可信智能计算服务

产品介绍

文档版本	01
发布日期	2022-04-16

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。

目 录

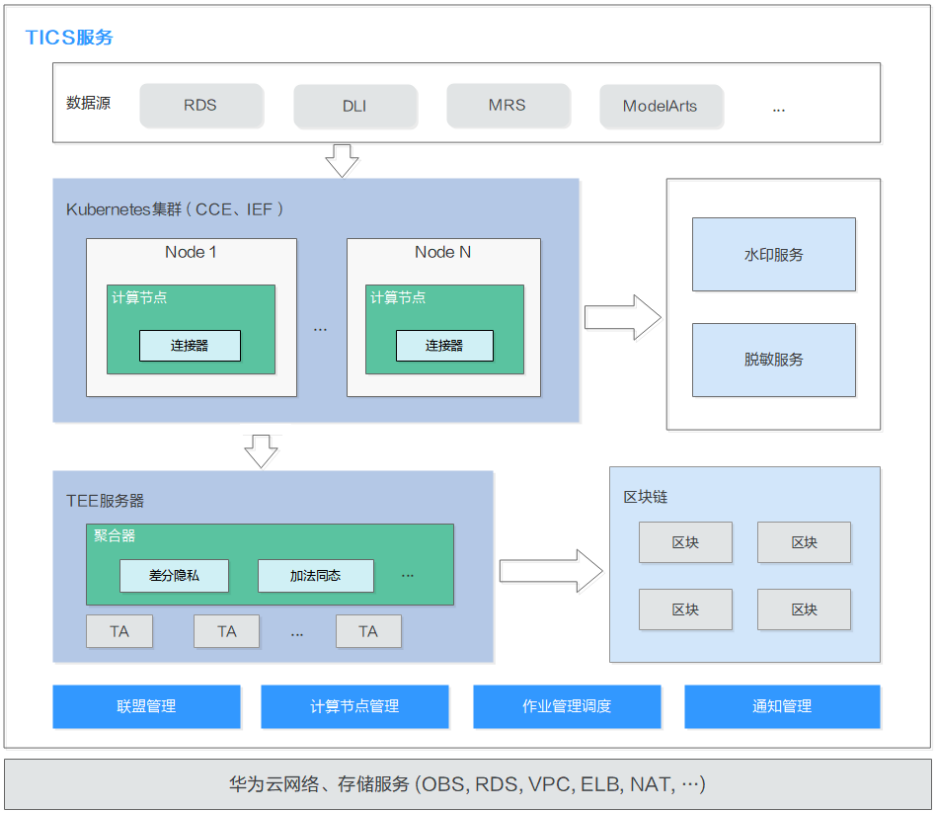
1 产品概述

可信智能计算服务TICS（ Trusted Intelligent 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。

产品架构

产品架构如图1-1所示。

图 1-1 产品架构



- **联盟管理**

邀请云租户作为数据方，动态构建可信计算联盟，实现联盟内严格可控的数据使用和监管。

- **数据融合分析**

  支持对接多个数据参与方的主流数据存储系统，为数据消费者实现多方数据的SQL Join等融合分析, 各方的敏感数据在具有可信执行环境ArmTrustZone安全支撑的聚合计算节点中实现安全统计。

- **计算节点**

  数据参与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（敏感，非敏感，脱敏）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。

- **联邦分析计算**

  对接主流深度学习框架实现横向和纵向的联邦训练，支持基于安全密码学(如不经意传输、差分隐私等)的多方样本对齐和训练模型的保护。

- **数据使用监管**

  为数据参与方提供可视化的数据使用流图，提供插件化的区块链对接存储，实现使用过程的可审计、可追溯。

- **容器化部署**

  容器化的多方数据源计算节点、聚合计算节点的部署管理，支持云上、边缘、HCS多种部署模式。

TICS 版本及规格说明

表 1-1 TICS 版本

版本	建议使用场景
企业版	满足企业级规模商用。

表 1-2 TICS 规格说明

规格	服务内容
联邦SQL分析	支持
横向联邦学习	支持
纵向联邦学习	支持

2 产品优势

多域协同

- 支持在分布式的、信任边界缺失的多个参与方之间建立互信联盟；
- 实现跨组织、跨行业的多方数据融合分析和多方联合学习建模。

灵活多态

- 支持对接主流数据源（如MRS, DLI, RDS, Oracle等）的联合数据分析；
- 支持对接多种深度学习框架(TICS，TensorFlow)的联邦计算；
- 支持控制流和数据流的分离，用户无需关心计算任务拆解和组合过程，采用有向无环图DAG实现多个参与方数据流的自动化编排和融合计算。

自主高效

- 数据使用全流程可视化展示，为数据参与方提供可感知、可监测的数据使用过程；
- 支持数据参与方、计算方的多种部署模式，包括云上（同Region、跨Region）、边缘节点、HCSO的部署模式；
- 采用容器化资源/部署管理，支持调度方、数据参与方、计算方的弹性扩缩容。

安全隐私

- 支持用户自定义隐私策略，实现敏感数据的识别、脱敏、水印保护，最大程度的保障隐私数据安全；
- 多方协同过程中隐私信息交互（SQL JOIN数据碰撞、联邦机器学习模型参数）的加密保护；
- 支持安全多方计算，如基于隐私集合求交PSI（Private Set Intersection）技术的多方样本对齐, 基于差分隐私、加法同态、秘密共享等技术的训练模型保护；
- 可插件化的对接区块链存储，实现多方数据的流动轨迹、使用过程的全程可追溯、可审计。

3 产品功能

动态联盟管理

动态构建可信计算联盟，实现联盟内严格可控的数据使用和监管。邀请云租户作为数据方，动态构建可信计算联盟，实现联盟内严格可控的数据使用和监管。联盟是联邦计算的载体，合作方只有加入联盟才能参与联邦计算。

安全的作业管理

作业时，数据使用的过程可审计、可追溯。TICS数据集成支持联邦数据分析、联邦机器学习和联邦预测作业等作业方式。

- **联邦数据分析**

  联邦数据分析是可信智能计算提供的关系型数据安全共享和分析功能。您可以创建联邦数据分析作业，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。

- **联邦机器学习**

  联邦机器学习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。

- **联邦预测作业**

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

可信智能计算节点

数据参与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）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。

多方融合分析

对接多种主流数据存储系统，为数据消费者实现多方数据的融合分析，参与方敏感数据能够在聚合计算节点中实现安全计算。

多方联邦训练

对接主流深度学习框架实现横向和纵向联邦建模，支持基于SMPC(如不经意传输、同态加密等)的多方样本对齐和训练模型保护。

云端容器化部署

参与方数据源计算节点云原生容器部署，聚合计算节点动态扩容，支持云、边缘、HCSO多种部署模式。

可视化数据监管

为数据参与方提供可视化的数据使用流图，提供插件化的区块链对接存储，实现使用过程的可审计、可追溯。

4 应用场景

政企信用联合风控

金融机构对于中小微企业的信用数据通常不足，央行征信数据覆盖率有限，不良企业多家骗贷事件屡有发生。金融机构与政府部门，如税务部门、市场监管部门、水电公司等在保护各方原始数据隐私的前提下，通过多方联合建模，金融机构补充了风控模型特征维度，提升模型准确率。

优势：

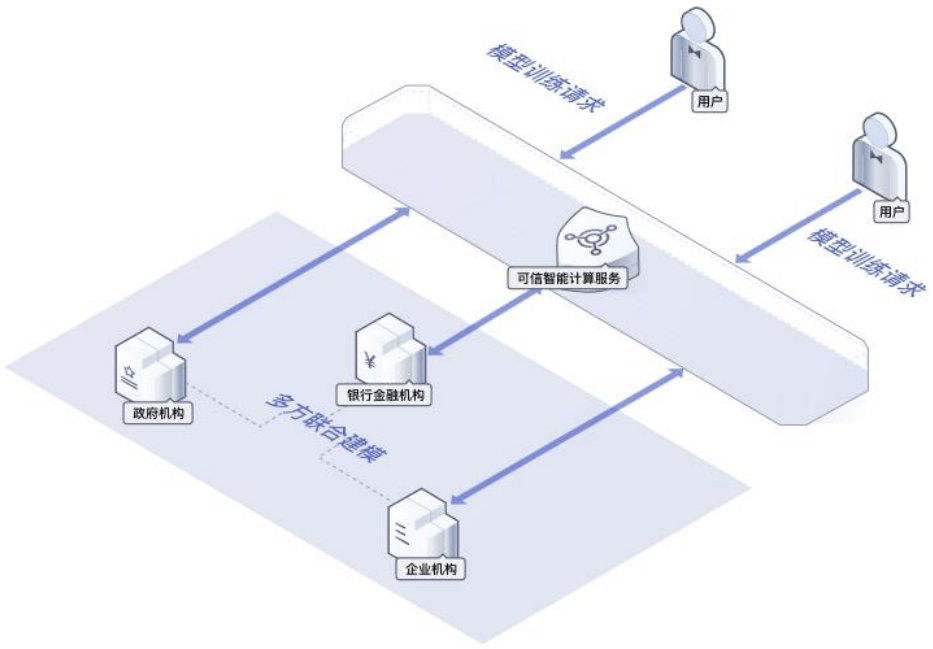
- 提升模型准确率

  多方机构实现算法层面联合建模，提升了需求方模型的预测效果。

- 数据隐私保护强

  多方采用隐私集合求交PSI对齐样本数据，本地数据或模型加密后在安全环境可信执行环境ArmTrustZone中运算，实现数据可用不可得。精细化的数据隐私保护策略，确保分析结果中强制执行隐私数据的脱敏。

图 4-1 政企信用联合风控



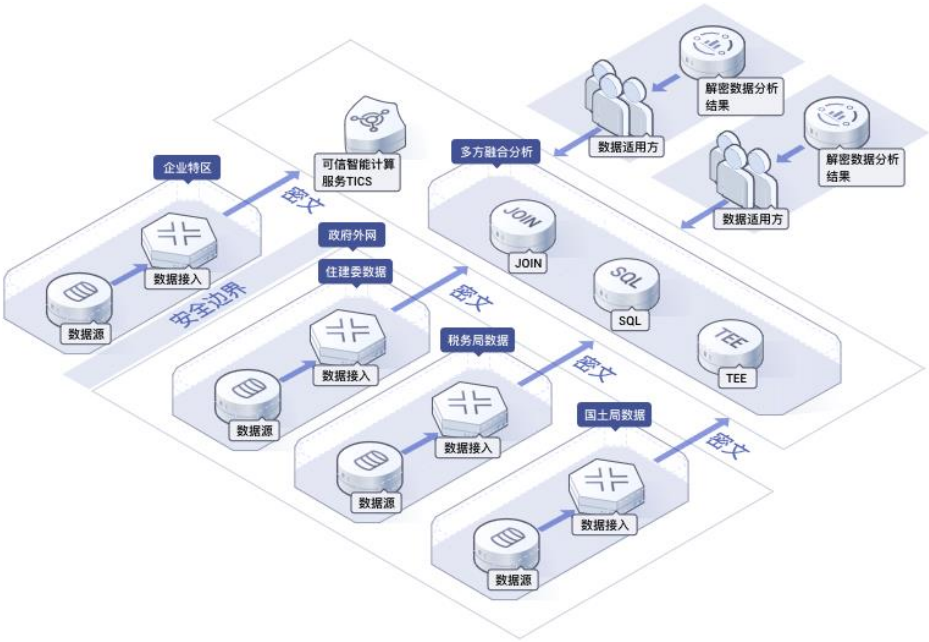
政府数据融合共治

由于数据安全以及隐私保护问题，政府各委办局数据尚未充分共享。多委办厅局数据的融合碰撞对于政府业务共治起到关键作用，例如本次疫情联防联控、综合治税等业务场景。共治场景均要实现在保护数据隐私的前提下，通过多个局委办数据的融合分析，得到数据碰撞结果，提升政府业务的治理效能。

优势：

- 政府多委办局之间密文数据融合计算，实现多方数据的融合分析。
- 基于隐私集合求交实现多方安全SQL JOIN分析， 原始数据保存在各个用户本地，统计分析算子下推到本地数据域执行。
- 多方分析JOIN算子进行数据隐私保护，计算过程将多方加密后数据完成计算，计算结果加密返回给数据使用方。
- 支持自定义脱敏保护策略，设定SQL语句安全等级检查，防止非法SQL执行。

图1-1 政府数据融合共治



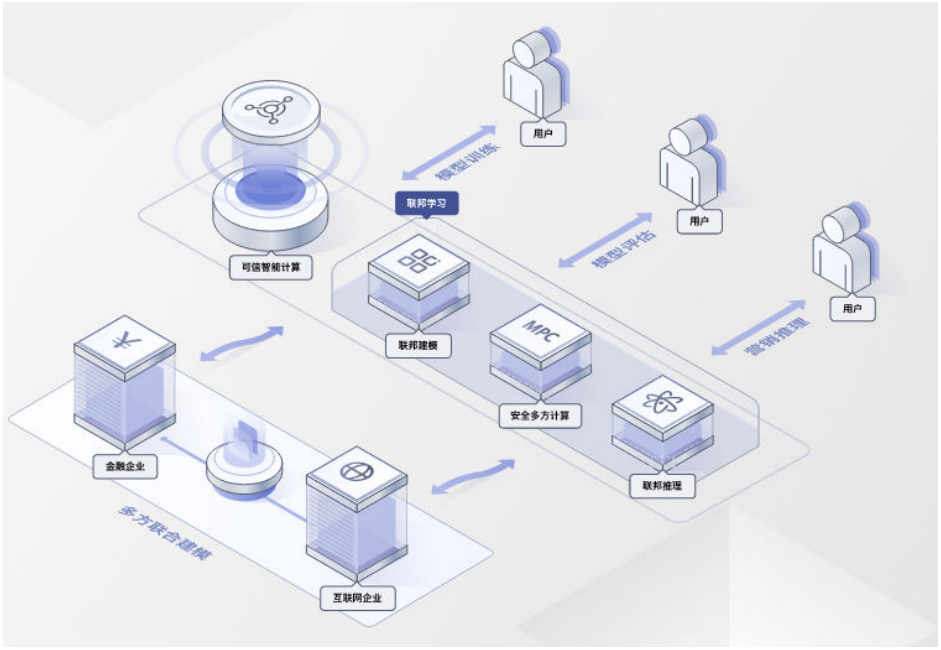
金融联合营销

传统金融企业联合营销模式中，金融企业往往需要将双方的数据集中到一个安全实验室中进行标签融合，模型训练，但常面临数据泄露和隐私等挑战。联邦建模采用分布式架构进行部署和建模，参与联合营销的企业原始和明细数据不出库的前提下进行跨域数据建模，实现精准营销，同时保障企业数据安全与个人隐私。

优势：

- 原始数据不出企业安全域、不出库，实现“数据不动、算法动”，数据使用自主可控。
- 联合多方正样本的效果，丰富模型的特征，提高模型的泛化能力。
- 计算全程保障企业数据安全与个人隐私。

图 4-2 金融联合营销



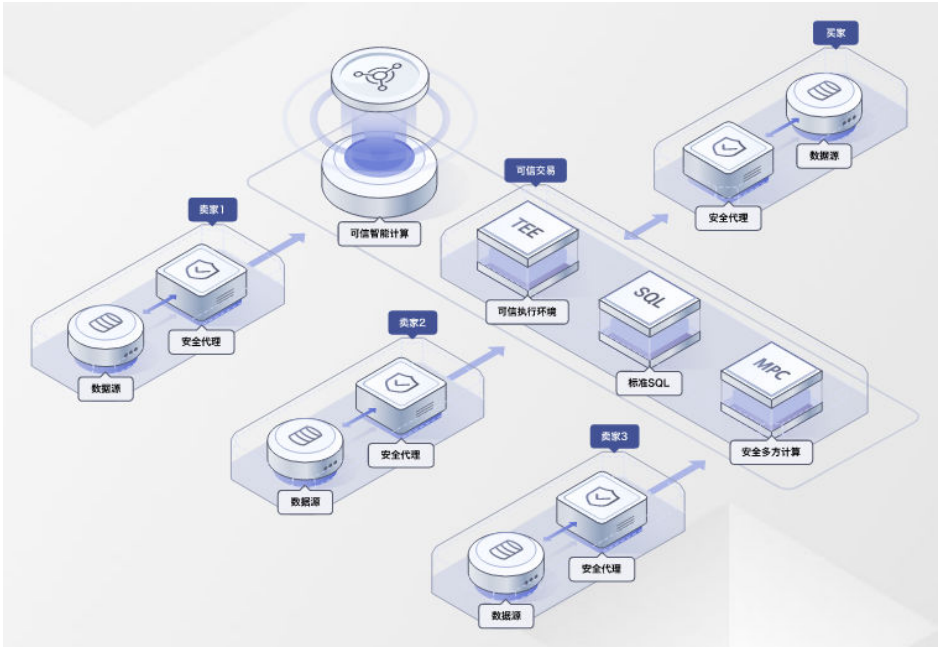
使能数据交易

传统数据交易方式，交易的是数据所有权，交易完成后，数据被无限制的拷贝和复制。采用可信交易方式，交易的不是数据，而是数据的使用权，卖家卖的是对某个数据的用法用量，不用担心数据被拷贝和复制。

优势:

- 数据不离开卖家，更放心。
- 卖家控制“隐私规则”，控制“用法和用量”。
- 支持三层异构，跨组织、跨地域、跨数据源。
- 低成本部署，支持边缘模式单节点部署。

图 4-3 使能数据交易



5 基本概念

联盟（League）

可信智能计算服务的逻辑概念，由组织方创建。联盟绑定不同数据保护方式的聚合器，并邀请多方数据提供者参与，在联盟内实现数据有限共享应用，提炼数据价值。

联盟是联邦计算的载体。联盟需要购买才能使用，在联盟中可以管理合作成员，合作数据以及查看可信智能计算环境。执行联邦计算任务需要指定联盟。

聚合器（AGG）

聚合器，进行多方数据运算结果的聚合。

合作方（Partner）

联盟成员，有权使用联盟中的数据，或者将自有数据发布到联盟，供其他合作方受限使用。

邀请（Invitation）

联盟组织者在联盟增添新的合作方，需要合作方接受邀请后，才能作为正式合作方参与到联盟运作中来。

计算节点

部署在参与方侧，是可信智能计算与合作方侧数据的桥梁，保障数据按照合作方意愿受限使用。

计算节点是管理参与方数据的最小单位。部署计算节点时需要指定联盟配置信息。在计算节点中支持配置连接器，注册数据集，任务执行，查看任务执行日志。

连接器（Connector）

连接器是可信智能计算节点内置的连接特定数据源所需的对象模板，目前支持连接MRS Hive、MySQL、RDS、Modelarts、DWS、ORACLE等多种连接器，并支持扩展增加新的连接器。

数据集（Data set）

数据集为计算节点获取并配置的合作方数据的元数据信息，以及附加其上的隐私策略。

字段分类（Field classification）

各数据集字段在其联邦分析上的业务分类，以明确字段用途和场景，避免不合理应用。

唯一标识（Unique Identifier）

用于标识某个事物实体身份的字段。例如身份证、工号、公司代码等。

敏感（Sensitive）

涉及隐私的数据，例如薪水、纳税、用电量、成交量等。

非敏感（Nonsensitive）

不涉及隐私的数据， 例如所处城市、公司类型等。

脱敏（Desensitization）

按照一定的算法，将原始数据的敏感部分隐去。

作业（Job）

作业是指用户创建的联邦分析、学习任务。

作业实例（Job instance）

作业每次运行都将产生一个作业实例，以区分、记录作业历次运行的状况。

作业实例任务（Job instance Task）

作业实例拆解出的更细粒度任务。

联邦数据分析

允许多合作方参与的结构化数据SQL分析作业。

联邦机器学习

允许多合作方参与的模型训练、评估作业。

联邦预测学习

允许多合作方参与的样本联合预测作业。

存储方式

指计算节点所属的CCE或IEF容器的工作负载，目前CCE容器仅支持“OBS存储”方式，IEF容器仅支持“主机存储”方式。“OBS存储”方式是将OBS服务中的路径映射

到服务容器内的本地路径，“主机存储”方式是指将计算节点所在机器的本地路径映射到服务容器内的本地路径。

主机路径

挂载使用的容器外部的路径，用于服务容器内和外部数据交互。用户只有在工作路径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工作目录，供用户查看、获取。

6 TICS 权限管理

如果您需要对华为云上购买的TICS资源，给企业中的员工设置不同的访问权限，以达到不同员工之间的权限隔离，您可以使用统一身份认证服务（Identity and Access Management，简称IAM）进行精细的权限管理。该服务提供用户身份认证、权限分配、访问控制等功能，可以帮助您安全的控制华为云资源的访问。

通过IAM，您可以在华为云帐号中给员工创建IAM用户，并授权来控制他们对华为云资源的访问范围。例如您的员工中有负责软件开发的人员，您希望他们拥有TICS的使用权限，但是不希望他们拥有删除工作空间等高危操作的权限，那么您可以使用IAM为开发人员创建用户，通过授予仅能使用TICS服务，但是不允许删除工作空间的权限，控制他们对TICS资源的使用范围。

如果华为云帐号已经能满足您的要求，不需要创建独立的IAM用户进行权限管理，您可以跳过本章节，不影响您使用TICS服务的其它功能。

IAM是华为云提供权限管理的基础服务，无需付费即可使用，您只需要为您帐号中的资源进行付费。关于IAM的详细介绍，请参见**《IAM产品介绍》**。

TICS 权限

默认情况下，管理员创建的IAM用户没有任何权限，需要将其加入用户组，并给用户组授予策略或角色，才能使得用户组中的用户获得对应的权限，这一过程称为授权。授权后，用户就可以基于被授予的权限对云服务进行操作。

TICS部署时通过物理区域划分，为项目级服务。授权时，“作用范围”需要选择“区域级项目”，然后在指定区域（如华北-北京1）对应的项目（如cn-north-1）中设置相关权限，并且该权限仅对此项目生效；如果在“所有项目”中设置权限，则该权限在所有区域项目中都生效。访问TICS时，需要先切换至授权区域。

权限根据授权精细程度分为角色和策略。

- **角色**：IAM最初提供的一种根据用户的工作职能定义权限的粗粒度授权机制。该机制以服务为粒度，提供有限的服务相关角色用于授权。由于云各服务之间存在业务依赖关系，因此给用户授予角色时，可能需要一并授予依赖的其他角色，才能正确完成业务。角色并不能满足用户对精细化授权的要求，无法完全达到企业对权限最小化的安全管控要求。

  TICS未提供基于IAM角色的权限控制功能。
- **策略**：IAM最新提供的一种细粒度授权的能力，可以精确到具体服务的操作、资源以及请求条件等。基于策略的授权是一种更加灵活的授权方式，能够满足企业对权限最小化的安全管控要求。例如：针对TICS服务，管理员能够控制IAM用户仅查看TICS服务，无法进行相关操作。

如表1所示，包括了TICS的所有系统权限。

表 6-1 TICS 系统策略

策略名称	描述	策略类别
TICS FullAccess	TICS管理员权限，拥有该权限的用户可以拥有TICS所有权限。	细粒度策略
TICS CommonOperations	TICS服务普通用户权限，拥有该权限的用户可以拥有MRS服务使用权限，无新增、删除资源权限。	细粒度策略
TICS ReadOnlyAccess	TICS服务只读权限，拥有该权限的用户仅能查看TICS的资源。	细粒度策略

相关链接

- IAM产品介绍

TICS FullAccess 策略内容

```
{
   "Version": "1.1",
   "Statement": [
      {
         "Action": [
            "tics:*:*"
         ],
         "Effect": "Allow"
      },
      {
         "Action": [
            "cce:cluster:list",
            "cce:node:list",
            "ecs:cloudServers:list",
            "mrs:cluster:list",
            "modelarts:trainJob:create",
            "modelarts:trainJobVersion:list"
         ],
         "Effect": "Allow"
      }
   ]
}
```

TICS CommonOperations 策略内容

```
{
   "Version": "1.1",
   "Statement": [
      {
         "Action": [
            "tics:*:get*",
            "tics:*:list*",
            "tics:league:*",
            "tics:job:*",
            "tics:agg:*",
```

```
            "tics:agent:*"
        ],
        "Effect": "Allow"
    },
    {
        "Action": [
            "cce:cluster:list",
            "cce:node:list",
            "ecs:cloudServers:list",
            "mrs:cluster:list",
            "modelarts:trainJob:create",
            "modelarts:trainJobVersion:list"
        ],
        "Effect": "Allow"
    }
  ]
}
```

TICS ReadOnlyAccess 策略内容

```
{
  "Version": "1.1",
  "Statement": [
    {
        "Action": [
            "tics:*:get*",
            "tics:*:list*"
        ],
        "Effect": "Allow"
    }
  ]
}
```

7 计费说明

TICS（可信智能计算服务）采用包周期的计费模式。为了便于您便捷的下单购买，在控制台购买界面中系统会为您计算好所购买的套餐包价格，您可一键完成整个配置的购买。

计费项

TICS可信计算节点采用包年/包月的计费模式。TICS可信计算节点计费套餐如下表所示：

表 7-1 TICS 计费套餐

计费套餐包	套餐包子类	计费模式	计费说明
TICS可信计算节点	企业版	包年/包月	TICS可信计算节点的计费详情，请参见TICS价格详情。 在使用TICS过程中，使用其他云服务的费用（如弹性公网IP/带宽、对象存储服务OBS等），需按照相应云服务的计费规则进行计费，TICS联盟包不包含此类费用。 例如，在部署计算节点过程中，创建了CCE集群，CCE服务所需的费用需按照CCE服务的计费规则进行计费。

计费模式

TICS可信计算节点支持包年/包月计费模式。您可以根据实际使用情况，选择合适的TICS可信计算节点套餐，然后根据购买时长一次性支付套餐的费用，最短购买时长为一个月。

续费

- **“包年/包月”的TICS可信计算节点**

  对于TICS可信计算节点，请在所购买的套餐包时长用完前进行续费。

  TICS可信计算节点，支持包年包月计费模式，在订单周期结束后，订单进入保留期。保留期届满时若您仍未续费订单，相应的资源将被释放，您资源中的数据也将被删除。在保留期内所产生的相关费用将在您续费时一并收取。

  TICS可信计算节点支持自动续费，自动续费的默认续费周期为：

  - 按月购买：自动续费周期为1个月。
  - 按年购买：自动续费周期为1年。

  您可以通过以下两种方式开通自动续费：

  - 登录TICS控制台，在购买TICS实例的页面中，勾选“自动续费”选项。
  - 如果您已购买TICS实例，请进入**续费管理**页面，在列表中查找所需续费的TICS实例，单击其所在行的“开通自动续费”，然后请根据页面提示完成自动续费的开通。

  您也可以进行手动续费，请进入**续费管理**页面，在列表中查找所需续费的TICS实例，单击其所在行的“续费”，进行手动续费操作。有关续费的更多信息，请参见**续费管理**。

到期与欠费

- **到期**
  - **TICS可信计算节点套餐**

    TICS可信计算节点套餐采用包年/包月计费模式，套餐到期后进入保留期。保留期内，数据仍予以保留，但是您将无法访问TICS实例，您无法在TICS管理控制台进行操作，相关接口也无法调用。如果在保留期结束时您没有续费，TICS将终止服务，系统中的数据也将被永久删除。
- **欠费**
  - TICS可信计算节点套餐采用包年/包月的计费模式，没有欠费的概念，在所购买的时长用完时套餐结束。

退订

TICS服务套餐生效期间，您可以根据需要，灵活退订TICS包年包月套餐包括依赖的CCE服务。有关退订的更多信息，请参见**退订管理**。

8 约束与限制

使用TICS前，您需要认真阅读并了解以下使用限制。

浏览器限制

您需要使用支持的浏览器版本登录TICS。

表 8-1 浏览器兼容性

浏览器版本	说明
Google Chrome浏览器88.x及以上	建议优选

9 与其他云服务的关系

统一身份认证服务

TICS使用统一身份认证服务（Identity and Access Management，简称IAM）实现认证和鉴权功能。

云审计服务

TICS使用云审计服务（Cloud Trace Service，简称CTS）审计用户在管理控制台页面的操作，可用于检视是否存在非法或越权操作，完善服务安全管理。

消息通知服务

TICS使用消息通知服务（Simple Message Notification，简称SMN）依据用户的订阅需求主动推送通知消息，使用户可以在触发告警（如质量监控）时能立即接收到通知。

