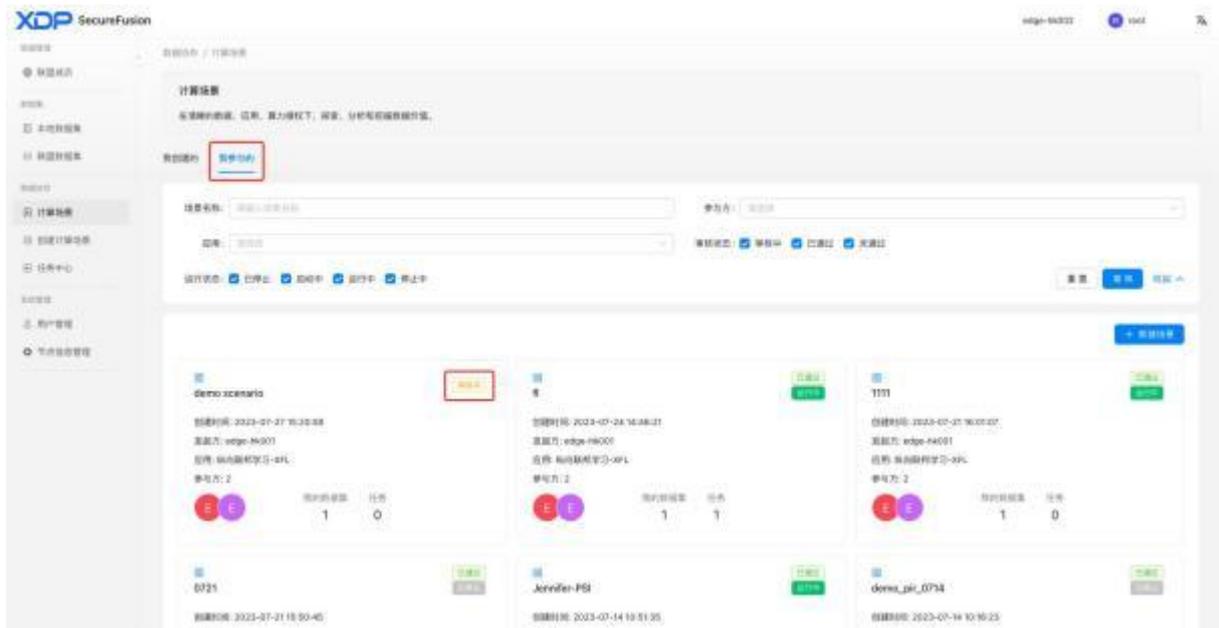


在所有参与方都批准之前，场景状态将为“审核中”，无法执行。

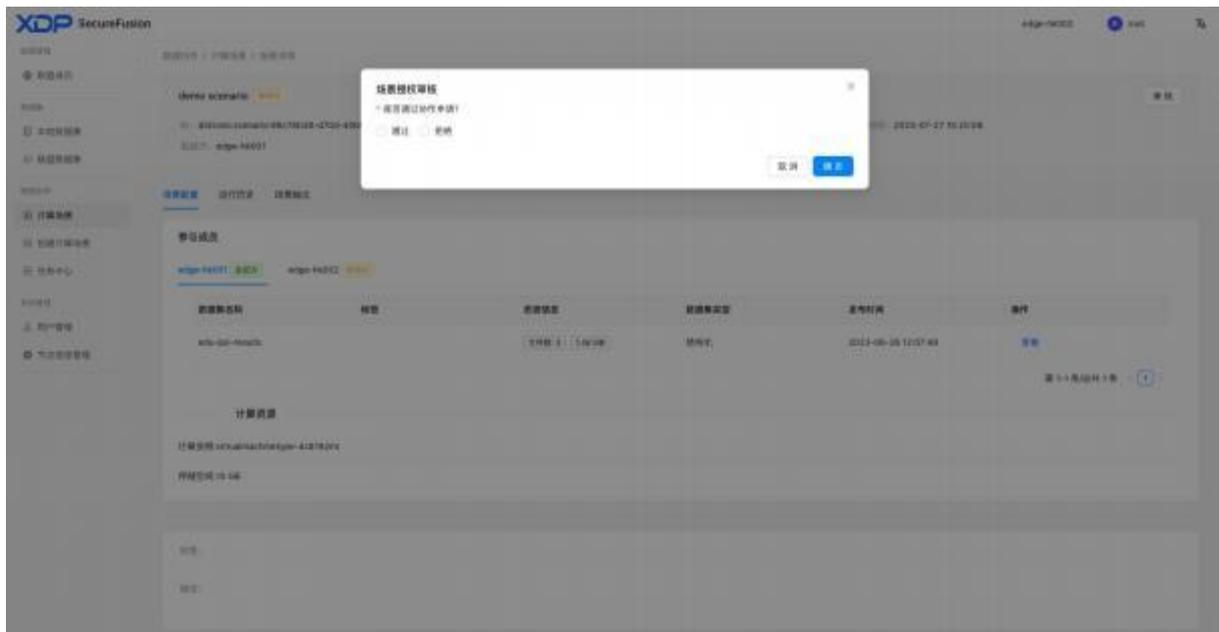


3.6.1.2. 场景授权

如果来自其他节点的用户希望在计算场景中使用您的数据，则需要您同意授权然后他们才能够开始执行该场景。要授权一个场景，请进入“数据协作”下的“计算场景”，然后点击“我参与的”。



进入场景并单击“审核”按钮。你可以决定批准或拒绝。一旦您批准了它，场景就可以执行了。



3.6.2.应用

3.6.2.1. 联邦学习

联邦学习是一种机器学习技术，它支持在分散的数据源上训练模型，而不需要将数据传输到中心位置。在联邦学习中，数据保留在本地设备上，模型训练在设备或本地服务器上进行。

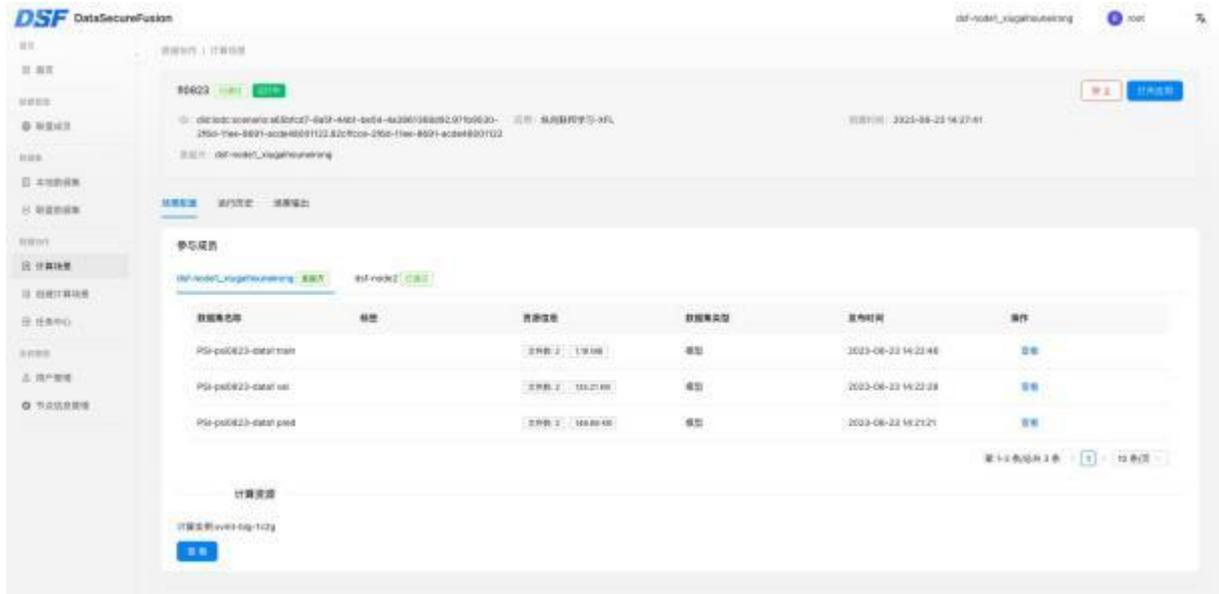
联邦学习背后的思想是允许多个设备或节点参与模型训练过程，而不需要将数据转移到中央服务器。这种方法有助于解决与汇集敏感数据相关的隐私和安全问题。

联邦学习在数据分布在多个节点的情况下特别有用。参与方们可以部署他们自己的 Secure

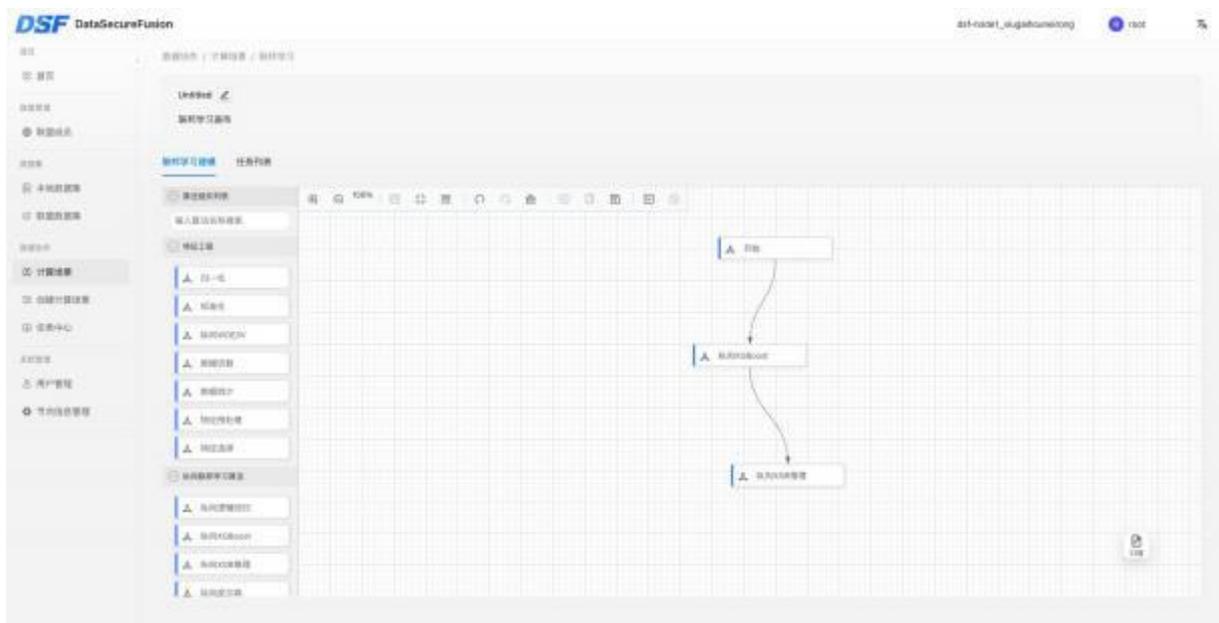
Fusion 节点，并使用 Secure Fusion 提供的联邦学习技术一起训练他们的模型。

Secure Fusion 的联邦学习

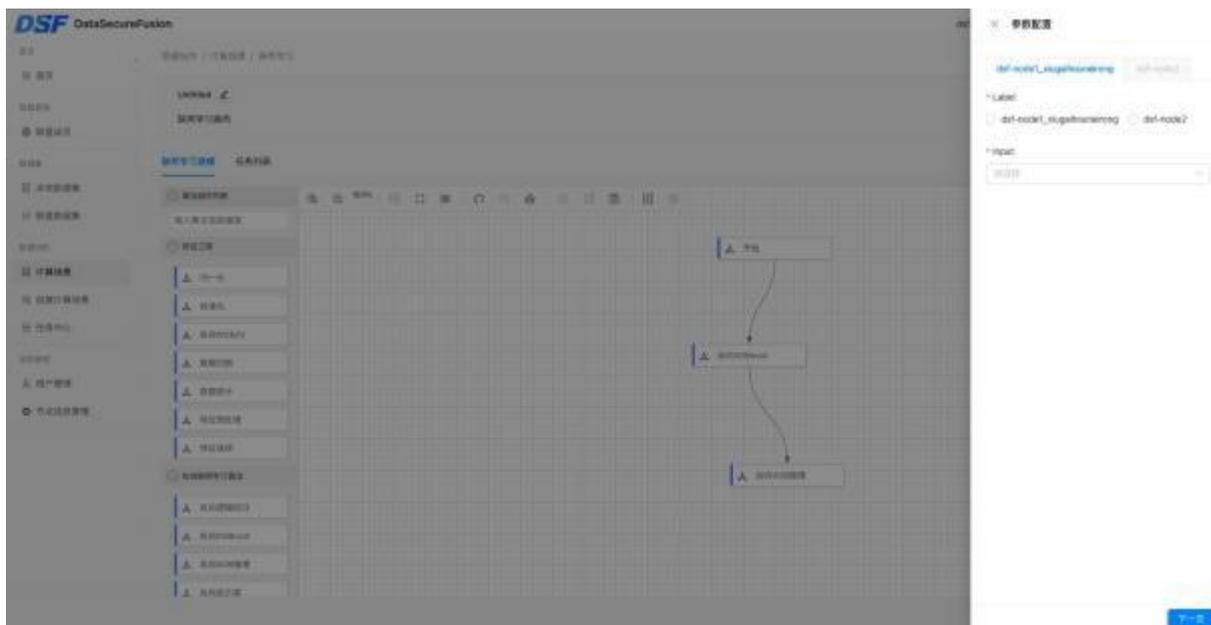
在创建场景时，选择联邦学习应用。创建场景后，进入场景并点击“打开应用”按钮。



您需要通过拖动左边的卡片来创建自己的工作流。例如，如果你想通过纵向联邦学习开发一个 AI 模型，您可能需要将“归一化”和“纵向 XGBoost”拖到您的工作流程中。然后您需要在每张卡片之间画一条线来完成工作流程。



一旦工作流被创建，下一步是为每个步骤配置输入。从开始开始，您需要为节点分配标签，并为两个节点选择输入文件。注意，如果您的工作流中有“归一化”或“标准化”，输出文件的名称中将添加文本“normalized_”/“standardized_”。因此，当您在联邦学习的步骤中选择输入时，您需要选择名称以“normalized_”/“standardized_”开头的文件。



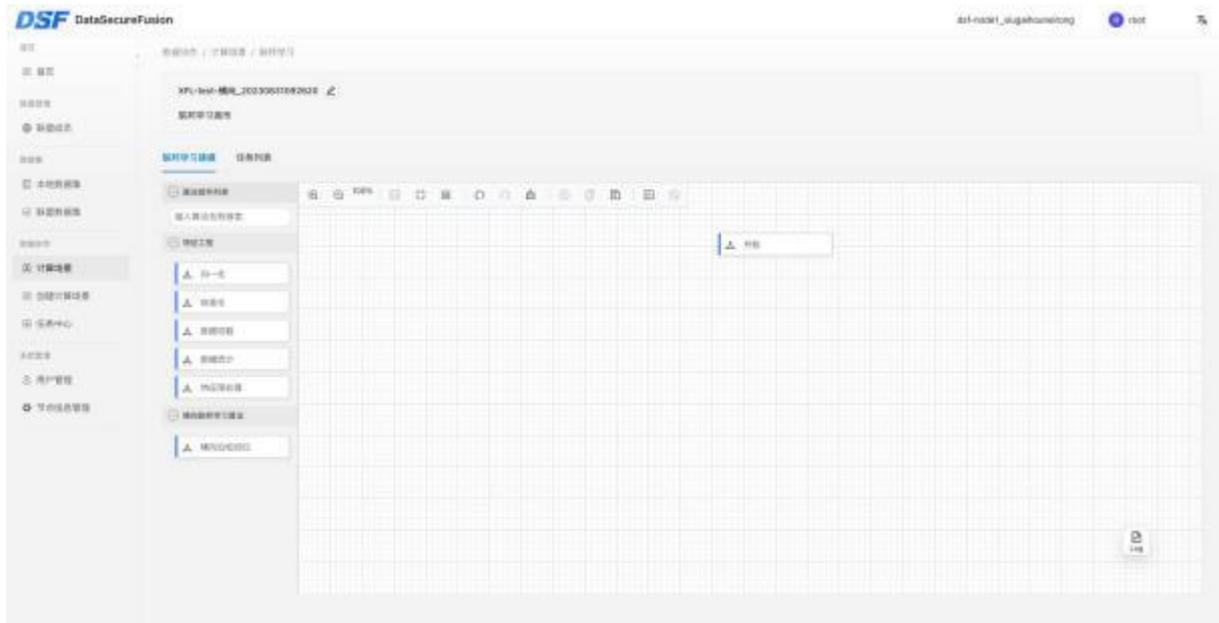
配置完成后，可以启动实例并开始训练模型。如果你不知道如何创建自己的工作流，你可以联系我们的团队，我们有专业的工程师来帮助你建立自己的人工智能模型。

横向联邦学习

横向联邦学习是联邦学习的一种，多个参与方在各自的本地数据集上联合训练机器学习模型而不共享原始数据。在横向联邦学习中，每一方都有相同类型的数据，但数据分布在多个位置。通过使用横向联邦学习，用户们可以协同训练机器学习模型，而无需与彼此或中央服务器共享他们的个人数据。

在横向联邦学习中，每一方使用自己的数据训练一个本地模型，并且只与其他各方共享模型参数的一小部分。然后将该部分与其他各方的参数结合起来，以创建更健壮的模式。这个过程不断重复，直到模型收敛到最优解。

与传统的机器学习技术相比，横向联邦学习具有几个优势，例如在保护数据隐私和安全性的同时支持协作进行机器学习，减少在中间位置处理大型数据集的计算负担，并允许对分布式数据进行持续学习。它已被用于各种用途，如医疗保健、金融和物联网，以实现协作机器学习，同时保护数据隐私和安全性。

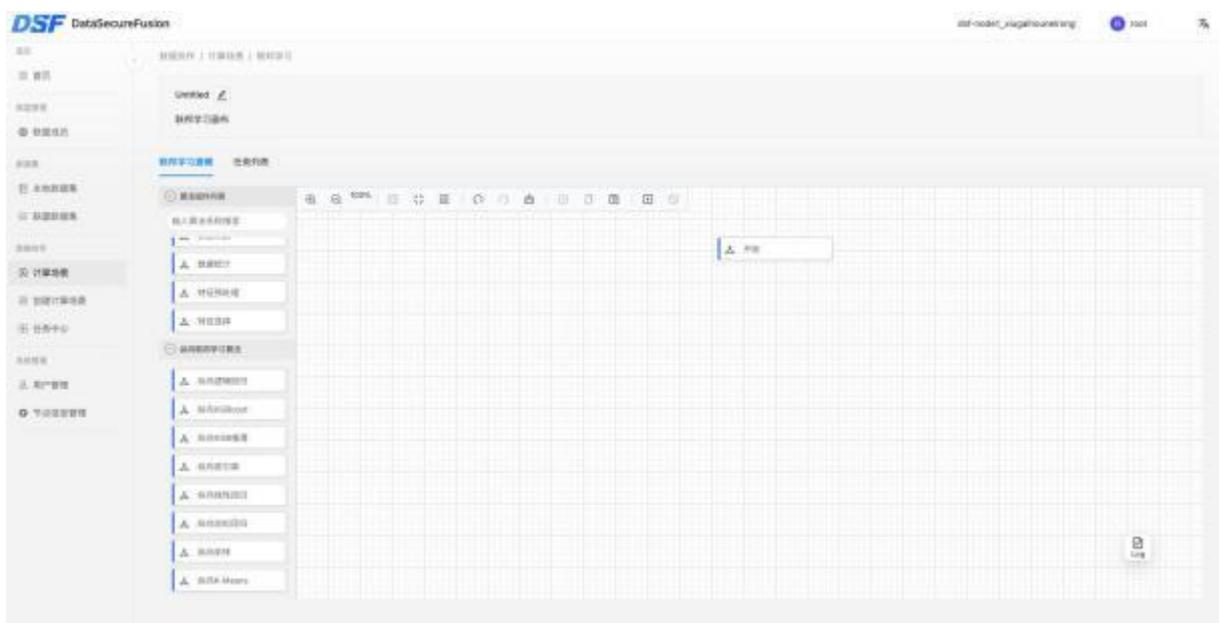
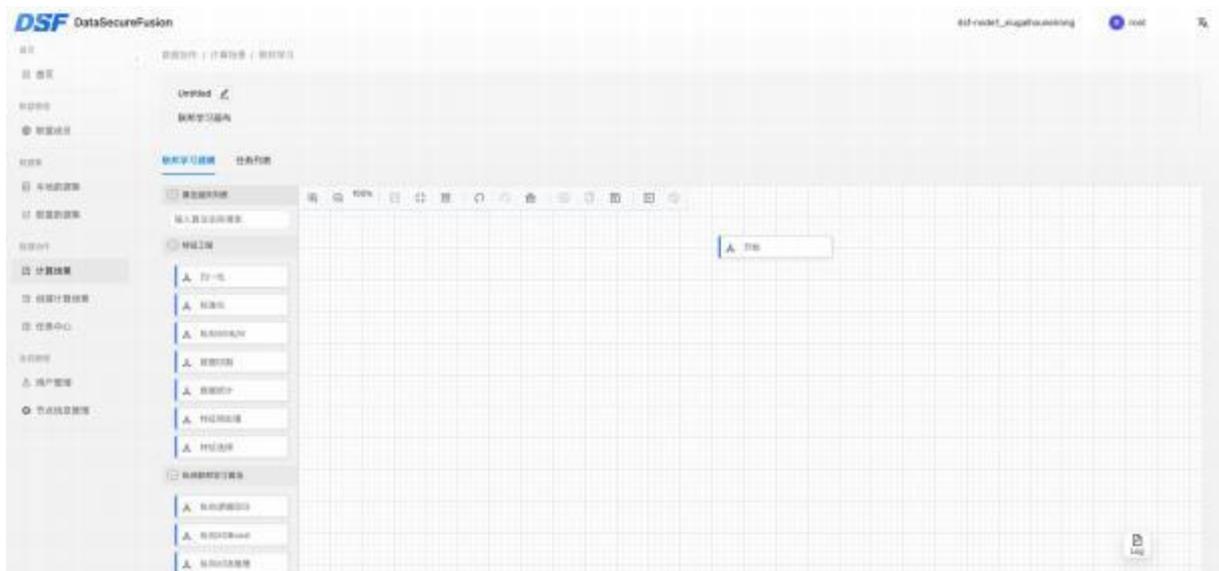


纵向联邦学习

纵向联邦学习是联邦学习的一种，它支持拥有不同类型数据的各方之间的协作。在传统的联邦学习中，多方拥有相同类型的数据，但在纵向联邦学习中，每一方都拥有不同类型的数据，这些数据是相互补充的。通过纵向联邦学习组合这些不同类型的数据，可以创建更准确、更全面的模型，而无需在各方之间共享原始数据。

在纵向联邦学习中，每一方使用自己的数据训练自己的模型，并且只与其他各方共享模型参数的一小部分。然后将该部分与其他各方的参数结合起来，以创建更健壮的模型。这个过程不断重复，直到模型收敛到最优解。

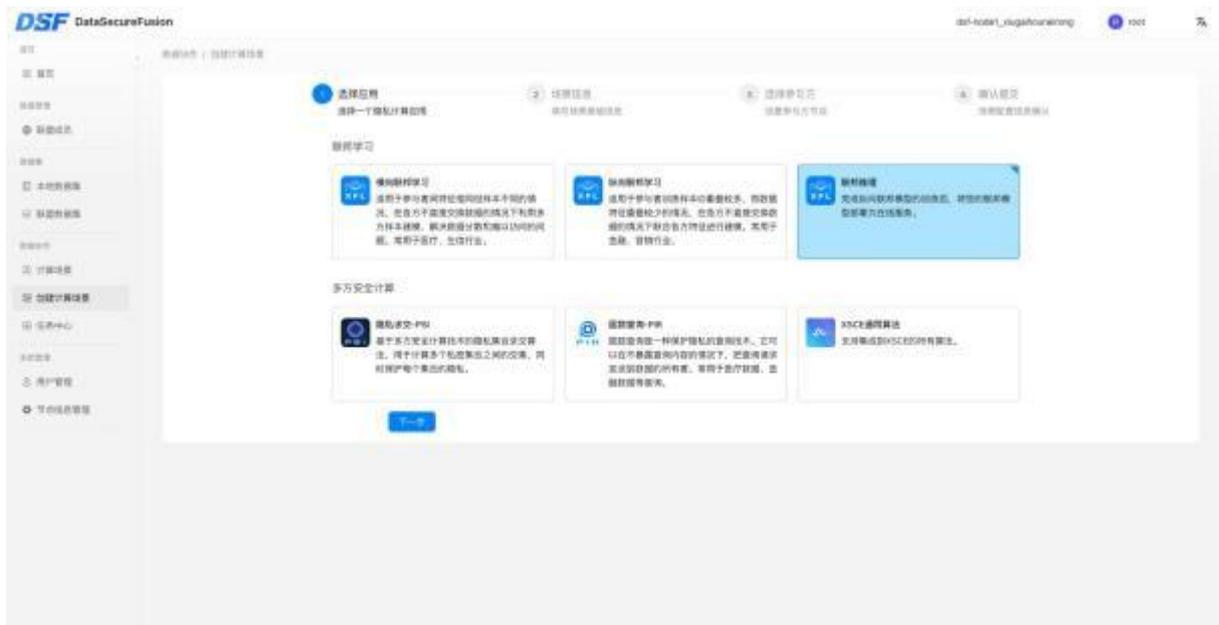
与传统的机器学习技术相比，纵向联邦学习具有几个优势，例如维护数据隐私和安全性、减少数据偏差以及支持具有不同类型数据的各方之间的协作。它已被用于各种用途，如医疗保健、金融、电子商务和政府，以实现协作机器学习，同时保护数据隐私和安全性。



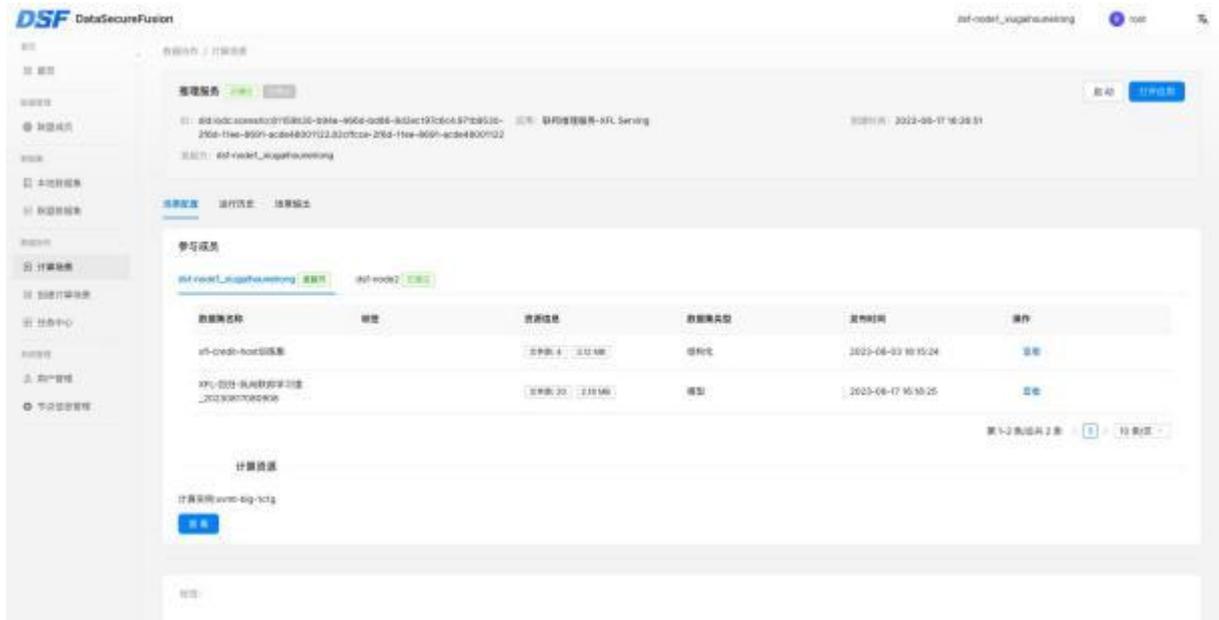
联邦推理

纵向联邦学习模型训练完成后，可以将其部署为在线推理服务。

在创建场景时，选择联邦推理应用。



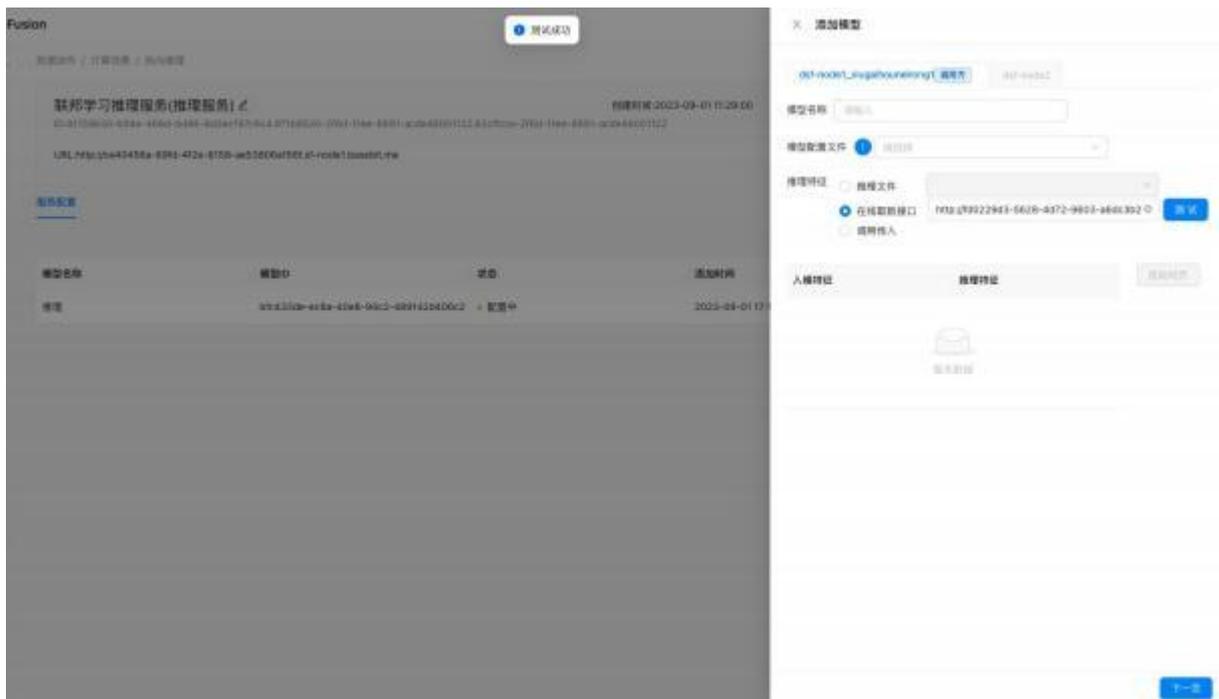
创建场景后，进入场景并点击“打开应用”按钮。

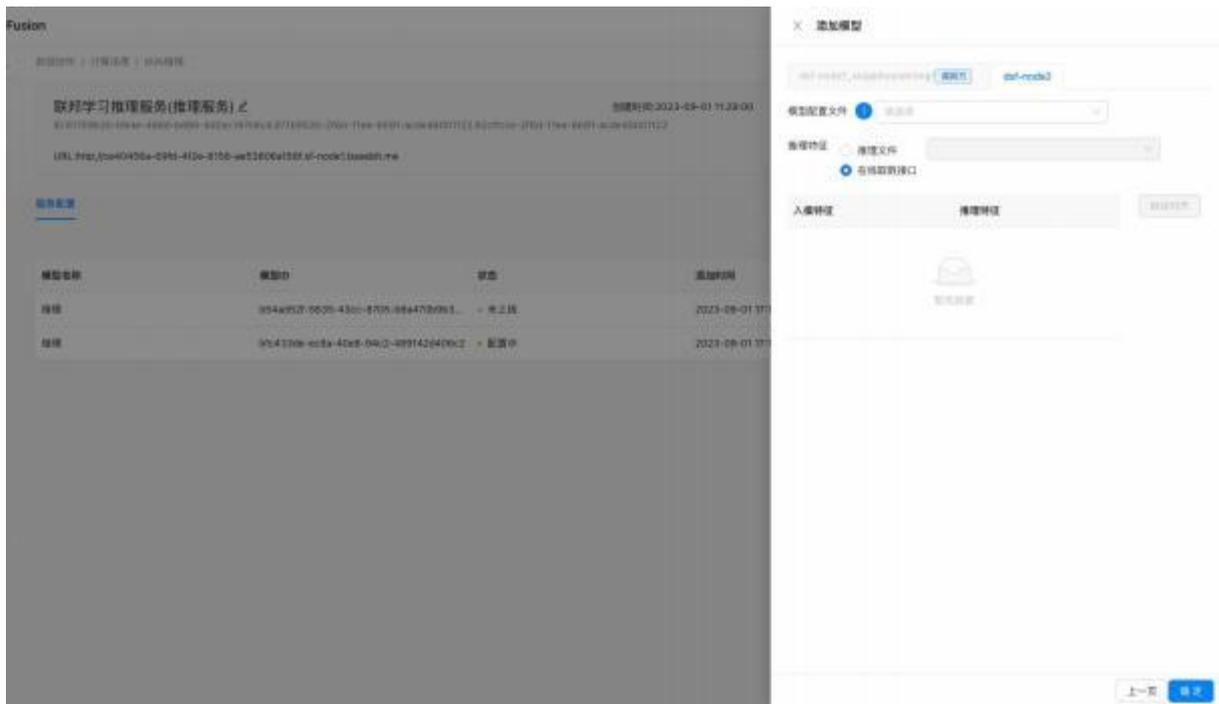


首先需要添加模型，点击“添加模型”。

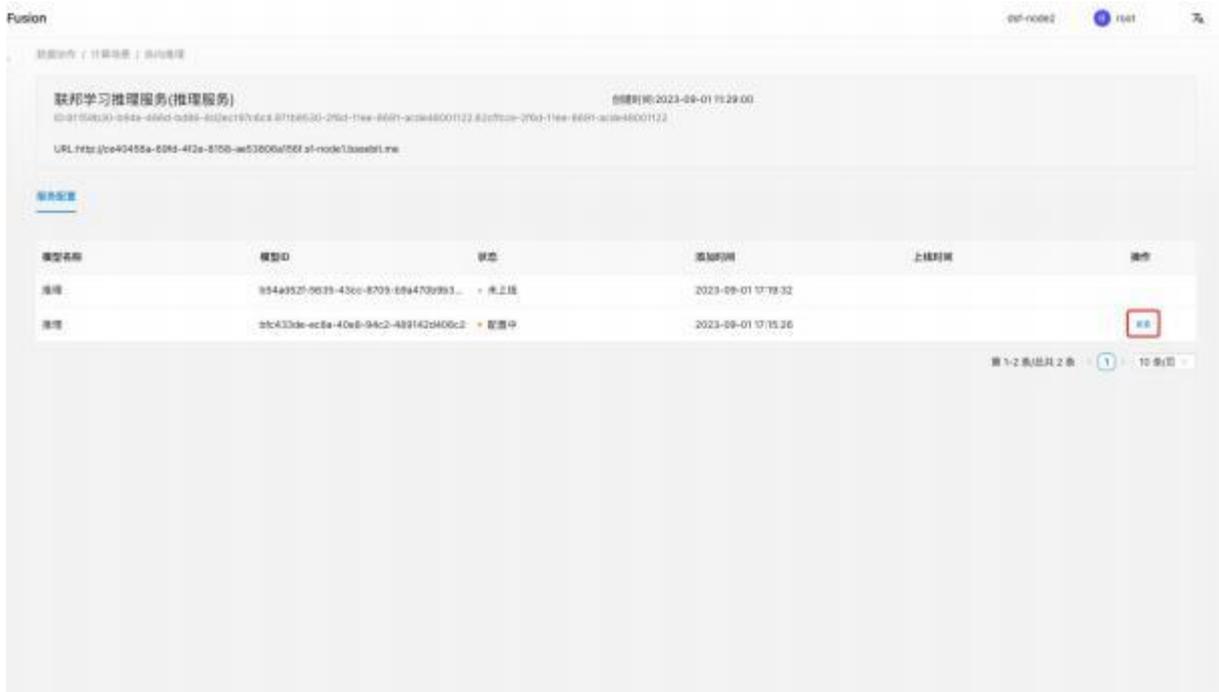


输入模型名称并配置相应的模型配置文件。然后选择输入推理特征的方式，目前支持通过文件输入或者通过在线取数接口输入特征。





如果配置了参与方的特征输入方式为在线取数接口，则参与方需要在平台上进行取数接口的配置，参与方配置完成后，模型才可以上线。



在 PSI 协议中，每一方持有一组数据，并希望找到这些数据集合的交集（即在两个集合中都存在的部分）。然而，他们不想向对方透露他们的整个集合，甚至不想透露他们每个人持有的数据的确切数量。

为了实现这一点，PSI 协议允许双方以一种让他们知道他们的集合之间是否有交集的方式进行交互，如果有交集，哪些部分在交集中。在协议结束时，任何一方都不了解任何关于不在交集的数据的信息，或者关于另一方集合的大小或内容的信息。

Secure Fusion 的 PSI

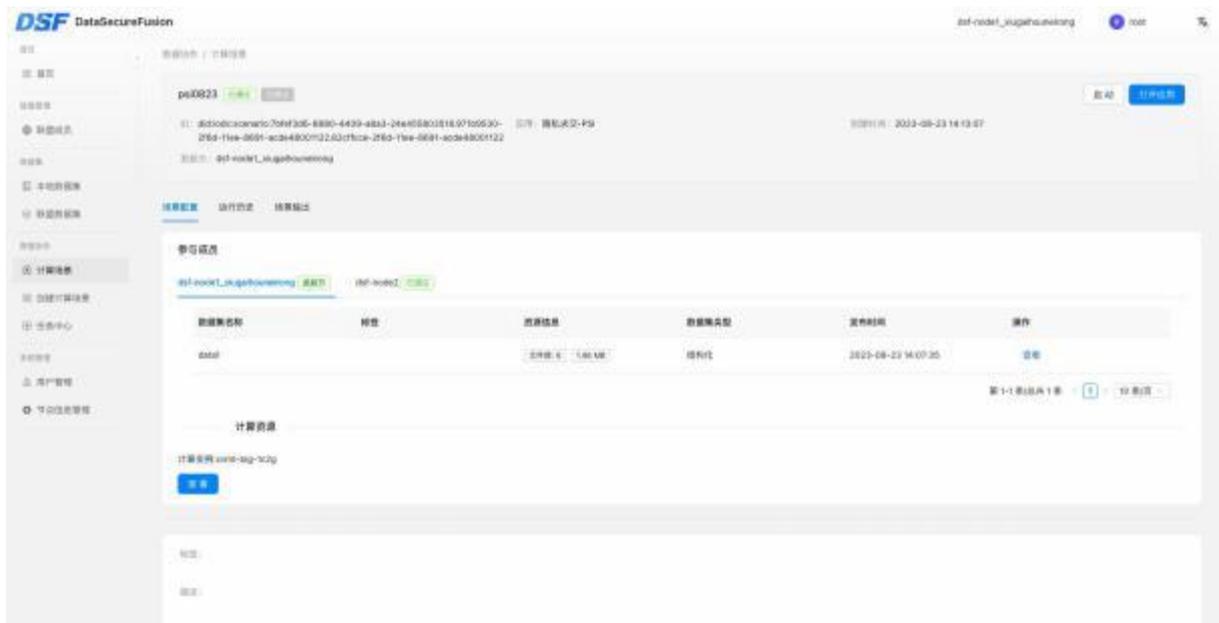
Secure Fusion 利用翼方健数的 MPC 技术，使用户能够安全地计算双方数据集的交集，并返回两个数据集中的 id。求交后的结果可以导出以进行进一步的操作，例如联邦学习。

首先，在创建计算场景时，在多方安全计算下选择隐私集合求交。关于创建计算场景，请参考【计算场景】模块。

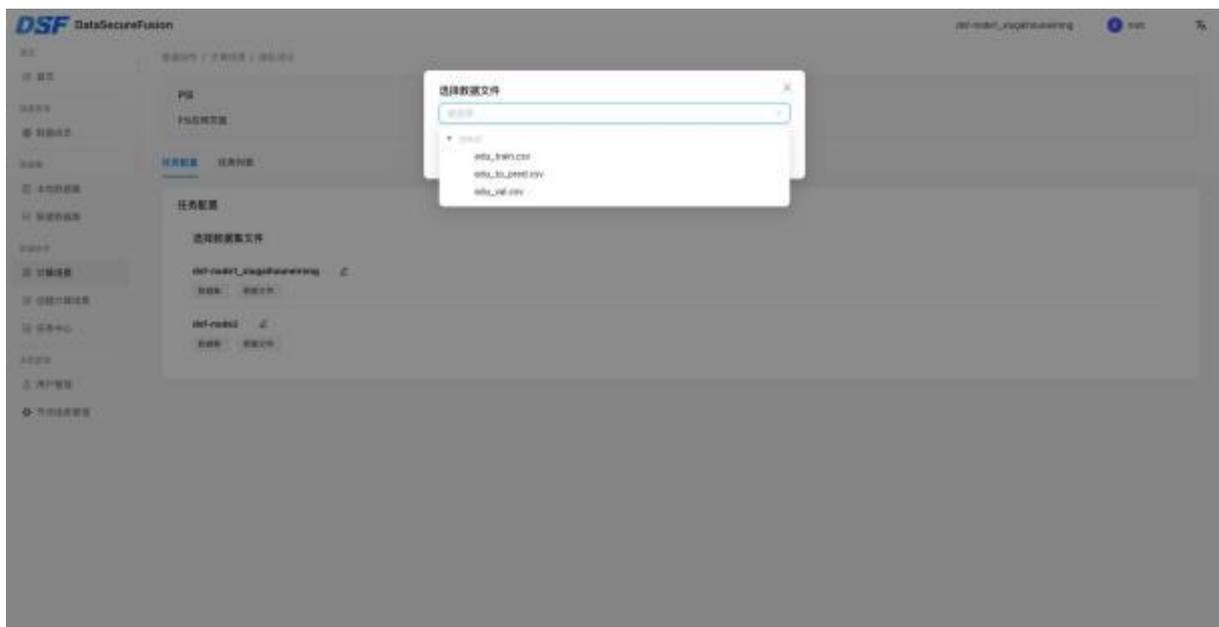


一旦场景被创建并得到所有参与方的批准就可以进入场景。在这里您可以看到场景的细节。接下来，我们需要指定要执行 PSI 的文件。

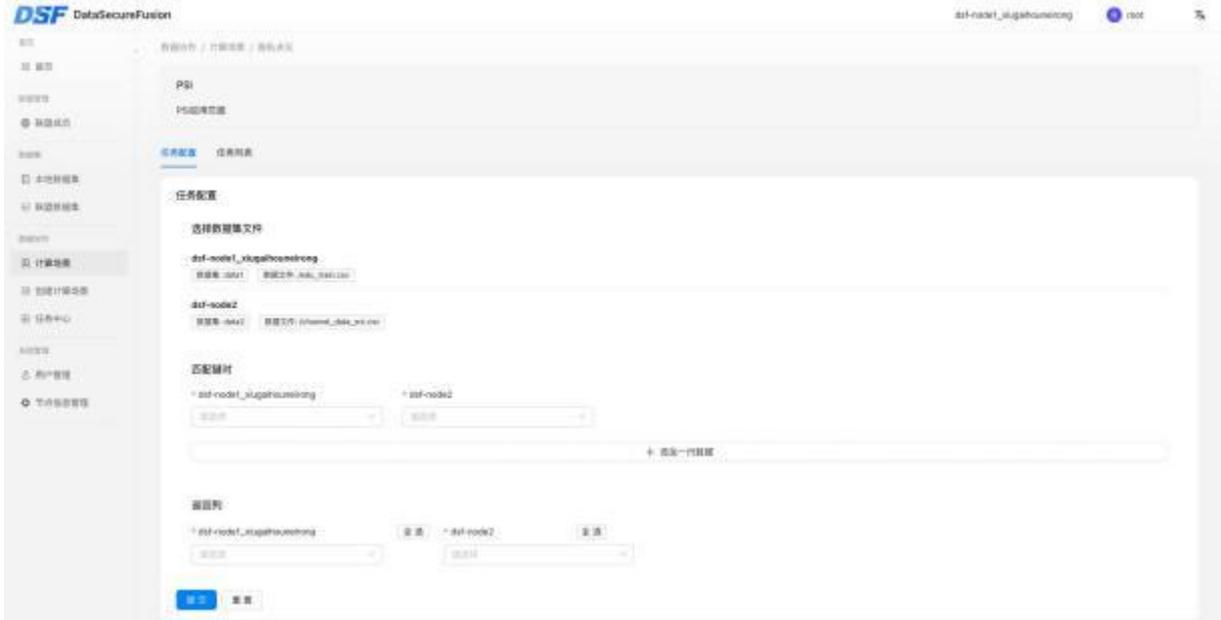
首先单击“启动”按钮以启动实例。实例启动后，点击“打开应用”进行配置。



单击每个参与方的编辑图标，选择 PSI 的输入文件。



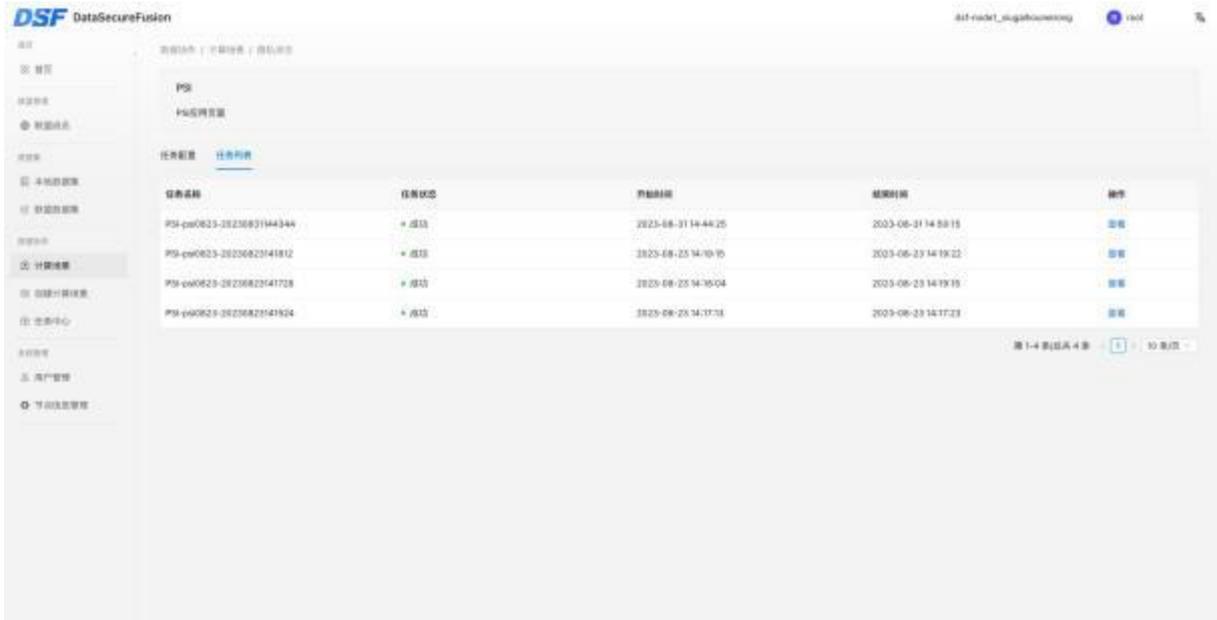
接下来，您需要为每个文件选择需要进行匹配的键对。例如，如果您为自己的文件选择 X，为参与者的文件选择 Y，PSI 将返回 $X = Y$ 的所有数据。单击“添加一行数据集”，并为每个参与者选择一列。



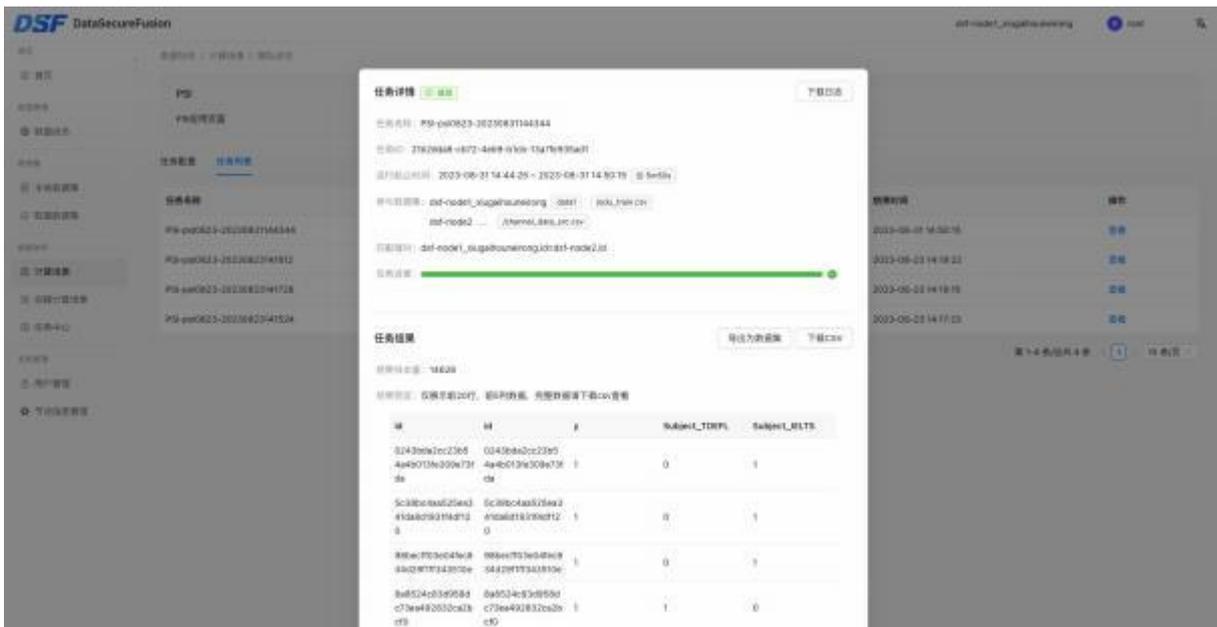
最后，您需要为您和参与方选择输出结果中需要返回的字段。一旦一切都配置好了，您就可以提交并运行 PSI。



要查看您提交的 PSI 任务，请点击“任务列表”。您可以提交多个 PSI 任务，只需要再次执行上面的配置过程即可。



要查看结果，请点击“查看”。在这里，您可以查看结果文件的前 20 行和前 5 列。您可以下载整个 CSV 文件或将其导出到新的数据集。



匿踪查询

介绍

匿踪查询 (Private Information Retrieval, PIR) 是一种加密协议，它允许用户从数据库检索特定的信息片段，而不会泄露任何关于查询的信息，也不会泄露被检索的数据库或任何其他第三方的数据。

PIR 的主要目标是保护用户查询和被检索数据的隐私，同时仍然允许用户访问他们需要的信息。这是通过使用高级加密技术实现的，例如同态加密、安全多方计算和不经意传输。

PIR 通常用于用户需要访问敏感数据（如医疗记录、财务数据或个人信息），但不希望透露有关其查询或正在访问的数据的任何信息的场景。PIR 也用于去中心化系统，例如点对点网络和区块链系统，用户希望在不泄露其身份或网络上其他用户访问的数据的情况下检索特定数据。

Secure Fusion 的 PIR

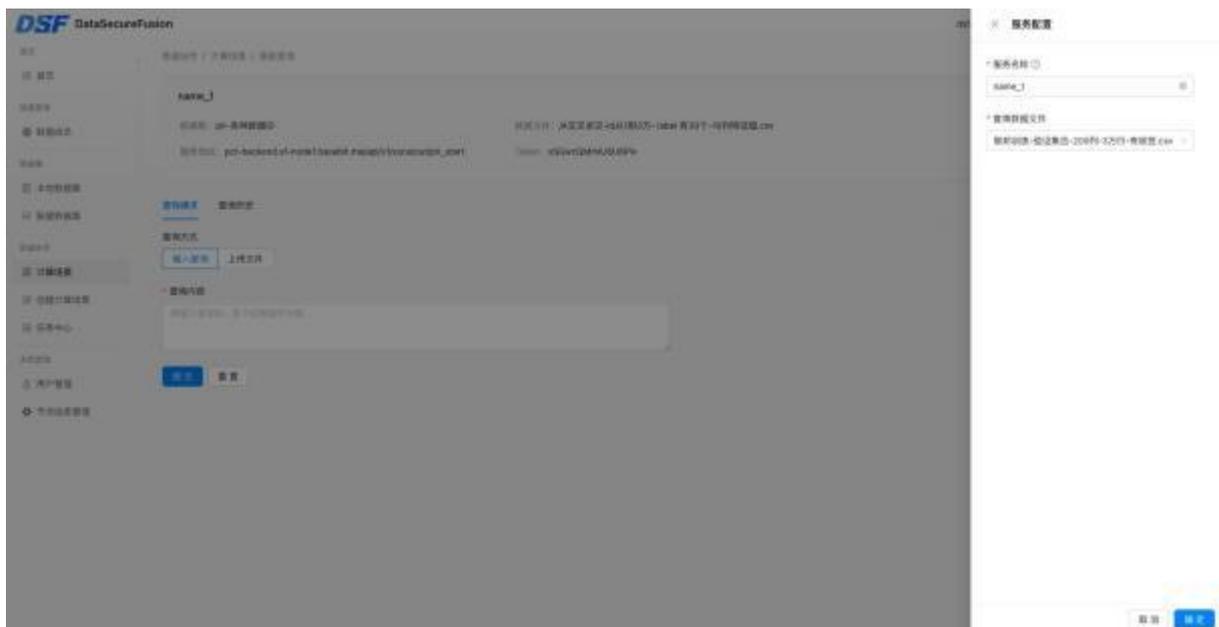
Secure Fusion 利用翼方健数的 MPC 技术，使用户能够在隐私保护下查询其他 DSF 节点的数据。结果可以导出以进行进一步的操作，例如联邦学习。

首先，在多方安全计算下选择匿踪查询，同时创建一个计算场景。关于创建计算场景，请参考【计算场景】模块。

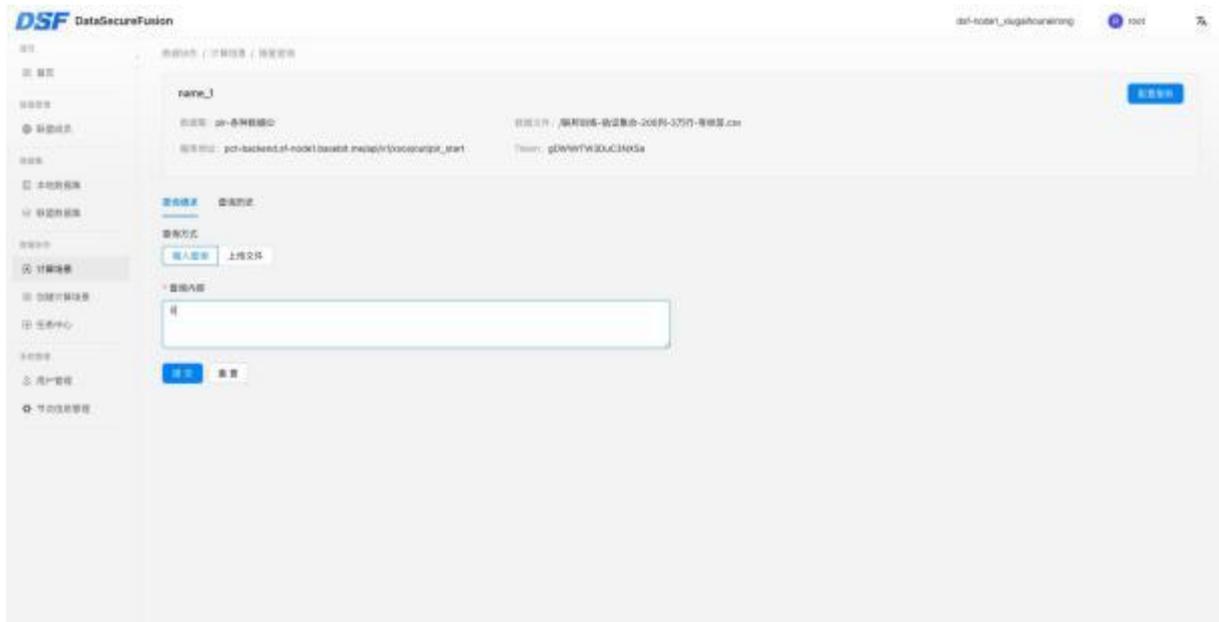


一旦场景被创建并得到所有参与方的批准，就可以进入场景。在这里您可以看到场景的细节。接下来，我们需要指定想要执行 PIR 的文件。

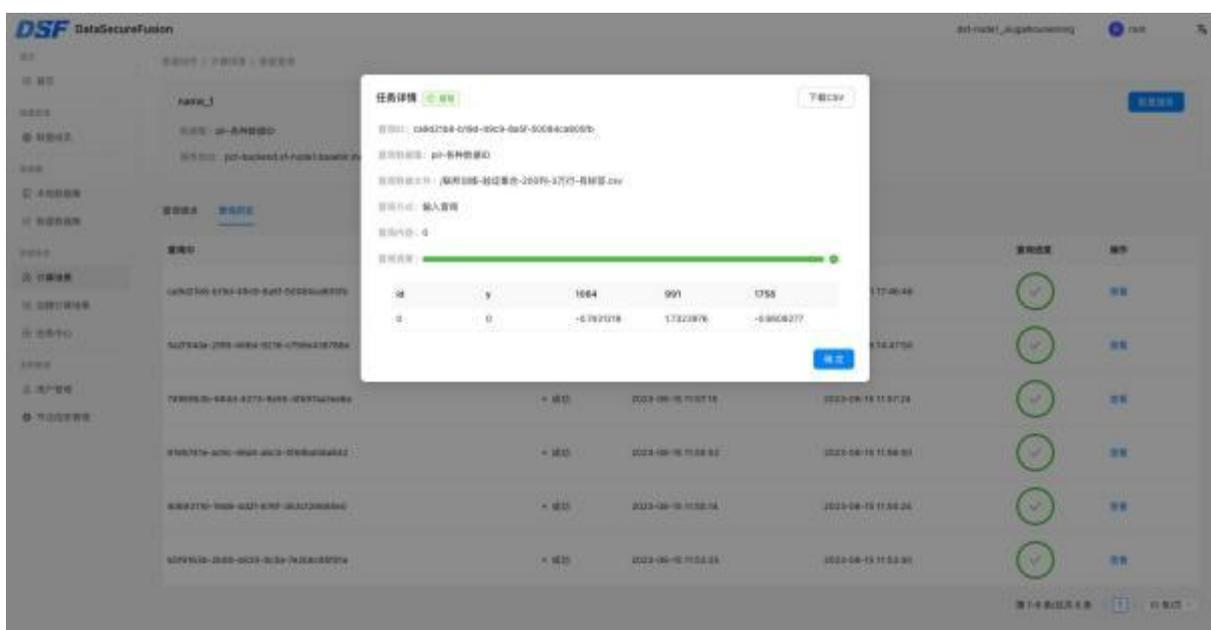
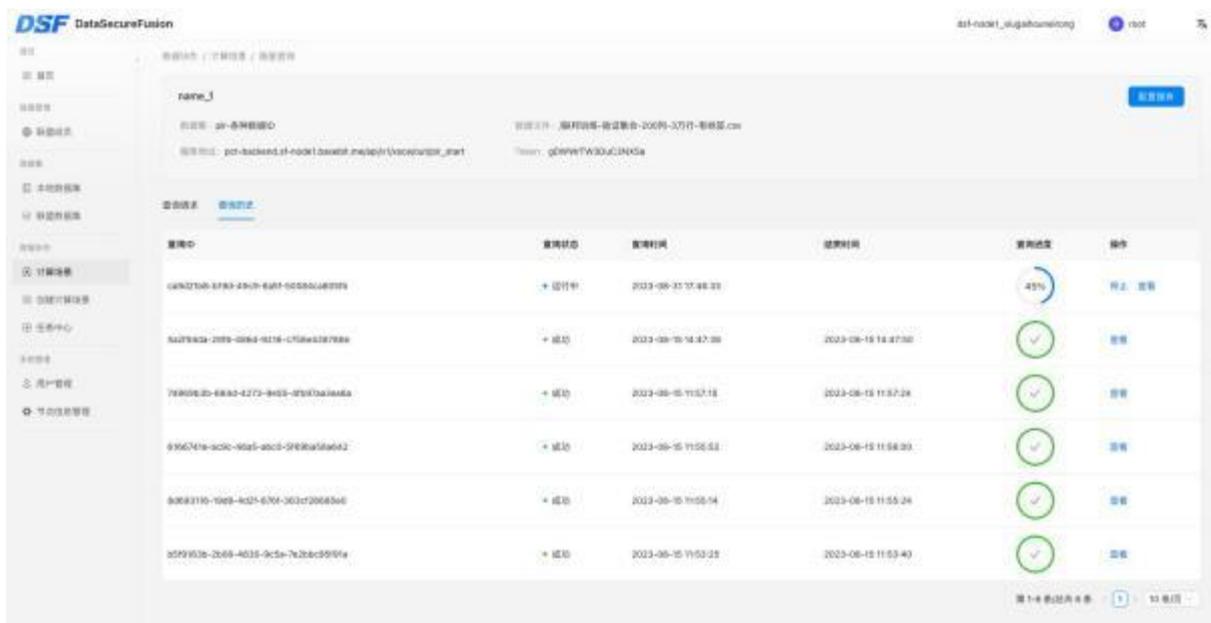
首先单击“启动”按钮以启动实例。实例启动后，点击“打开应用”进行配置。



您可以手动输入查询内容，也可以上传查询文件。



提交查询后，您可以通过点击“查询历史”查看查询结果。点击“查看”查看结果。



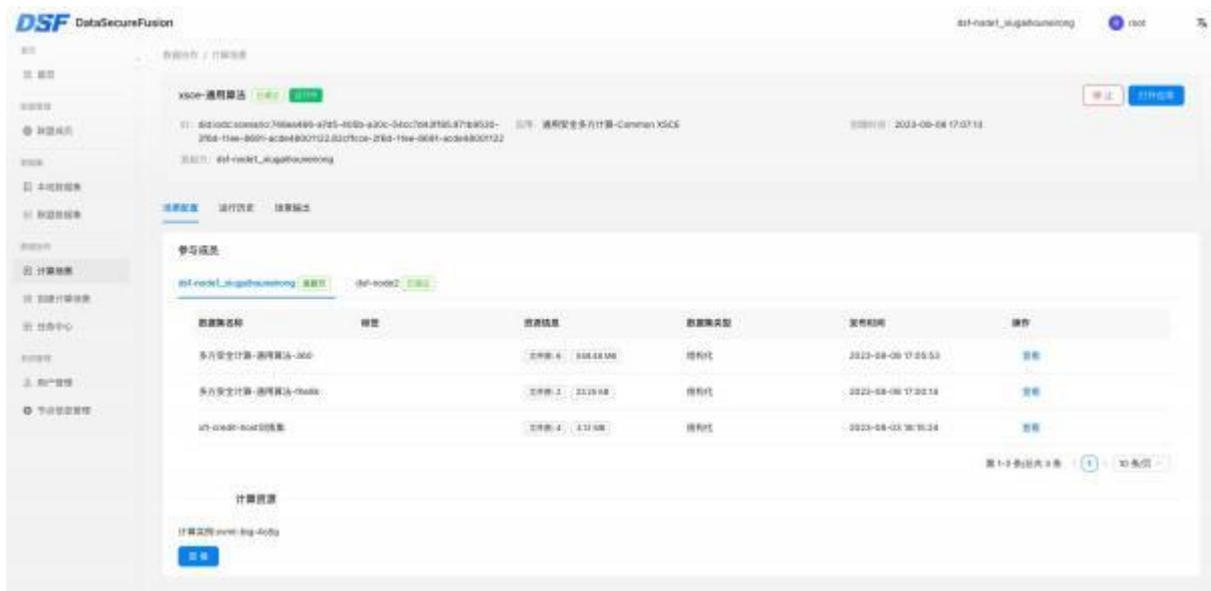
XSCE 通用算法

除了隐私集合求交和匿踪查询，平台还集成了一些其他的多方安全计算能力，包括多列的 PSI 和 PIR，以及全同态加密计算等。

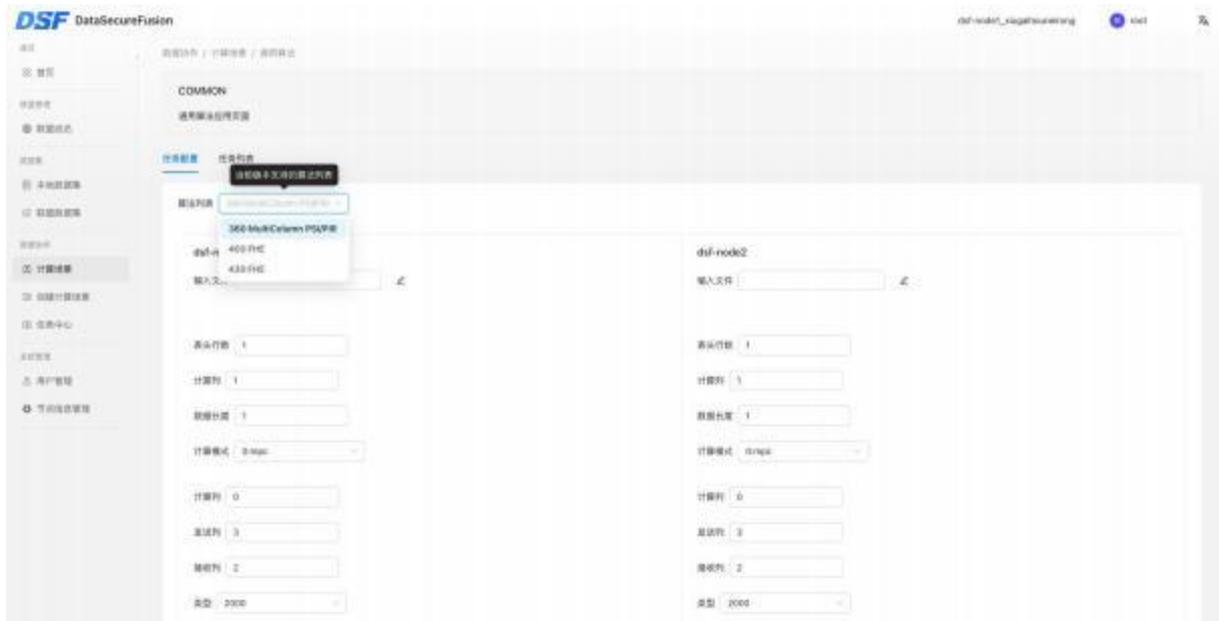
选择多方安全计算下的 XSCE 通用算法，同时创建一个计算场景。关于创建计算场景，请参考【计算场景】模块。



一旦场景被创建并得到所有参与方的批准，就可以进入场景。在这里您可以看到场景的细节。单击“启动”按钮以启动实例。实例启动后，点击“打开应用”进行配置。

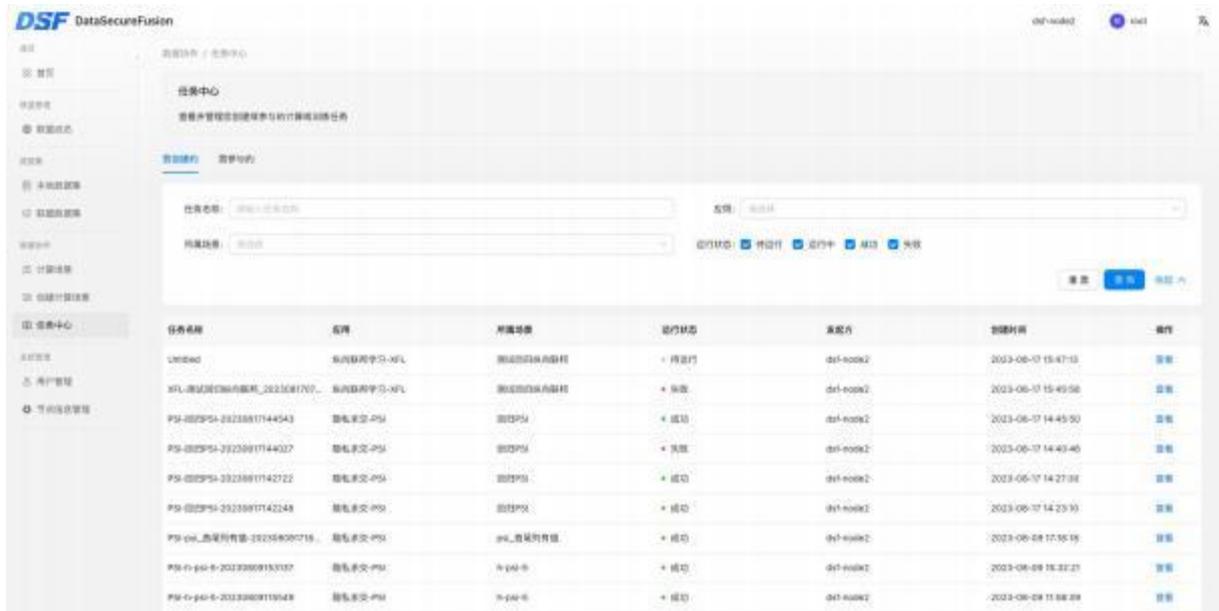


首先选择需要使用的 XSCS 算法，然后再进行具体任务参数的配置，配置完成后即可提交任务。



3.6.3.任务中心

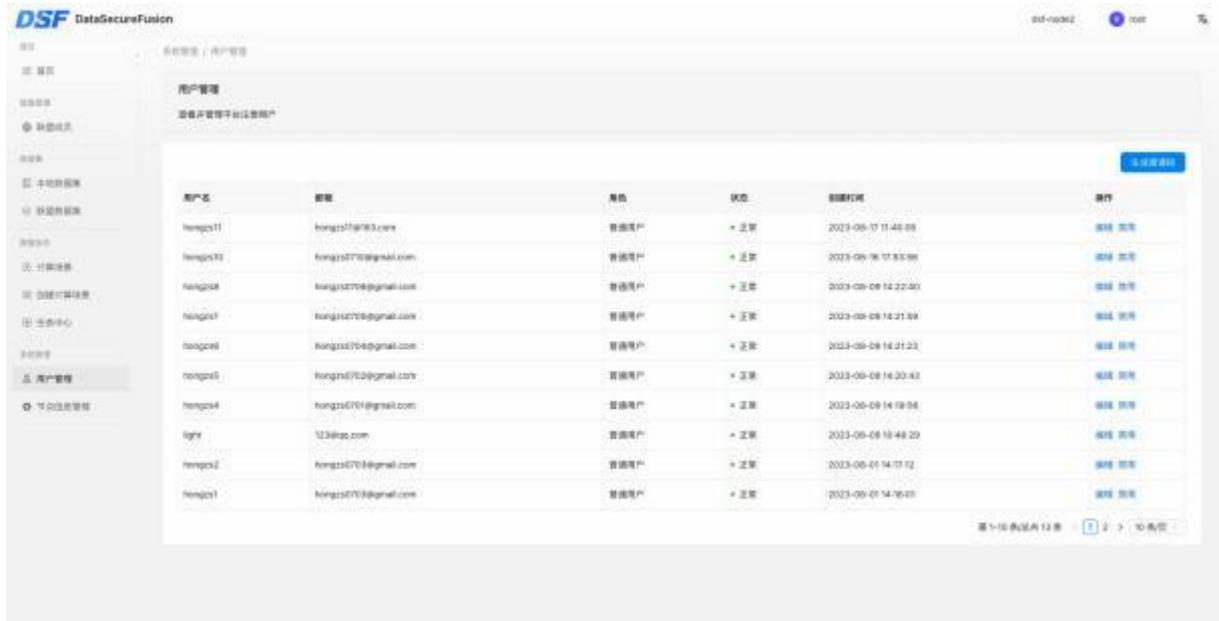
从导航栏进入“任务中心”模块，您可以在这里查看、搜索所有在该节点创建及参与的任务。除了搜索任务名称，您还可以通过应用、场景和任务运行状态进行任务的筛选。点击查看即可跳转到任务详情页查看具体任务信息。



3.7. 系统管理

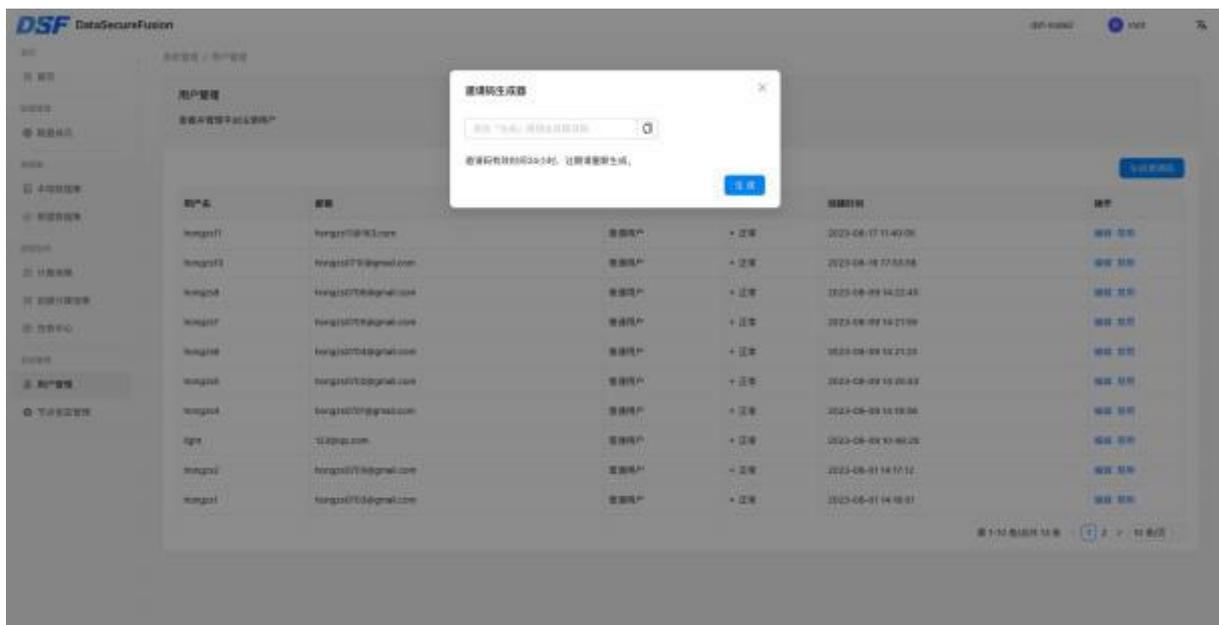
3.7.1. 用户管理

如果您是平台管理员，您可以在导航栏“系统管理”下的“用户管理”对平台用户进行管理。您可以查看所有平台用户的列表。



邀请用户

要注册一个新用户，请点击“生成邀请码”。点击弹出窗口上的“生成”按钮，将生成一个代码。复制并发送代码给用户，以便其可以在注册过程中输入此代码。请注意，代码将在 24 小时后过期。

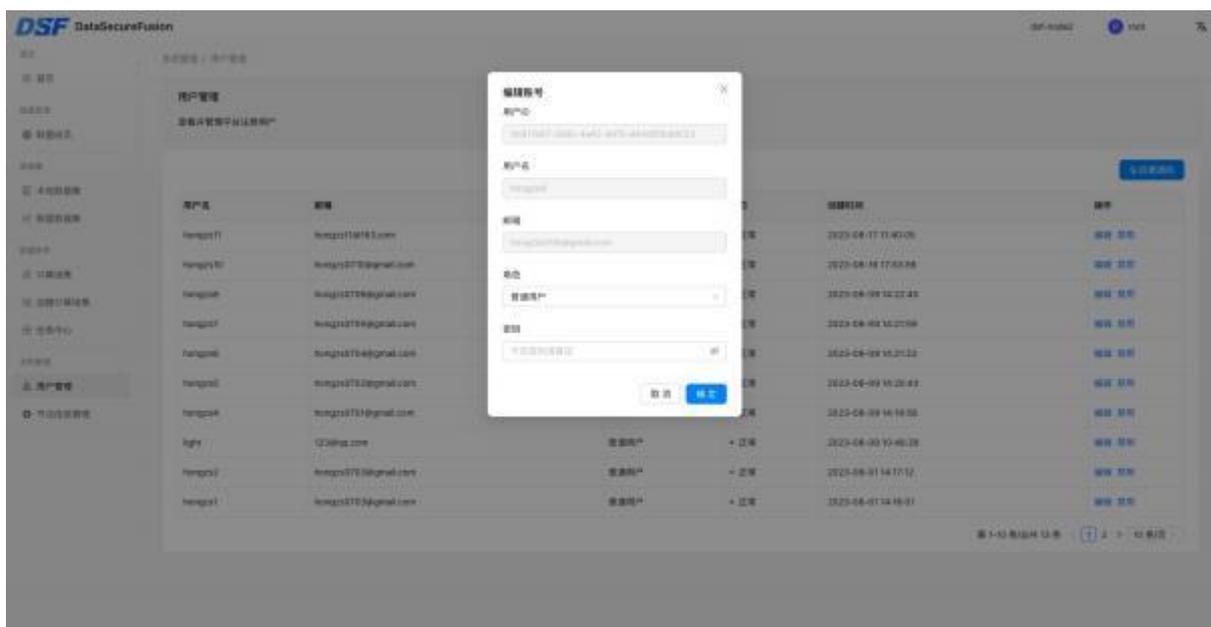


管理用户

出于安全考虑，Secure Fusion 只允许管理员修改平台用户的密码。要帮助用户修改密码，点击

用户的“编辑”按钮，然后在“密码”栏中输入密码。

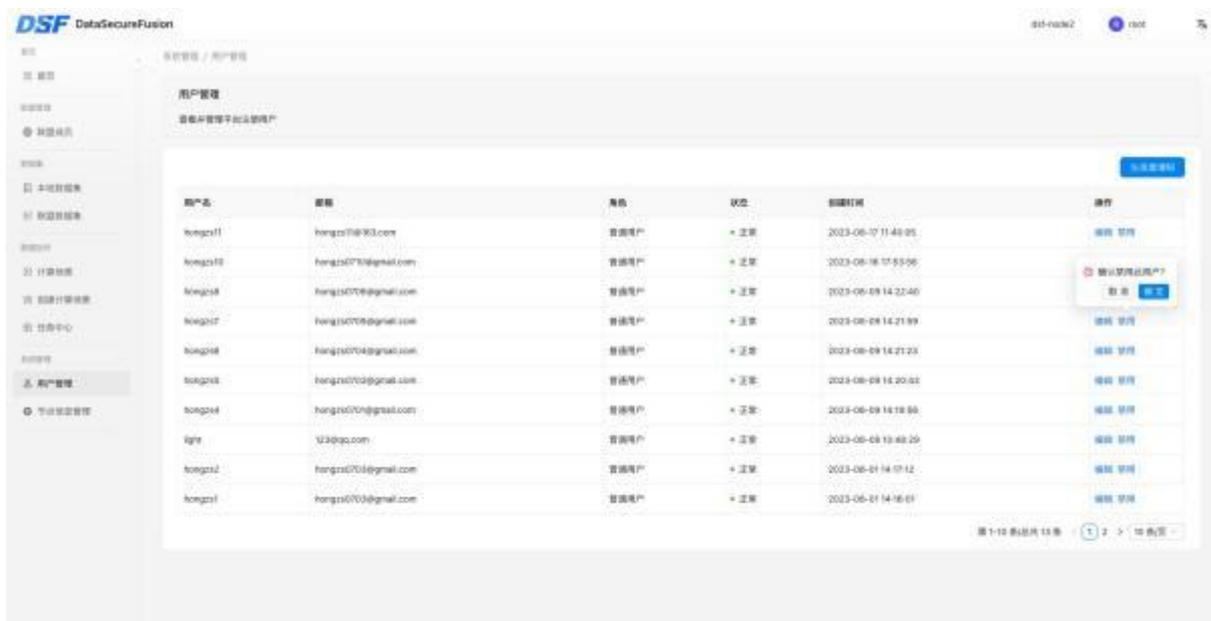
在这里，您还可以为用户分配管理员角色；只需在“角色”字段中选择角色即可。



启用/禁用用户

如果您想要删除某个平台用户的访问权限，您可以点击该用户的“禁用”按钮。用户状态为“禁用”时无法再访问平台。

要重新激活该用户，请单击该用户的“启用”按钮。当其状态变为“正常”时，用户可以再次使用该平台。



3.7.2.节点信息管理

如果您是平台管理员，您可以管理您的 SF 节点对其他 SF 节点的可见性。进入导航栏“系统管理”

