

Octopus Cloud Service

产品介绍

文档版本 01
发布日期 2024-08-09



版权所有 © 华为技术有限公司 2024。保留一切权利。

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

商标声明



HUAWEI和其他华为商标均为华为技术有限公司的商标。

本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

华为技术有限公司

地址： 深圳市龙岗区坂田华为总部办公楼 邮编： 518129

网址： <https://www.huawei.com>

客户服务邮箱： support@huawei.com

客户服务电话： 4008302118

安全声明

漏洞处理流程

华为公司对产品漏洞管理的规定以“漏洞处理流程”为准，该流程的详细内容请参见如下网址：

<https://www.huawei.com/cn/psirt/vul-response-process>

如企业客户须获取漏洞信息，请参见如下网址：

<https://securitybulletin.huawei.com/enterprise/cn/security-advisory>

目录

1 什么是 Octopus.....	1
2 功能介绍.....	4
3 基本概念.....	6
4 计费说明.....	7
4.1 计费概述.....	7
4.2 计费模式.....	7
4.3 计费项.....	8
4.4 续费.....	11
4.5 欠费与到期.....	11
4.6 费用账单.....	12
5 与其他服务的关系.....	13
6 配额说明.....	15
7 安全.....	16
7.1 责任共担.....	16
7.2 资产识别与管理.....	17
7.3 身份认证与访问控制.....	17
7.4 数据保护技术.....	18
7.5 审计与日志.....	18
7.6 服务韧性.....	20
7.7 故障恢复.....	21
7.8 更新管理.....	21
7.9 认证证书.....	21
7.10 安全风险知会.....	22
8 个人数据说明.....	23
9 权限管理.....	24

1 什么是 Octopus

自动驾驶云服务（Octopus）是面向车企、研究所的全托管平台，在华为云上提供自动驾驶数据云服务、自动驾驶标注云服务、自动驾驶训练云服务、自动驾驶仿真云服务、自动驾驶大模型云服务、配置管理服务，帮助车企以及研究所快速开发自动驾驶产品。

“一站式”是指自动驾驶产品开发的各个环节，包含数据资产、数据合规、数据处理、数据标注、增量数据集、模型训练、仿真测试等操作都可以在Octopus上完成，支持用户从数据到应用的全流程开发；从技术上看，Octopus底层支持各种异构计算资源，开发者可以根据需要灵活选择使用，而不需要关心底层的技术，让自动驾驶开发变得更简单、更方便。

产品架构

自动驾驶云服务（Octopus）是一个一站式的开发平台，能够支撑开发者从数据收集到仿真应用的全流程开发过程。整体由数据资产、数据合规、数据处理、标注服务、训练服务、仿真服务、智驾模型服务、公共配置管理组成。

图 1-1 Octopus 基础功能架构图

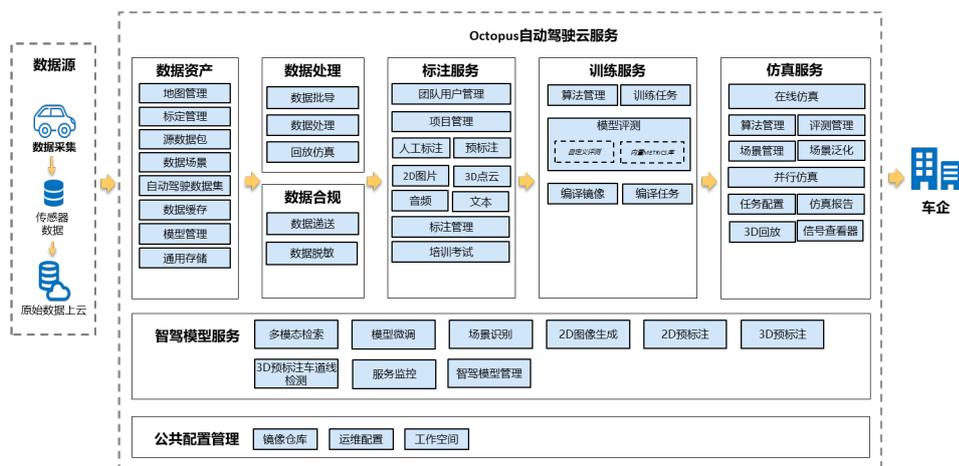
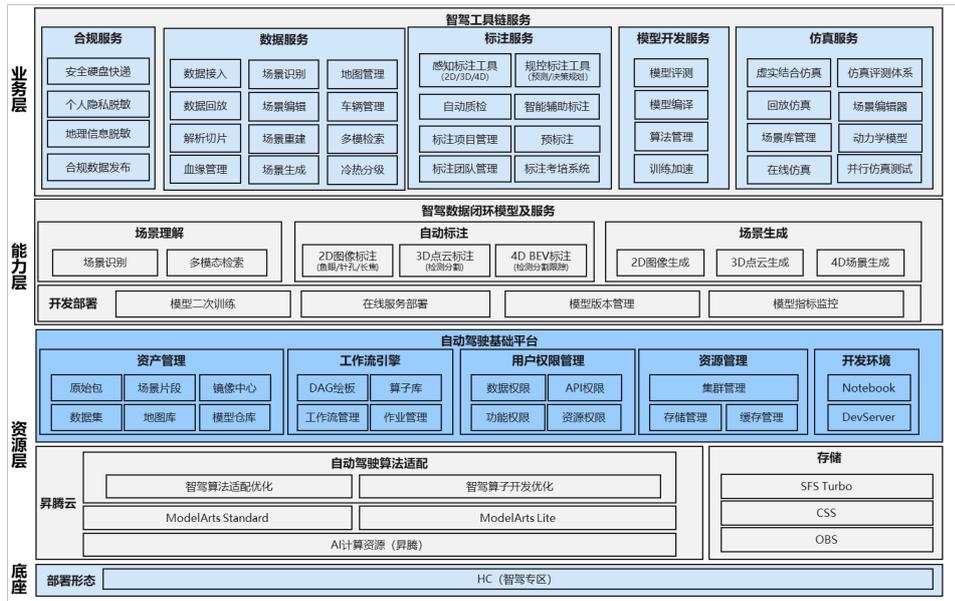


图 1-2 Octopus 高级功能架构图



产品优势

- 一站式**
 开箱即用，全托管的自动驾驶云服务，用户无需从零搭建一套复杂的自动驾驶大数据平台、AI平台、仿真平台、标注平台等多个工具平台，只需聚焦于核心价值（自动驾驶算法、标注数据、仿真场景），快速开展自动驾驶业务，跟上瞬息多变的市场节奏。
- 海量数据**
 平台可支持PB级数据存储和亿级数据秒级检索。
- 软硬件加速**
 感知算法训练和仿真需要使用大量算力资源，Octopus依托华为自研软硬件能力提供的强大算力支持，满足每天百万公里仿真测试和算法训练。
- 自动化标注**
 自动驾驶算法的持续提升依托于持续增加的高质量标注数据集，平台提供预标注范例模型，能对常用的物体如乘用车、大巴车、行人、骑行者、交通灯、可行驶区域等进行预标注，同时通过难例挖掘持续提升标注数据集质量。
- 仿真场景库**
 提供场景库管理和分布式运行能力，覆盖大部分驾驶路况，提升自动驾驶安全性。
- 并行仿真**
 实车测试成本高，危险系数高，提供并行仿真能力，能够利用云端资源快速回归仿真场景，提供上千个并行仿真节点，完成日行百万公里虚拟里程。
- 合规性**
 脱敏算子对数据包进行脱敏处理（包括人脸、车牌、gnss高程），保证用户数据上传的合规性，避免个人隐私泄露，保护用户的数据信息和财产安全。
- 昇腾云助力**
 昇腾云具有稳定安全的底层算力，提供极致性价比。昇腾双栈AI算力，支持万节点计算集群管理。全流程昇腾迁移工具链，典型自动驾驶感知算法适配昇腾，可

以大幅度缩短迁移周期（迁移周期<2周）。统一资源调度，资源极致利用，可以大幅度提升综合分配率（综合分配率达90%），弹性调度、训练和推理融合调度，大幅度缩减资源发放时间（资源发放<30分钟）。

- **大模型赋能**

盘古大模型赋能自动驾驶，分钟级完成数据处理。自动驾驶场景理解代替人工打标签分类，万段视频片段分钟级处理完成。自动驾驶场景生成，通过NeRF技术实现车型变换、车道变换、场景组合渲染等应用。自动驾驶预标注，代替人工标注，支持2D、3D、4D自动标注，准确率超过90%。自动驾驶多模态检索支持以文搜图、以图搜图等多维检索能力，实现百万图片分钟级检索。

如何访问 Octopus

Octopus提供了简洁易用的管理控制台，包含数据收集、数据处理、数据标注、模型训练、在线仿真等功能，您可以在管理控制台完成您的自动驾驶开发。

使用Octopus管理控制台，需要先注册华为云。如果您已注册华为云，可在控制台直接搜索Octopus登录。如果未注册，请参见[注册账号](#)。

2 功能介绍

自动驾驶行业的关键开发工具对自动驾驶汽车开发和量产有着重要的推动作用。然而，自动驾驶面临许多问题，如海量的数据存储、模型迭代资源耗费、人工标注高成本、孤岛工具链等，开环验证和闭环仿真都很难快速迭代起来。为解决这个问题，Octopus自动驾驶云服务覆盖自动驾驶数据、模型、训练、仿真、标注等主要业务，让用户开箱即用，一站式开发体验，打通孤岛工具链，以实车数据驱动算法迭代模型和仿真评价。Octopus分别提供以下功能：

数据服务

- 以数据为核心。
- 提供数据批导、源数据包、数据处理、数据缓存、数据集管理。
- 数据结构化：处理车载硬件平台上输出的传感器数据，详细统计各类传感器信息。
- 数据集治理：支持PB级海量存储。
- 提供通用存储、模型仓库，方便集中处理数据以及模型信息。

标注服务

- 以标注为核心。
- 平台提供点云和图片的人工标注和预标注。
- 支持数据预标注功能，节省大量人力成本。

训练服务

- 以模型为核心。
- 平台提供软硬件加速模型训练和推理，大幅缩短训练时间，提升训练效率。
- 支持上传自定义算法和自定义模型，提升算法泛化能力和识别率。
- 支持模型管理与评测，提高模型的准确性，持续提升自动驾驶安全系数。

仿真服务

- 以测试为核心。
- 提供车辆动力学仿真、自动驾驶算法仿真、传感器仿真、交通流仿真等功能，实现对自动驾驶算法的大规模仿真测试，持续提升自动驾驶算法的安全性。

- 在数据服务和训练服务的基础上，提供在线仿真管理、算法管理、评测管理、场景管理、任务管理等应用工具，确保自动驾驶规模合规、安全、可度量，版本快速集成。

智驾模型服务

- 以盘古大模型为核心。
- 自动驾驶场景理解代替人工打标签分类，万段视频片段分钟级处理完成。
- 自动驾驶预标注，代替人工标注，支持2D/2.5D/3D自动标注，准确率超90%。
- 自动驾驶场景生成，通过NeRF技术实现车型变换、车道变换、场景组合渲染等应用。
- 自动驾驶多模态检索支持以文搜图、以图搜图等多维检索能力，实现百万图片分钟级检索。

3 基本概念

抽帧

抽帧是将解压后的Rosbag数据，抽出单幅画面，生成图片数据或者视频数据。

自动驾驶汽车在进行测试时会产生大量数据，车企需要对这些数据高效处理与分析，因此在进行自动驾驶研究时需要对这些原始数据有选择性、针对性地进行提取和分析，抽帧便是一种筛选数据的方式。针对数据类型，Octopus将抽帧任务分为图片抽帧和点云抽帧。

点云

点云是一种由激光雷达收集到的数据类型，包含三维坐标、反射强度等信息，用来检测和识别车行道上的物体。

雷达会在车辆行驶过程中不断收集点云数据来了解周围的环境，并利用点云数据所获得的环境信息帮助车辆定位，提高车辆定位的精度。

接管

接管是从自动驾驶系统转换为驾驶员对汽车管理，即驾驶员接管自动驾驶系统对汽车进行管理，常用来考核自动驾驶系统完善程度，如接管次数、接管里程等。

数据标注

对数据进行场景标记，用以场景识别并进行模型训练。

难例

难例是模型训练过程中，出错率很高的一部分样本。是数据经过自动标注后，未标注成功或者标注错误的数据，需要通过人工筛选得到。可以通过维护难例集，将这部分样本集中维护，最终重新用于训练，持续提升算法和模型精度。

4 计费说明

4.1 计费概述

八爪鱼自动驾驶云服务是用于开发自动驾驶产品的一站式全托管平台。

Octopus服务的计费方式简单、灵活，根据不同使用场景，您可以选择不同的计费模式和计费项。

通过阅读本章内容，您可以快速了解Octopus服务的[计费模式](#)、[计费项](#)、[续费](#)、[欠费与到期](#)和[费用账单](#)。

4.2 计费模式

Octopus当前支持包年/包月、套餐包和按需计费三种计费模式，满足不同场景下用户需求。

- **包年/包月**：是一种预付费模式，即先付费再使用，按照订单的购买周期进行结算，因此在购买之前，用户必须保证账户余额充足。
- **套餐包**：一种预付费模式，即先付费再使用，您可以根据实际需求购买套餐包获取更多的优惠。
- **按需计费**：一种后付费模式，即先使用再付费，按照实际使用次数、处理数据量进行结算。

表 4-1 计费模式说明

计费模式	包年/包月	套餐包	按需计费
付费方式	预付费	预付费	后付费
计费周期	按订单的实际购买时长计费。	按照订单的有效周期结算。	按照单次生成订单费用结算。
适用计费项	基础版、扩容资源	模型	模型

适用功能模块	数据服务、标注服务、训练服务、仿真服务、合规服务	智驾模型服务	智驾模型服务、合规服务
适用场景	适用于可预估资源使用周期的场景。推荐长期使用用户购买。	适用于可预估资源使用周期的场景，价格比按需计费模式更优惠。	适用于需求波动大的场景，随时适用。

4.3 计费项

使用Octopus自动驾驶云服务进行自动驾驶全流程开发时，涉及到计费项主要包括**云服务费用**、**扩容资源费用**、**合规脱敏费用**、**智驾模型微调费用**、**模型费用**、**存储费用**。

云服务费用

云服务费用是指购买服务所需要的费用，包含了服务运行所需公共资源产生的费用。

表 4-2 云服务基础版计费说明

云服务名称	计费模式	计费说明	计费公式
八爪鱼自动驾驶云服务-基础版	包年/包月	购买八爪鱼自动驾驶云服务-基础版产生的费用。	规格单价 * 购买时长 * 套（仅支持1套）
数据服务-基础版		购买数据服务-基础版产生的费用。	
标注服务-基础版		购买标注服务-基础版产生的费用。	
训练服务-基础版		购买训练服务-基础版产生的费用。	
仿真服务-基础版		购买仿真服务-基础版产生的费用。	
合规服务-基础版		购买合规服务-基础版产生的费用。	

扩容资源费用

扩展资源费用是指使用Octopus时需额外购买的仿真扩展包、增强计算资源和存储扩容资源等产生的费用。除服务中自带的资源外，用户可增量购买扩容资源，提高计算性能和扩容存储空间。

表 4-3 扩容资源计费项说明

计费项	计费子项	计费模式	计费说明	计费公式			
存储扩容包	自动驾驶数据管理缓存扩容包	包年/ 包月	使用弹性文件服务 (SFS) 缓存文件, 产生的费用。	规格单价 * 购买时长 * 套			
	自动驾驶数据管理存储扩容包		使用对象存储服务 (OBS) 存储数据和模型, 产生的费用。				
通用处理节点	octopus计算型 CPU(16u32g) 专属实例		增强计算性能, 产生的费用。				
	octopus计算型 CPU(64u128g) 专属实例						
AI处理节点	octopus计算型 GPU(ant0324g 24u96g) 专属实例						
	octopus.hp.s2						
	octopus计算型 NPU(x866sntp 24g96u384g) 专属实例						
标注服务扩容包	同时在线用户数扩容包	支持多人在线标注, 产生的费用。					
仿真服务扩容包	规控仿真引擎-在线	购买在线仿真器, 产生的费用。					
	感知规控仿真引擎-在线						
	仿真场景编辑器						
	规控仿真引擎-并行			增加并行任务数, 产生的费用。			

合规脱敏费用

合规脱敏费用是指使用合规脱敏扩展包处理数据量所产生的费用。

表 4-4 合规脱敏计费项说明

计费项	计费模式	计费说明	计费公式
合规脱敏	按需计费	使用模型处理脱敏数据量进行收费。	按需计费：规格单价 * TB

智驾模型微调费用

模型费用是在使用智驾模型服务模型微调能力时，所产生的费用。

表 4-5 智驾模型微调计费项说明

计费项	计费模式	计费说明	计费公式
智驾模型微调	按需计费	根据创建模型微调任务时使用的资源按需收费。	按需计费：规格单价 * 小时

模型费用

模型费用是在使用智驾模型服务多模态检索、场景识别、2D预标注、2D图像生成、3D预标注等功能时，调用API所产生的费用。

表 4-6 模型计费项说明

计费项	计费模式	计费说明	计费公式
预标注	套餐包、 按需计费	使用模型时API调用次数产生的费用。	套餐包：套餐包规格单价 * 购买数量 * 有效周期（当前仅支持1个月）
2D图像生成			
场景识别		购买模型套餐包，价格比按需计费模式更优惠。	按需计费：规格单价 * API调用次数
多模态检索			

存储费用

存储费用是指使用Octopus时，在对象存储服务（OBS）存储数据产生的费用。

表 4-7 存储计费项说明

计费项	计费模式	计费说明	计费公式
对象存储（OBS）	包年/包月、按需计费	Octopus使用OBS存储数据，产生的费用。	具体费用可参见 对象存储价格详情 。

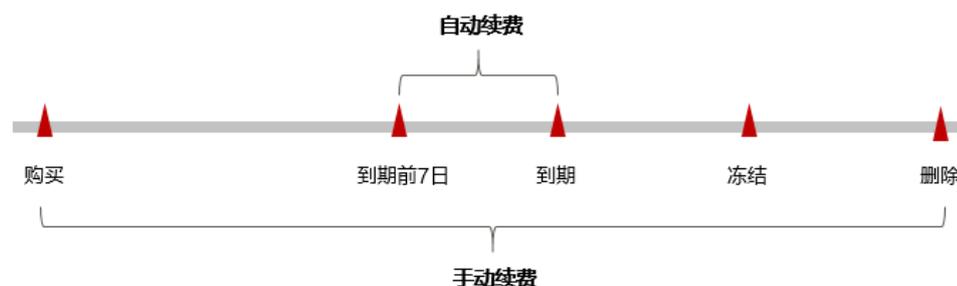
4.4 续费

包年/包月自动驾驶云服务到期后会影响到云服务器正常运行。如果您想继续使用，需要在指定的时间内为服务、资源、模型续费，否则将终止服务，系统中的数据也将被永久删除。在到期前续费成功，所有资源、数据得以保留，且服务的使用不受影响。

表 4-8 续费相关功能

功能	说明
手动续费	包年/包月云服务、资源从购买到自动删除之前，您可以随时在自动驾驶云服务控制台续费，以延长使用时间。
自动续费	开通云服务时勾选自动续费选项，系统会在每次到期前为您自动续费，避免因忘记手动续费而导致资源、数据被自动删除。

图 4-1 自动续费



4.5 欠费与到期

如下图所示，包年/包月资源各个阶段的状态。购买后，在计费周期内资源正常运行，此阶段为有效期；资源到期而未续费时，将陆续进入宽限期和保留期。

当您的账号欠费后，资源不会立即停止服务，资源进入**宽限期**。在宽限期内客户可正常访问和使用此服务资源。

如果您在宽限期内仍未续费服务资源，那么就会进入**保留期**，资源状态变为“已冻结”，针对已购买的服务、扩展资源、模型，允许访问、修改、删除其中的数据，不允许创建数据。

保留期到期后，如果服务资源仍未续费，那么服务资源以及其中的数据将被自动删除，无法恢复。

图 4-2 包年/包月资源生命周期



4.6 费用账单

您可以在“费用中心 > 账单管理 > 流水和明细账单”查看费用账单，以了解自动驾驶云服务某个产品在某个时间段的使用量和计费信息。

账单上报周期

包年/包月计费模式的资源完成支付后，会实时上报一条账单到计费系统进行结算。

按需计费模式的资源按照固定周期上报使用量到计费系统进行结算。按需计费模式产品根据使用量类型的不同，分为按小时、按天、按月三种周期进行结算，具体扣费规则可以参考[按需产品周期结算说明](#)。

按需计费资源的扣费时间可能会滞后于结算周期，例如：按小时结算上报账单的自动驾驶合规服务，8:00~9:00期间产生的费用，通常会在9:45左右才进行扣费。在“费用中心 > 账单管理 > 流水和明细账单 > 流水账单”中，“消费时间”即按需产品的实际使用时间。

查询费用账单

步骤1 登录“费用中心”，左侧菜单选择“账单管理 > 流水和明细账单”。

步骤2 选择“明细账单”页签。

步骤3 在筛选条件中选择产品（以自动驾驶合规服务为例），单击图标即可搜索该产品的账单。

图 4-3 查询费用账单



账单号	产品类型	产品	计费模式	账单类型	资源名称ID	资源名称	区域	可用区	使用量类型	单价	单价单位	使用量/定价量	使用单位
202404	自动驾驶云	自动驾驶合规	按需	合规-使用	compliance_...	自动驾驶合规	华北-乌兰察布	-	TB	560.00	元/TB	0.001855	TB
202404	自动驾驶云	自动驾驶合规	按需	合规-使用	compliance_...	自动驾驶合规	华北-乌兰察布	-	TB	560.00	元/TB	0.001855	TB
202404	自动驾驶云	自动驾驶合规	按需	合规-使用	compliance_...	自动驾驶合规	华北-乌兰察布	-	TB	560.00	元/TB	0.001855	TB

----结束

5 与其他服务的关系

统一身份认证服务

Octopus使用统一身份认证服务（Identity and Access Management，简称IAM）实现认证功能。IAM的更多信息请参见《[统一身份认证服务用户指南](#)》。

对象存储服务

Octopus服务使用对象存储服务（Object Storage Service，简称OBS）存储原始Rosbag数据以及预处理后的视频、抽帧图片等数据，实现安全、高可靠和低成本存储需求。OBS的更多信息请参见《[对象存储服务控制台指南](#)》。

表 5-1 Octopus 各环节与 OBS 的关系

功能	子任务	Octopus与OBS的关系
数据资产	地图管理	高精地图上传后存储在OBS中。
	标定管理	传感器标定上传的标定文件存储在OBS中。
	数据场景	场景挖掘后切出的rosvbag片段存储在OBS中。
	数据集	<ul style="list-style-type: none">数据集存储在OBS中。数据集的标注信息存储在OBS中。
	模型管理	模型文件存储在OBS中。
	通用存储	支持数据导出存储在OBS中。
数据处理	数据批导	支持导入OBS存储数据，支持实时扫描数据在OBS客户端操作。
	数据处理	数据处理后的结果存储在OBS中。

功能	子任务	Octopus与OBS的关系
标注服务	项目管理	<ul style="list-style-type: none"> 标注的图片、点云数据存储存储在OBS中。 标注信息数据、标注规范存储在OBS中。 标注任务日志和审核报告存储在OBS中。
训练服务	算法管理	算法文件存储在OBS中。
	训练任务	训练产物、训练任务日志存储在OBS中。
	模型评测	评测脚本文件、评测产物、评测任务日志存储在OBS中。
	编译管理	编译产物、编译任务日志存储在OBS中。
仿真服务	场景管理	场景文件存储在OBS中。
	逻辑场景管理	逻辑场景的参数空间敏感性分析文件存储在OBS中。
	并行仿真	仿真结果存储在OBS中。
智驾模型服务	2D图像生成	获取OBS访问授权，生成的2D图像存储在OBS中。
	模型微调	获取OBS访问授权，模型微调使用的训练数据集从OBS中获取。

6 配额说明

本服务应用的基础设施是对象存储服务。

关于如何查看配额，如何申请扩大配额，请参考[关于配额](#)。

7 安全

7.1 责任共担

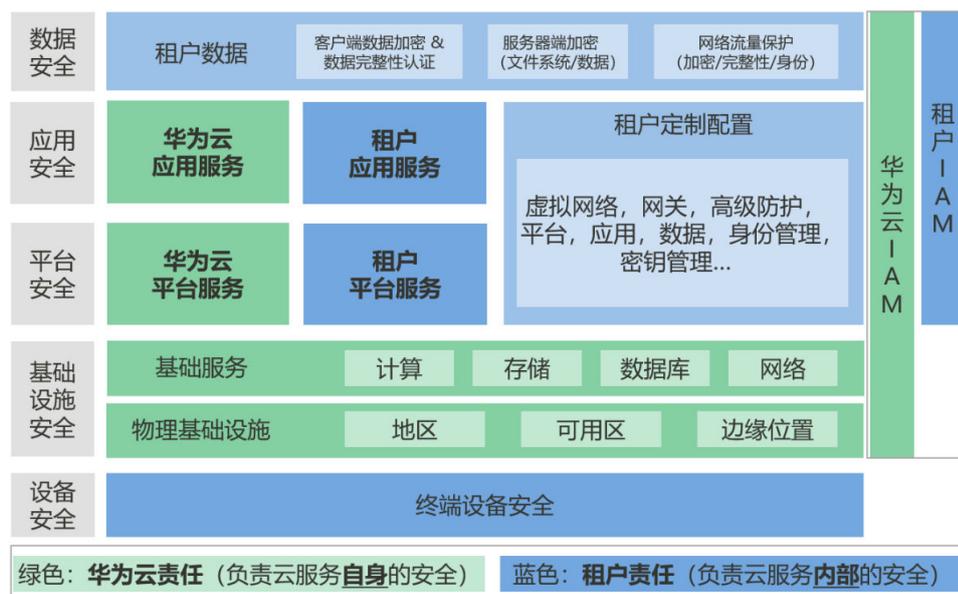
华为云秉承“将对网络和业务安全性保障的责任置于公司的商业利益之上”。针对层出不穷的云安全挑战和无孔不入的云安全威胁与攻击，华为云在遵从法律法规业界标准的基础上，以安全生态圈为护城河，依托华为独有的软硬件优势，构建面向不同区域和行业的完善云服务安全保障体系。

安全性是华为云与您的共同责任，如[图1](#)所示。

- 华为云：负责云服务自身的安全，提供安全的云。华为云的安全责任在于保障其所提供的IaaS、PaaS和SaaS各类各项云服务自身的安全，涵盖华为云数据中心的物理环境设施和运行其上的基础服务、平台服务、应用服务等。这不仅包括华为云基础设施和各项云服务技术的安全功能和性能本身，也包括运维运营安全，以及更广义的安全合规遵从。
- 租户：负责云服务内部的安全，安全地使用云。华为云租户的安全责任在于对使用的IaaS、PaaS和SaaS类各项云服务内部的安全以及对租户定制配置进行安全有效的管理，包括但不限于虚拟网络、虚拟主机和访客虚拟机的操作系统，虚拟防火墙、API网关和高级安全服务，各项云服务，租户数据，以及身份账号和密钥管理等方面的安全配置。

《[华为云安全白皮书](#)》详细介绍华为云安全性的构建思路与措施，包括云安全战略、责任共担模型、合规与隐私、安全组织与人员、基础设施安全、租户服务与租户安全、工程安全、运维运营安全、生态安全。

图 7-1 华为云安全责任共担模型



7.2 资产识别与管理

资产识别

用户在数据资产包括用户上传的数据集以及用户提供的一些个人信息。

数据资产包括但不限于文本、图形、音频、视频、照片、图像、代码、算法、模型等。

资产管理

对于用户上传至Octopus的资产，Octopus会做统一的保存管理。

- 对于文件类型的资产，Octopus会将资产保存在Octopus官方的OBS桶内。
- 对于镜像类型的资产，Octopus会将资产保存在Octopus官方的SWR仓库内。

对于用户提供的一些个人信息，Octopus会保存在数据库中。

7.3 身份认证与访问控制

身份认证

用户访问Octopus的方式有多种，包括Octopus控制台、API，无论访问方式封装成何种形式，其本质都是通过Octopus提供的REST风格的API接口进行请求。

Octopus的接口均需要进行认证鉴权以此来判断是否通过身份认证。通过控制台发出的请求需要通过Token认证鉴权，调用API接口认证鉴权支持Token认证和AK/SK认证两种方式。

访问控制

Octopus作为一个完备的自动驾驶工具链，支持用户对其进行细粒度的权限配置，以达到精细化资源、权限管理之目的。为了支持客户对Octopus的权限做精细化控制，提供了IAM权限控制方面的能力来支撑。

IAM权限控制。

用户使用Octopus的任何功能，都需要通过IAM权限体系进行正确的权限授权。例如：用户希望在Octopus创建训练作业，则该用户必须拥有 "训练服务" 的权限才可以完成操作（无论界面操作还是API调用）。

管理员新创建的用户在没有配置细粒度授权策略时，默认具有Octopus所有权限。如果需要控制用户的详细权限，管理员可以通过IAM为用户组配置细粒度授权策略，使用户获得策略定义的权限，操作对应云服务的资源。基于策略授权时，管理员可以按Octopus的资源类型选择授权范围。详细的资源权限项可以参见API参考中的权限策略和授权项章节。

7.4 数据保护技术

Octopus通过多种数据保护手段和特性，保障存储在Octopus中的数据安全可靠。

表 7-1 表 1 多种数据保护手段

数据保护手段	简要说明
传输加密（HTTPS）	支持HTTP和HTTPS两种传输协议，为保证数据传输的安全性，推荐您使用更加安全的HTTPS协议。
数据备份	支持设置数据库的备份和恢复，来保障数据的可靠性。
权限最小化	临时AK/SK和SecurityToken是系统颁发给用户的临时访问令牌，通过接口设置有效期，范围为15分钟至24小时，过期后需要重新获取。临时AK/SK和SecurityToken遵循权限最小化原则。使用临时AK/SK鉴权时，临时AK/SK和SecurityToken必须同时使用。

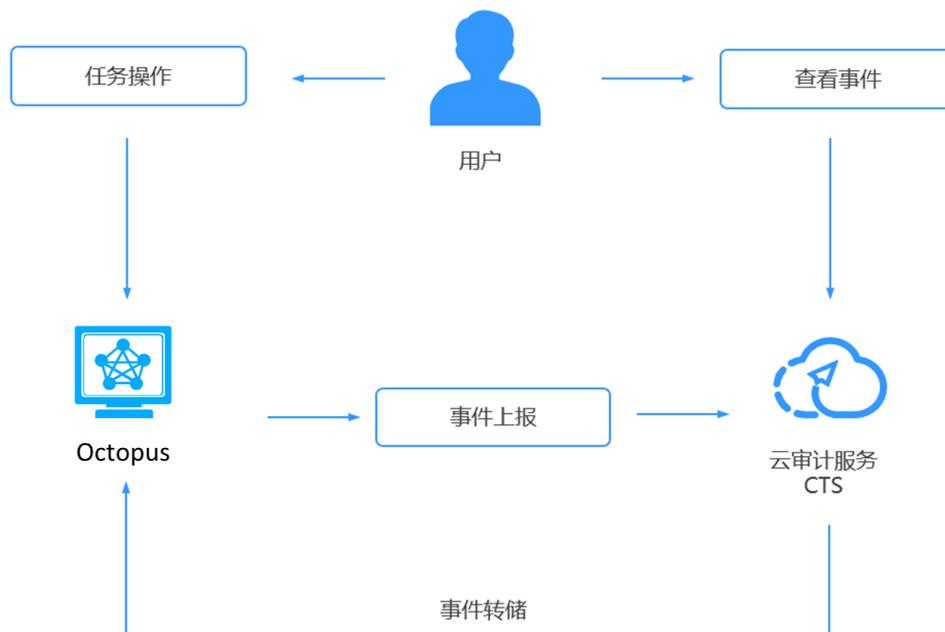
7.5 审计与日志

云审计服务（Cloud Trace Service, CTS），是华为云安全解决方案中专业的日志审计服务，提供对各种云资源操作记录的收集、存储和查询功能，可用于支撑安全分析、合规审计、资源跟踪和问题定位等常见应用场景。

用户开通云审计服务后，CTS可记录八爪鱼的管理事件用于审计。

- CTS的详细介绍和开通配置方法，请参见[CTS快速入门](#)。
- Octopus支持审计的操作事件，请参见[支持云审计的关键操作](#)。
- 查看审计日志，请参见[查看审计日志](#)。

图 7-2 云审计服务



如何查看审计日志

操作场景

在您开启了云审计服务后，系统开始记录云服务器的相关操作。云审计服务管理控制台保存最近7天的操作记录。

本节介绍如何在云审计服务管理控制台查看最近7天的操作记录。

操作步骤

1. 登录管理控制台。
2. 单击管理控制台左上角的📍，选择区域和项目。
3. 单击“服务列表”，选择“管理与监管 > 云审计服务”，进入云审计服务信息页面。
4. 单击左侧导航树的“事件列表”，进入事件列表信息页面。
5. 事件列表支持通过筛选来查询对应的操作事件。当前事件列表支持四个维度的组合查询，详细信息如下：
 - 事件类型、事件来源、资源类型和筛选类型。
在下拉框中选择查询条件。
其中筛选类型选择事件名称时，还需选择某个具体的事件名称。
选择资源ID时，还需选择或者手动输入某个具体的资源ID。
选择资源名称时，还需选择或手动输入某个具体的资源名称。
 - 操作用户：在下拉框中选择某一具体的操作用户，此操作用户指用户级别，而非租户级别。
 - 事件级别：可选项为“所有事件级别”、“normal”、“warning”、“incident”，只可选择其中一项。

- 可在界面右上角选择查询最近七天内任意时间段的操作事件。
 - 6. 展开需要查看的事件，查看详细信息。
 - 7. 在需要查看的记录右侧，单击“查看事件”，弹窗中显示了该操作事件结构的详细信息。
- 更多关于云审计的信息，请参见《[云审计服务用户指南](#)》。

7.6 服务韧性

韧性特指安全韧性，即云服务受攻击后的韧性，不含可靠性、可用性。本章主要阐述 Octopus 服务受入侵的检测响应能力、防抖动的能力、域名合理使用、内容安全检测等能力。

安全防护套件覆盖和使用堡垒机，增强入侵检测和防御能力

Octopus 服务部署主机层、应用层、网络层和数据层的安全防护套件。及时检测主机层、应用层、网络层和数据层的安全入侵行为。

- Octopus 服务涉及对互联网开放的 Web 应用，采用了统一推荐的 Web 安全组件防范 Web 安全风险，并且通过 WAF 进行安全防护。
- 所有承载 Octopus 服务的主机部署了主机安全防护和容器安全产品。包括但不限于华为自研 HSS/CGS 或计算安全平台 CSP。
- Octopus 服务部署了漏洞扫描服务并自行进行例行扫描，能快速发现漏洞并能及时修复。
- Octopus 服务通过统一的安全管控平台对云上资源进行安全运维。
- Octopus 服务部署了态势感知服务，以感知攻击现状，还原攻击历史，同时及时发现合规风险，对威胁告警及时响应。
- Octopus 对存放关键数据的数据库部署了数据库安全服务。

云服务防抖动和遭受攻击后的应急响应/恢复策略

Octopus 服务具备租户资源隔离能力，避免单租户资源被攻击导致爆炸半径大，影响其他租户。

- Octopus 服务具备资源池和隔离能力，避免单租户资源被攻击导致爆炸半径过大风险。
- Octopus 服务定义并维护了性能规格用于自身的抗攻击性。例如：设置 API 访问限制，防止恶意接口调用等场景。
- Octopus 服务在攻击场景下，具备告警能力及自我保护能力。
- Octopus 服务提供了业务异常行为感知能力。
- Octopus 服务具备遭受攻击时的风险控制 and 应急响应能力。例如快速识别恶意租户，恶意 IP。
- Octopus 服务具备攻击流量停止后，快速恢复业务的能力。

云服务域名使用安全及租户内容安全策略

Octopus 服务使用的租户可见域名、租户不可见域名均满足如下安全相关要求，避免了域名使用过程中的合规和钓鱼风险。其中：

租户可见域名：指租户可访问的域名，需要格外重视安全性和合规性。

租户不可见域名：指华为云服务在内网相互调用使用的域名，外部用户无法访问到对应的权威DNS服务器；或者Internet受限访问域名，只允许华为办公网络黄&绿区华为员工及合作方或外包人员访问的域名。

- 华为云基础域名安全使用，避免直接为租户分配基础域名。
- 华为云服务在内网互相调用使用的域名，避免使用外部已备案域名。

7.7 故障恢复

Octopus全球基础设施围绕华为云区域和可用区构建。华为云区域提供多个在物理上独立且隔离的可用区，这些可用区通过延迟低、吞吐量高且冗余性高的网络连接在一起。利用可用区，您可以设计和操作在可用区之间无中断地自动实现故障转移的应用程序和数据库。与传统的单个或多个数据中心基础设施相比，可用区具有更高的可用性、容错性和可扩展性。

Octopus通过对DB的数据进行备份，保证在原数据被破坏或损坏的情况下可以恢复业务。

7.8 更新管理

Octopus支持定期更新或修补OS、应用程序证书、漏洞和配置。建议用户定期更新账户密码。

镜像更新升级

Octopus包含数据资产、数据处理、标注服务、训练服务、仿真服务等功能模块，各模块采用统一的流程提供基础镜像。这些镜像会不定期更新升级，修复已知漏洞。

密码更新

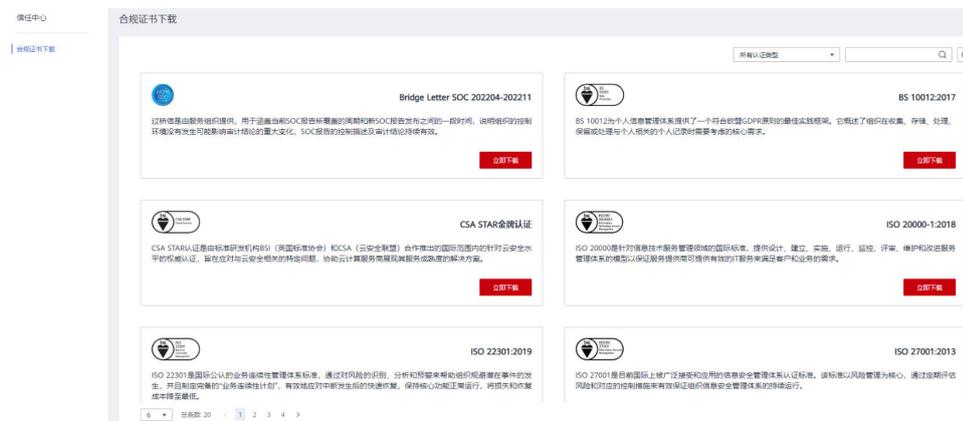
建议定期更新密码，以提升账户的安全性。账户密码的复杂性需根据安全要求进行配置。

7.9 认证证书

合规证书

华为云服务及平台通过了多项国内外权威机构（ISO/SOC/PCI等）的安全合规认证，用户可自行[申请下载](#)合规资质证书。

图 7-3 合规证书下载



资源中心

华为云还提供以下资源来帮助用户满足合规性要求，具体请查看[资源中心](#)。

图 7-4 资源中心



7.10 安全风险知会

自动驾驶云服务中，为了最大化资源利用率，租户的子用户可以共享[计算资源](#)用于运行容器化的作业。这意味着租户的不同子用户的[容器化处理作业](#)可以运行在同一个计算节点上，共享节点的CPU、内存、磁盘、操作系统内核等资源，这里就会存在容器逃逸的风险。

自动驾驶云服务适用于您的子用户是可控的、可信的场合，不适用于子用户不可控、不可信的场合，例如您授权其他客户作为子用户共同使用自动驾驶云服务的情况。请确保您的子用户是可控和可信的。

- 计算资源：您在自动驾驶云服务中订购的通用处理节点、AI处理节点。
- 容器化处理作业：数据处理任务、标注任务、训练任务、推理任务、并行仿真、场景泛化、智驾模型训练、智驾模型推理等。

8 个人数据说明

Octopus自动驾驶服务平台在自动驾驶开发的过程中，在以下场景中需要您同意授权我们收集和使用您的内容数据，其中可能包括个人信息或个人敏感信息，对于这部分数据您有义务根据所适用国家的法律制定必要的用户隐私政策并采取足够的措施以确保用户的个人数据受到充分的保护。

表 8-1 个人数据说明

使用个人数据的场景	数据批导	数据集通用存储	数据合规递送
收集的个人信息项	路采数据包（含有人像的2D图片，音频或视频）	自定义数据集（含有人像的2D图片，音频或视频）	路采数据包（含有人像的2D图片，音频或视频）
个人数据收集的来源和方式	对象存储导入	本地标注 OBS通用存储	数据递送
使用个人数据的目的以及安全保护措施	路采数据导入平台转换为平台支持的opendata格式	用于数据转换，标注，训练，仿真服务	对数据包中的人脸、车牌、点云、高程进行脱敏
个人数据的存留期限与存留策略	用户自行决定存留期限和策略。	用户自行决定存留期限和策略。	合规数据推送到数据服务后，会将源数据删除。
个人数据的销毁方式	用户自行删除	用户自行删除	平台删除
个人数据的导出方式	不涉及	提供数据集下载功能	不涉及
个人数据的导出指导	不涉及	OBS导出	不涉及

9 权限管理

Octopus自动驾驶云服务支持用户对其进行细粒度的权限配置，以达到精细化资源、权限管理之目的。

为了支持客户对Octopus的权限做精细化控制，提供了3个方面的能力来支撑，分别是：**权限**、**委托**和**工作空间**。下面分别讲解。

理解 Octopus 的权限与委托

如果您需要对华为云上购买的Octopus自动驾驶云服务资源，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，您可以在华为云账号中给员工创建IAM用户，并使用策略来控制IAM用户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Octopus的使用权限，但是不希望他们拥有删除通道等高危操作的权限，那么您可以使用IAM为开发人员创建用户，通过授予仅能使用通道，但是不允许删除通道的权限策略，控制他们对通道资源的使用范围；在使用Octopus云资源过程中需要访问用户的其他服务，需要先获得用户的授权，这个动作就是一个“委托”，用户委托Octopus代表自己访问特定的云服务，已完成其在Octopus平台上的操作。

- **权限**：使用Octopus自动驾驶云服务平台上的镜像仓库、运维配置、工作空间、数据资产、数据合规、数据处理、标注服务、训练服务、仿真服务的所有功能，均需要通过IAM权限体系进行正确权限授权。
- **委托**：使用Octopus自动驾驶云服务平台上的智驾模型服务中的模型微调和2D图像生成功能需要访问对象存储服务（OBS），均需要获得用户的委托授权。

IAM是华为云提供权限管理的基础服务，无需付费即可使用，您只需要为您账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](#)》。

说明

如果华为云账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Octopus的其它功能。

Octopus 权限管理

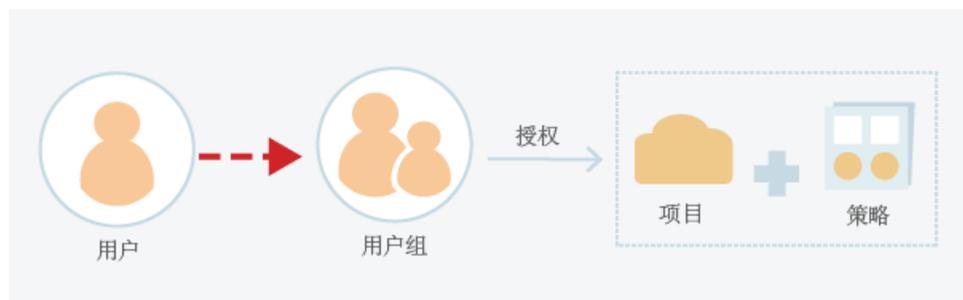
默认情况下，管理员创建的IAM用户没有任何权限，需要将其加入用户组，并给用户组授予策略或角色，才能使得用户组中的用户获得对应的权限，这一过程称为授权。

授权后，用户就可以基于被授予的权限对云服务进行操作。创建用户并授权使用八爪鱼自动驾驶云服务请参考[创建用户并授权使用服务](#)。

注意

Octopus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（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Octopus时，需要先切换至授权区域。

图 9-1 权限授权



IAM在对用户组授权的时候，并不是直接将具体的某个权限进行赋权，而是需要先将权限加入到“策略”当中，再把策略赋给用户组。为了方便用户的权限管理，各个云服务都提供了一些预置的“系统策略”供用户直接使用。如果预置的策略不能满足您的细粒度权限控制要求，则可以通过“自定义策略”来进行精细控制。请参考[创建自定义策略](#)。

如表1所示，包括了Octopus的所有系统权限。

表 9-1 表 1 Octopus 系统策略

策略名称	描述	策略类别	角色/策略内容
Octopus FullAccess	Octopus管理员权限，拥有该权限的用户可以操作并使用所有Octopus服务。	系统策略	Octopus FullAccess策略内容
Octopus CommonOperations	Octopus操作权限，拥有该权限的用户拥有Octopus服务的除智驾模型服务、数据合规递送、创建工作空间、编辑工作空间、删除工作空间之外的所有操作权限。	系统策略	Octopus CommonOperations策略内容

表2列出了Octopus常用操作与系统权限的授权关系，您可以参照该表选择合适的系统权限。

表 9-2 Octopus 常用操作与系统权限的授权关系

服务	功能	操作	Octopus FullAccess	Octopus CommonOperations
镜像仓库	ALL	ALL	√	√
运维配置	ALL	ALL	√	√
标注服务	ALL	ALL	√	√
训练服务	ALL	ALL	√	√
仿真服务	ALL	ALL	√	√
智驾模型服务	ALL	ALL	√	x
数据资产	ALL	ALL	√	√
数据合规	数据合规递送	创建合规订单	√	x
		获取合规订单列表	√	x
		获取合规订单配置信息	√	x
		更新合规订单状态	√	x
		获取合规数据包列表	√	x
		推送合规数据包	√	x
	合规处理模板	创建合规处理模板	√	x
		查询合规处理模板列表	√	x
		查询合规处理模板详情	√	x
		更新合规处理模板	√	x
		删除合规处理模板	√	x
	合规作业	查询合规作业列表	√	x
		查询合规作业详情	√	x
		创建合规作业	√	x

服务	功能	操作	Octopus FullAccess	Octopus CommonOperations
		操作合规作业和作业队列	√	x
		删除合规作业	√	x
数据处理	ALL	ALL	√	√
工作空间	ALL	获取工作空间列表	√	√
		查看工作空间详情	√	√
		创建工作空间	√	x
		编辑工作空间	√	x
		删除工作空间	√	x

更详细的细粒度策略支持的授权项请参考《Octopus API参考》中“[策略及授权项说明](#)”章节。

智驾模型委托授权

图 9-2 委托授权



在使用智驾模型服务模型微调和2D图像生成时，需要访问对象存储服务（OBS），因此需要用户委托Octopus平台访问OBS。

步骤1 登录华为云账号，访问统一身份认证服务。

步骤2 在“统一身份认证服务”控制台，单击“委托 > 创建委托”，填写委托参数。

图 9-3 创建委托

* 委托名称

* 委托类型 普通账号
将账号内资源的操作权限委托给其他华为云账号。
 云服务
将账号内资源的操作权限委托给华为云服务。

* 云服务

* 持续时间

描述

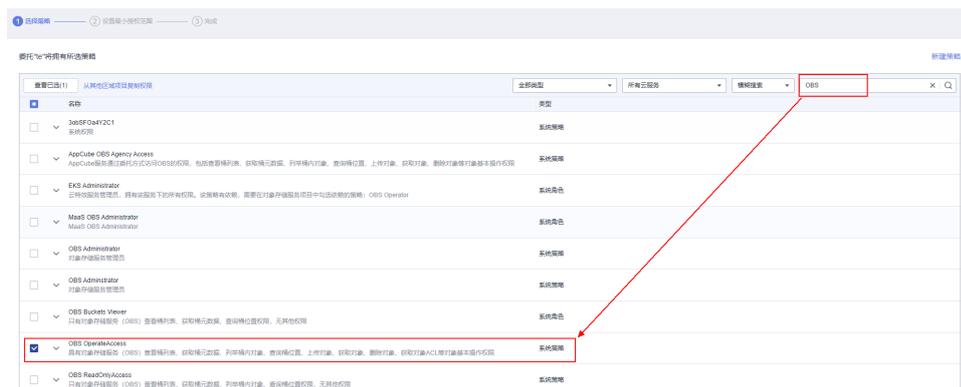
0/255

- 委托名称：自定义名称，不得超过64个字符；建议为：octopus_obs_agency。
- 委托类型：选择“云服务”。
- 云服务：选择“自动驾驶云服务”。
- 持久时间：可自定义持续时间。
- 描述：简要描述委托信息，不包含“@#%\$%^&* < > \”，不得超过255个字符。

步骤3 单击“下一步”，设置最小授权范围。

在模糊搜索，输入“OBS”，选择“OBS OperateAccess”。

图 9-4 设置最小授权范围



步骤4 单击“下一步”，选择授权范围方案。

图 9-5 选择授权范围方案



步骤5 授权后需要等待15-30分钟方可生效。

图 9-6 生效时间提醒



步骤6 单击“完成”，授权完成。

在“授权记录”界面，可查看授权记录。

图 9-7 授权记录



步骤7 访问Octopus自动驾驶云服务，在Octopus控制台左侧菜单分别选择“智驾模型服务 > 模型微调”、“智驾模型服务 > 2D图像生成”，单击“修改”，填写委托名称。

图 9-8 填写委托名称



----结束

工作空间隔离资源

工作空间：是Octopus自动驾驶云服务面向企业客户提供的—个高阶功能，用于进一步将用户的资源划分在多个逻辑隔离的空间中，并支持以空间维度进行访问的权限限定。

工作空间默认有一个“default”空间，在没有创建新的工作空间之前，您操作的所有资源均默认在该空间下。当您创建新的工作空间之后，相当于您拥有了一个新的“Octopus分身”，您可以通过菜单栏的左上角进行工作空间的切换，不同工作空间中的工作互不影响。只有被授权的用户才能访问特定的工作空间（在创建、编辑工作空间进行配置），像数据资产、仿真服务等，均可以借助工作空间做访问的限制。

图 9-9 工作空间



Octopus FullAccess 策略内容

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Action": [
        "octopus:*:*"
      ],
      "Effect": "Allow"
    }
  ]
}
```

Octopus CommonOperations 策略内容

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Action": [
        "octopus:annotation:*:*",
        "octopus:common:*:*",
        "octopus:dataCache:*:*",
        "octopus:dataCalibration:*:*",
        "octopus:dataExpress:create",
        "octopus:dataExpress:delete",
        "octopus:dataExpress:get",
        "octopus:dataExpress:list",
        "octopus:dataExpress:updateBaseInfo",
        "octopus:dataExpress:updateTaskConfig",
        "octopus:dataImportRecord:*:*",
        "octopus:dataJob:*:*",
        "octopus:dataMap:*:*",
        "octopus:dataOverview:get",

```

```
"octopus:dataPackage:*",  
"octopus:dataProcessors:*",  
"octopus:dataReplay:get",  
"octopus:dataScenario:*",  
"octopus:dataset:*",  
"octopus:dataTag:*",  
"octopus:dataVehicle:*",  
"octopus:dataWarehouse:*",  
"octopus:imageRepo:*",  
"octopus:resource:*",  
"octopus:sim:*",  
"octopus:training:*",  
"octopus:workspace:list",  
"octopus:workspace:get"  
  ],  
  "Effect": "Allow"  
}  
]  
}
```