

ModelArts

最佳实践

文档版本 01
发布日期 2024-01-08



版权所有 © 华为云计算技术有限公司 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云计算技术有限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，华为云计算技术有限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 官方案例列表	1
2 第三方案例列表	5
3 LLM	6
3.1 开源大模型基于 ModelArts 的一键推理部署	6
3.2 LLaMA 系列模型基于 ModelArts 的全参数微调训练	11
3.3 LLaMA2-13B (PyTorch) 基于 DevServer 训练推理指导	19
3.3.1 场景介绍	19
3.3.2 准备工作	21
3.3.2.1 准备环境	21
3.3.2.2 准备代码	21
3.3.2.3 准备数据	24
3.3.2.4 准备镜像	24
3.3.3 预训练	27
3.3.3.1 预训练数据处理	27
3.3.3.2 预训练超参配置	28
3.3.3.3 预训练任务	29
3.3.3.4 断点续训练	30
3.3.3.5 查看日志和性能	32
3.3.4 微调训练	33
3.3.4.1 增量预训练	33
3.3.4.1.1 数据处理	33
3.3.4.1.2 增量预训练权重转换	34
3.3.4.1.3 增量预训练超参配置	35
3.3.4.1.4 增量预训练任务	36
3.3.4.1.5 查看性能	37
3.3.4.2 LoRA 微调训练	37
3.3.4.2.1 数据处理	38
3.3.4.2.2 LoRA 微调权重转换	38
3.3.4.2.3 LoRA 微调超参配置	38
3.3.4.2.4 LoRA 微调任务	39
3.3.4.2.5 查看性能	40
3.3.5 推理前的权重合并转换	40

3.3.5.1 权重合并和转换介绍.....	41
3.3.5.2 预训练权重合并及转换.....	41
3.3.5.3 LoRA 微调权重合并及转换.....	42
3.3.6 推理部署 (ATB)	44
3.3.6.1 推理场景说明.....	44
3.3.6.2 推理服务部署.....	45
3.3.6.3 推理性能测试.....	48
3.3.6.3.1 benchmark 方法介绍.....	48
3.3.6.3.2 静态 benchmark.....	48
3.3.6.3.3 动态 benchmark.....	50
3.3.6.4 推理精度测试.....	51
3.3.7 常见问题.....	53
3.3.7.1 访问目录时提示 Permission denied.....	53
3.3.7.2 如何安装依赖包.....	53
3.4 Baichuan-13B (PyTorch) vLLM 基于 DevServer 推理部署.....	53
3.4.1 场景介绍.....	53
3.4.2 安装推理容器环境.....	55
3.4.3 启动 vLLM 服务器服务.....	57
3.4.4 启动 OpenAI 服务器服务.....	59
3.4.5 推理性能测试.....	62
3.4.6 推理精度测试.....	63
3.4.6.1 安装精度测试工具.....	63
3.4.6.2 推理评测.....	64
3.4.7 附录.....	65
3.4.7.1 评测脚本 vllm_api.py.....	65
4 AIGC.....	67
4.1 SDXL 文生图 ComfyUI 插件适配 NPU 指导.....	67
4.2 SDXL PyTorch 文生图 Diffusers 框架适配 NPU 指导.....	72
4.3 SDXL PyTorch 文生图 WebUI 适配 NPU 指导.....	78
4.4 AIGC 工具 tailor 使用指导.....	85
5 数字人.....	91
5.1 数字人 Wav2Lip 适配 PyTorch NPU 指导.....	91
6 业务迁移.....	98
6.1 LLM 训练业务昇腾迁移指导.....	98
6.1.1 场景介绍.....	98
6.1.2 环境准备.....	98
6.1.3 迁移适配.....	99
6.1.4 精度对齐.....	102
6.1.5 性能调优.....	109
6.1.6 常见问题.....	111
6.1.6.1 报错提示 “ RuntimeError: Default process group has not been initialized, please make sure to call init_process_group. ”	111

6.1.6.2 训练运行报错 AttributeError: 'torch_npu.C.NPUDeviceProperties' object has no attribute 'multi_processor_count'.....	112
6.1.6.3 deepspeed 多卡训练报错 TypeError: deepspeed_init() got an unexpected keyword argument 'resume_from_checkpoint'.....	112
6.1.6.4 Huggingface 缓存目录空间不足，出现 OSError: [Errno 122] Disk quota exceeded:.....	113
6.1.6.5 调用 transformers 出现 ImportError: Using the `Trainer` with `PyTorch` requires `accelerate`: Run `pip install --upgrade accelerate`.....	113
6.1.6.6 调用 transformers 出现 ImportError: libcblas.so.3: cannot open shared object file: No such file or directory.....	113
6.1.6.7 transformers 调用 cuda 上的操作，或者执行卡死.....	114
6.2 训练业务昇腾迁移通用指导.....	114
6.2.1 简介.....	114
6.2.2 昇腾迁移快速入门案例.....	115
6.2.3 环境准备.....	115
6.2.4 训练业务代码适配昇腾 PyTorch 代码适配.....	115
6.2.5 PyTorch 迁移精度调优.....	118
6.2.6 PyTorch 迁移性能调优.....	121
6.2.6.1 性能调优总体原则和思路.....	121
6.2.6.2 性能调优五板斧.....	122
6.2.6.3 训练 profiling 工具使用.....	124
6.2.6.4 优化算子下发.....	126
6.2.6.5 优化算子执行.....	127
6.2.7 训练网络迁移总结.....	133
6.2.8 常见问题.....	133
6.3 AIGC 推理业务昇腾迁移指导.....	133
6.3.1 场景介绍.....	134
6.3.2 迁移环境准备.....	134
6.3.3 pipeline 应用准备.....	135
6.3.4 应用迁移.....	138
6.3.4.1 模型适配.....	138
6.3.4.2 pipeline 代码适配.....	143
6.3.5 迁移效果校验.....	148
6.3.6 模型精度调优.....	149
6.3.6.1 场景介绍.....	149
6.3.6.2 精度问题诊断.....	149
6.3.6.3 精度问题处理.....	150
6.3.7 性能调优.....	151
6.3.7.1 单模型性能测试工具 Mindspore lite benchmark.....	151
6.3.7.2 单模型性能调优 AOE.....	151
6.3.8 常见问题.....	153
6.3.8.1 模型转换失败怎么办?	153
6.3.8.2 图片大 Shape 性能劣化严重怎么办?	153
6.3.8.3 同样功能的 PyTorch Pipeline，因为指导要求适配 onnx pipeline，两个 pipeline 本身功能就有差别，如何适配?	153

6.3.8.4 AOE 的自动性能调优使用上完全没有效果怎么办?	154
6.3.8.5 迁移后应用出图效果相比 GPU 无法对齐怎么办?	154
6.3.8.6 模型精度有问题怎么办?	154
6.3.8.7 模型转换失败时如何查看日志和定位原因?	154
6.3.8.8 Stable Diffusion WebUI 如何适配?	155
6.3.8.9 LoRA 适配流是怎么样的?	155
6.3.8.10 数据类型不匹配问题如何处理?	155
6.4 推理业务昇腾迁移通用指导	156
6.4.1 简介	156
6.4.2 昇腾迁移快速入门案例	157
6.4.3 迁移评估	160
6.4.4 环境准备	160
6.4.5 模型适配	163
6.4.5.1 基于 MindSpore Lite 的模型转换	163
6.4.5.2 动态 shape	165
6.4.6 精度校验	166
6.4.7 性能调优	168
6.4.8 迁移过程使用工具概览	171
6.4.9 常见问题	172
6.4.9.1 MindSpore Lite 问题定位指南	172
6.4.9.2 模型转换报错如何查看日志和定位?	172
6.4.9.3 日志提示” Compile graph failed.”	173
6.4.9.4 日志提示 “Custom op has no reg_op_name attr.”	173
6.4.10 附录	174
6.4.10.1 推理业务迁移评估表	174
7 权限管理	179
7.1 ModelArts 权限管理基本概念	179
7.2 权限控制方式	185
7.2.1 IAM	185
7.2.2 委托和依赖	193
7.2.3 工作空间	217
7.3 典型场景配置实践	217
7.3.1 个人用户快速配置 ModelArts 访问权限	217
7.3.2 配置 ModelArts 基本使用权限	221
7.3.2.1 场景描述	221
7.3.2.2 Step1 创建用户组并加入用户	222
7.3.2.3 Step2 为用户配置云服务使用权限	224
7.3.2.4 Step3 为用户配置 ModelArts 的委托访问授权	229
7.3.2.5 Step4 测试用户权限	230
7.3.3 给予用户配置开发环境基本使用权限	231
7.3.4 给予用户配置训练作业基本使用权限	240
7.3.5 给予用户配置部署上线基本使用权限	246

7.3.6 管理员和开发者权限分离.....	252
7.3.7 查看所有子账号的 Notebook 实例.....	260
7.3.8 使用 Cloud Shell 登录训练容器.....	261
7.3.9 限制用户使用公共资源池.....	263
7.3.10 给予用户配置文件夹级的 SFS Turbo 访问权限.....	265
7.4 FAQ.....	269
7.4.1 使用 ModelArts 时提示“权限不足”，如何解决？.....	269
8 自动学习.....	275
8.1 口罩检测（使用新版自动学习实现物体检测应用）.....	275
8.2 垃圾分类（使用新版自动学习实现图像分类）.....	281
9 开发环境.....	289
9.1 使用算法套件快速完成水表读数识别.....	289
9.2 基于 SFS 创建、迁移和管理 Conda 虚拟环境.....	300
9.3 本地开发的 MindSpore 模型迁移至云上训练.....	303
9.4 使用 ModelArts VS Code 插件进行模型开发（Ascend）.....	321
9.4.1 方案概述.....	321
9.4.2 资源规划.....	321
9.4.3 操作步骤.....	323
10 模型训练.....	332
10.1 使用 AI Gallery 的订阅算法实现花卉识别.....	332
10.2 使用自定义算法构建模型（手写数字识别）.....	338
10.3 示例：从 0 到 1 制作自定义镜像并用于训练（Pytorch+CPU/GPU）.....	357
10.4 示例：从 0 到 1 制作自定义镜像并用于训练（MPI+CPU/GPU）.....	364
10.5 示例：从 0 到 1 制作自定义镜像并用于训练（Horovod-PyTorch+GPU）.....	373
10.6 示例：从 0 到 1 制作自定义镜像并用于训练（MindSpore+GPU）.....	385
10.7 示例：从 0 到 1 制作自定义镜像并用于训练（Tensorflow+GPU）.....	397
10.8 示例：从 0 到 1 制作自定义镜像并用于训练（MindSpore+Ascend）.....	404
10.8.1 场景描述.....	404
10.8.2 Step1 创建 OBS 桶和文件夹.....	405
10.8.3 Step2 准备脚本文件并上传至 OBS 中.....	405
10.8.4 Step3 制作自定义镜像.....	417
10.8.5 Step4 上传镜像至 SWR.....	420
10.8.6 Step5 在 ModelArts 上创建 Notebook 并调试.....	422
10.8.7 Step6 在 ModelArts 上创建训练作业.....	422
11 推理部署.....	424
11.1 免费体验：一键完成商超商品识别模型部署.....	424
11.2 从 0-1 制作自定义镜像并创建 AI 应用.....	429
11.3 推理服务访问公网.....	433
11.4 推理服务端到端运维.....	435
11.5 使用自定义引擎创建 AI 应用.....	438
11.6 使用大模型创建 AI 应用部署在线服务.....	442

11.7 第三方推理框架迁移到推理自定义引擎.....	445
11.8 推理服务支持虚拟私有云（VPC）直连的高速访问通道.....	455
11.9 WebSocket 在线服务全流程开发.....	459
12 专属资源池训练.....	464
12.1 资源选择推荐.....	464
12.2 步骤总览.....	466
12.3 资源购买.....	468
12.4 基本配置.....	469
12.4.1 权限配置.....	470
12.4.1.1 配置 IAM 权限.....	470
12.4.1.2 配置 ModelArts 委托权限.....	473
12.4.1.3 配置 SWR 组织权限.....	474
12.4.1.4 测试用户权限.....	474
12.4.2 创建网络.....	475
12.4.3 专属资源池 VPC 打通.....	476
12.4.4 ECS 服务器挂载 SFS Turbo 存储.....	477
12.4.5 在 ECS 中创建 ma-user 和 ma-group.....	478
12.4.6 obsutil 安装和配置.....	478
12.4.7（可选）工作空间配置.....	478
12.5 调试与训练.....	479
12.5.1 单机单卡.....	479
12.5.1.1 线下容器镜像构建及调试.....	479
12.5.1.2 上传镜像.....	482
12.5.1.3 上传数据和算法至 OBS（首次使用时需要）.....	484
12.5.1.4 使用 Notebook 进行代码调试.....	490
12.5.1.5 创建训练任务.....	495
12.5.1.6 监控资源.....	496
12.5.2 单机多卡.....	497
12.5.2.1 线下容器镜像构建及调试.....	497
12.5.2.2 上传镜像.....	497
12.5.2.3 上传数据和算法至 SFS（首次使用时需要）.....	497
12.5.2.4 使用 Notebook 进行代码调试.....	500
12.5.2.5 创建训练任务.....	503
12.5.3 多机多卡.....	505
12.5.3.1 线下容器镜像构建及调试.....	505
12.5.3.2 上传镜像.....	505
12.5.3.3 上传数据至 OBS（首次使用时需要）.....	505
12.5.3.4 上传算法至 SFS.....	506
12.5.3.5 使用 Notebook 进行代码调试.....	507
12.5.3.6 创建训练任务.....	507
12.6 FAQ.....	509
12.6.1 CUDA 和 CUDNN.....	509

12.6.1.1 Vnt1 机型软件版本建议.....	509
12.6.1.2 CUDA Compatibility 如何使用?	509
12.6.1.3 专属池驱动版本如何升级?	509
12.6.2 CloudShell 调试方法.....	510
12.6.3 run.sh 脚本测试 ModelArts 训练整体流程.....	510
12.6.4 ModelArts 环境挂载目录说明.....	511
12.6.5 如何查看训练环境变量.....	512
12.6.6 infiniband 驱动的安装.....	513
12.6.7 Tensorboard 的使用.....	514
12.6.8 如何保证训练和调试时文件路径保持一致.....	521
13 ModelArts+HiLens.....	522
13.1 手势识别技能开发 (ModelArts+华为 HiLens)	522

1 官方案例列表

在最佳实践文档中，提供了针对多种场景、多种AI引擎的ModelArts案例，方便您通过如下案例快速了解使用ModelArts完成AI开发的流程和操作。

配置 ModelArts 使用权限（基础教程）

样例	对应功能	场景	说明
场景描述	IAM权限配置、全局配置	为子用户配置权限	当一个华为云账号下需创建多个IAM用户（即子用户）时，可参考此样例，为IAM用户赋予使用ModelArts所需的权限。避免IAM用户因权限问题导致使用时出现异常。

自动学习样例列表（基础教程）

表 1-1 自动学习样例列表

样例	对应功能	场景	说明
口罩检测	自动学习	物体检测	基于AI Gallery口罩数据集，使用ModelArts自动学习的物体检测算法，识别图片中的人物是否佩戴口罩。
垃圾分类	自动学习	图像分类	该案例基于华为云AI开发者社区AI Gallery中的数据资产，让零AI基础的开发者完成“图像分类”的AI模型的训练和部署。

开发工具样例列表（高阶教程）

表 1-2 Notebook 样例列表

样例	镜像	对应功能	场景	说明
本地开发的MindSpore模型迁移至云上训练	MindSpore	PyCharm ToolKit工具	目标检测	本案例介绍如何在本地进行MindSpore模型开发，并将模型迁移至ModelArts训练。
使用ModelArts VS Code插件进行模型开发（Ascend）	MindSpore	VS Code Toolkit工具	目标检测	本案例以Ascend Model Zoo为例，介绍如何通过VS Code插件及ModelArts Notebook进行云端数据调试及模型开发。

表 1-3 算法套件样例列表

样例	镜像	对应功能	场景	说明
使用算法套件快速完成水表读数识别	PyTorch	Notebook	图像识别	本案例提供了一个水表表盘读数识别的样例，使用ModelArts的自研分割算法(ivgSegmentation)和开源OCR算法(mmOCR)完成水表读数识别项目，并使用算法开发套件将其部署为华为云在线服务。

模型训练-预置算法样例列表（基础教程）

表 1-4 预置算法样例列表

样例	镜像	对应功能	场景	说明
使用AI Gallery的订阅算法实现花卉识别	TensorFlow	AI Gallery> 预置算法	图像分类	此样例介绍如何从AI Gallery，订阅一个预置算法resnet_v1_50，同时使用算法训练得到模型，最终将模型部署为在线服务的端到端指导。

模型训练-自定义算法样例列表（高阶教程）

表 1-5 自定义算法样例列表

样例	镜像	对应功能	场景	说明
使用自定义算法构建模型（手写数字识别）	PyTorch	自定义算法	手写数字识别	使用用户自己的算法，训练得到手写数字识别模型，并部署后进行预测。
示例：从 0 到 1 制作自定义镜像并用于训练（Pytorch+CPU/GPU）	PyTorch	镜像制作自定义镜像训练	-	此案例介绍如何从0到1制作镜像，并使用该镜像在ModelArts平台上进行训练。镜像中使用的AI引擎是PyTorch，训练使用的资源是CPU或GPU。
示例：从 0 到 1 制作自定义镜像并用于训练（MPI+CPU/GPU）	MPI	镜像制作自定义镜像训练	-	此案例介绍如何从0到1制作镜像，并使用该镜像在ModelArts平台上进行训练。镜像中使用的AI引擎是MPI，训练使用的资源是CPU或GPU。
示例：从 0 到 1 制作自定义镜像并用于训练（Horovod-PyTorch+GPU）	Horovod-PyTorch	镜像制作自定义镜像训练	-	此案例介绍如何从0到1制作镜像，并使用该镜像在ModelArts平台上进行训练。镜像中使用的AI引擎是Horovod-PyTorch，训练使用的资源是GPU。
示例：从 0 到 1 制作自定义镜像并用于训练（MindSpore+GPU）	MindSpore	镜像制作自定义镜像训练	-	此案例介绍如何从0到1制作镜像，并使用该镜像在ModelArts平台上进行训练。镜像中使用的AI引擎是MindSpore，训练使用的资源是GPU。
示例：从 0 到 1 制作自定义镜像并用于训练（Tensorflow+GPU）	Tensorflow	镜像制作自定义镜像训练	-	此案例介绍如何从0到1制作镜像，并使用该镜像在ModelArts平台上进行训练。镜像中使用的AI引擎是Tensorflow，训练使用的资源是GPU。
示例：从 0 到 1 制作自定义镜像并用于训练（MindSpore+Ascend）	MindSpore	镜像制作自定义镜像训练	-	此案例介绍如何从0到1制作镜像，并使用该镜像在ModelArts平台上进行训练。镜像中使用的AI引擎是MindSpore，训练使用的资源是NPU。

推理部署（基础教程）

表 1-6 推理部署列表

样例	镜像	对应功能	场景	说明
免费体验：一键完成商超商品识别模型部署	-	在线服务	物体检测	此案例以“商超商品识别”模型为例，完成从AI Gallery订阅模型，到ModelArts一键部署为在线服务的免费体验过程。

推理部署（高阶教程）

表 1-7 推理部署列表

样例	镜像	对应功能	场景	说明
从0-1制作自定义镜像并创建AI应用	-	镜像制作 模型推理部署	-	此案例介绍在ModelArts平台使用自定义镜像导入模型的样例，帮助您快速熟悉平台的使用方法

2 第三方案例列表

📖 说明

第三方案例来源为[华为云开发者社区“云驻计划”](#)。由于ModelArts产品的持续更新和迭代，第三方案例中的界面和步骤可能因时效性而与最新产品有所差异，仅供学习和参考。

表 2-1 第三方案例列表

分类	文章名称	作者
自动学习	2步打通ModelArts和Astro实现AI应用落地	胡琦
开发环境	想不想让一张静态的照片动起来	林欣
	基于TensorFlow训练轻量化ssdlite_mbv2人脸手机检测模型	AI练习生
	基于ModelArts的手写数字识别	AXYZdong
	AI 文字编辑图片 instruct-pix2pix 案例	AXYZdong
推理部署	上线二维码检测识别服务	林欣
	使用ModelArts对8类常见生活垃圾进行分类	福州司马懿
	使用ModelArts搭建"花卉种类识别"服务	福州司马懿

3 LLM

3.1 开源大模型基于 ModelArts 的一键推理部署

本文为您介绍如何通过AI Gallery订阅开源大模型并在ModelArts控制台上进行推理部署。

场景介绍

ModelArts针对当前主流的开源大模型做了昇腾芯片和MindSpore引擎的适配工作，用户可以使用昇腾Snt9b芯片进行模型的训练或推理部署。

本文以[ChatGLM2-6B-推理](#)模型为例，介绍如何在AI Gallery上订阅模型，并一键部署到ModelArts上进行推理预测。

约束限制

本教程中推荐的模型，推理部署建议使用“西南-贵阳一”Region上的昇腾Snt9b芯片。

操作流程

开始使用如下样例前，请务必按[准备工作](#)指导完成必要操作。

1. **Step1 申请并订阅模型**：在AI Gallery中订阅开源大模型。
2. **Step2 部署模型并推理预测**：在ModelArts上部署模型，并进行推理预测。
3. **Step3 清理资源**：体验完成后，停止服务，避免不必要的资源浪费。

准备工作

开始进行体验前，请仔细阅读以下准备工作，并完成必要操作。

- 已注册华为帐号并开通华为云，进行了实名认证，且在使用ModelArts前检查帐号状态，帐号不能处于欠费或冻结状态。
 - [注册华为帐号并开通华为云](#)
 - [进行实名认证](#)

Step1 申请并订阅模型

开源大模型共享在AI Gallery中。您可以前往AI Gallery，免费申请订阅此模型。

1. 在AI Gallery的模型页面，申请模型使用权限，此处以**ChatGLM2-6B-推理**为例。单击“申请”，根据提示提交联系方式。预计1-2个工作日完成订阅权限开通。
2. 权限申请通过后，在模型详情页，单击“订阅”，阅读并勾选同意《数据安全与隐私风险承担条款》和《华为云AI Gallery服务协议》，单击“继续订阅”。订阅模型完成后，页面的“订阅”按钮显示为“已订阅”。

图 3-1 已订阅模型



3. 在模型详情页，单击“前往控制台”，并在弹出的“选择云服务区域”窗口选择“西南-贵阳一”，单击“确定”，跳转至ModelArts控制台的“AI应用管理 > AI应用 > 我的订阅”页面。
4. 在ModelArts控制台的“AI应用管理 > AI应用 > 我的订阅”页面，找到刚订阅“ChatGLM2-6B”模型并选中，在页面下方的“版本列表”中，可以看到系统正在同步该模型。当模型的状态显示为“就绪”时，表示模型已经订阅成功，可以部署在线服务，如图3-2。

图 3-2 模型同步

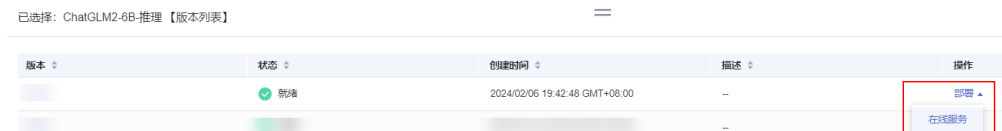


Step2 部署模型并推理预测

模型订阅成功后，可将此模型部署为在线服务，进行预测。

1. 在“AI应用管理 > AI应用 > 我的订阅”页面，选中订阅的资产，在下方的“版本列表”中单击“部署 > 在线服务”跳转至部署页面。

图 3-3 部署模型



说明

由于模型版本在持续迭代更新，此处创建在线服务时，请选择最新版本。

2. 在部署页面，选择“资源池”为“公共资源池”，其他参数可以使用默认值。

图 3-4 部署在线服务



关键参数解释如下：

- “名称”：自定义一个在线服务的名称，也可以使用默认值。
 - “资源池”：当前订阅的模型仅支持选择“公共资源池”。
 - “AI应用来源”：系统会自动选择“我的订阅”。
 - “选择AI应用及版本”：系统会自动选择订阅的模型和版本。
 - “计算节点规格”：系统会自动选择Ascend单卡，例如：“Ascend: 1*xxx”，1表示单卡。
 - “计算节点个数”：系统自动设置为“1”，表示当前仅支持单机单卡，暂不支持分布式推理。
3. 参数配置完成后，单击“下一步”，确认规格参数后，单击“提交”，提示在线服务的部署任务提交成功。

图 3-5 提交部署任务



📖 说明

- 如果在线服务提交失败，提示“ModelArts.3520: 在线服务数量超限，限制为20”，表示当前已部署的在线服务数量超出配额，请参考FAQ处理。
4. 单击“查看服务详情”，进入“在线服务”详情页面，等待服务状态变为“运行中”时，表示服务部署成功。

图 3-6 等待服务部署成功



- 5. 在“预测”页签，在输入栏输入JSON Prompt请求体，如{"prompt":"Hello world"}，单击“预测”查看预测结果。

注意

因为模型规模较大，部署状态变成“运行中”后，建议等待10-20分钟，后台编译成功后再进行预测。

图 3-7 预测输入及结果



Step3 清理资源

体验结束后，建议暂停或删除服务，避免占用资源，造成资源浪费。

- 停止在线服务：在“在线服务”列表，单击对应服务操作列的“更多 > 停止”。
- 删除在线服务：在“在线服务”列表，单击对应服务操作列的“更多 > 删除”。

3.2 LLaMA 系列模型基于 ModelArts 的全参数微调训练

本文为您介绍如何通过AI Gallery订阅LLaMA系列算法，并在ModelArts使用昇腾Snt9b芯片进行算法的训练微调和模型的推理部署。

场景介绍

LLaMA是基于Transformer结构的自回归语言模型，提供多种尺寸的LLaMA参数。表3-1中提供的算法均基于MindSpore引擎做了适配，适用于昇腾Snt9b芯片。

表 3-1 开源大模型（用于训练）

序号	模型	引擎	AI Gallery地址
1	Llama-7B 训练	MindSpore	https://developer.huaweicloud.com/develop/aigallery/algo/detail?id=8e3e9e04-d439-4267-854d-9c800e3672fc
2	Llama2-7B 训练	MindSpore	https://developer.huaweicloud.com/develop/aigallery/algo/detail?id=d4ca115d-9de4-4a36-86d5-e059bf147649
3	Llama-13B 训练	MindSpore	https://developer.huaweicloud.com/develop/aigallery/algo/detail?id=8956ed2f-0fc3-40dc-bad4-027e3653c341
4	Llama2-13B 训练	MindSpore	https://developer.huaweicloud.com/develop/aigallery/algo/detail?id=23d07690-654e-4ee5-8b78-68f9543477cd

本文以“Llama-7B”算法为例，介绍如何在AI Gallery上订阅算法，并通过ModelArts进行微调训练和模型推理部署。表3-1中提供的算法在ModelArts上的使用流程一致，均可参考此教程操作。

约束限制

本教程中推荐的模型，算法训练和部署模型时建议使用“西南-贵阳一”Region上的昇腾Snt9芯片。

本教程中使用的是开源数据集，主要用于体验在ModelArts上训练和部署大模型的流程。客户的实际业务开展需要根据数据集格式要求匹配自己的业务数据来做精细的调参。

产品当前也提供了训练好的模型，您可以参考[开源大模型基于ModelArts的一键推理部署](#)文档操作直接订阅模型进行推理。

操作流程

开始使用如下样例前，请务必按[准备工作](#)指导完成必要操作。

1. **Step1 准备算法**: 在AI Gallery中订阅算法。
2. **Step2 准备训练数据**: 准备训练数据。创建OBS桶和文件夹, 并将训练数据上传到OBS中。
3. **Step3 全量微调训练**: 对算法进行全量微调。
4. **Step4 部署模型并推理预测**: 训练完成后, 部署模型并进行推理预测。
5. **Step5 清理资源**: 运行完成后, 停止服务并删除OBS中的数据, 避免不必要的资源浪费。

准备工作

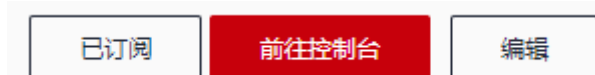
开始进行体验前, 请仔细阅读以下准备工作, 并完成必要操作。

- 已注册华为帐号并开通华为云, 进行了实名认证, 且在使用ModelArts前检查帐号状态, 帐号不能处于欠费或冻结状态。
 - [注册华为帐号并开通华为云](#)
 - [进行实名认证](#)
- 准备一个“西南-贵阳一” Region上的OBS桶。创建OBS桶和文件夹的操作指导请参见[创建桶](#)。OBS桶所在区域和ModelArts使用区域必须都选择“西南-贵阳一”。

Step1 准备算法

1. 在AI Gallery的算法页面, 申请算法使用权限。具体地址如[表3-1](#)所示, 此处以[Llama-7B训练](#)为例。单击“申请”, 根据提示提交联系方式。预计1-2个工作日完成订阅权限开通。
2. 权限申请通过后, 在算法详情页, 单击右侧的“订阅”, 根据界面提示完成算法订阅。订阅算法完成后, 页面的“订阅”按钮显示为“已订阅”。

图 3-8 已订阅算法



3. 单击详情页的“前往控制台”, 此时弹出“选择云服务区域”对话框, 选择“西南-贵阳一”区域, 然后再单击“确定”。

图 3-9 选择云服务区域“西南-贵阳一”



页面将自动跳转至ModelArts的“算法管理 > 我的订阅”中同步对应的算法。

Step2 准备训练数据

以Llama-7B为例，全量微调训练使用的是开源的wiki2048数据集。下载数据集之后，需要将开源数据集转化为MindSpore可以读取的数据格式，然后上传到OBS桶中，用于后续的算法训练。

1. 下载WikiText2数据集到用户本地电脑，并转化数据集格式为MindSpore可以读取的数据格式（xxx.mindrecord.db和xxx.mindrecord），具体操作请参见[文档](#)。
2. 请参考以下要求创建OBS桶中的文件夹，并上传数据到OBS桶中，用于后续的算法微调训练。

OBS文件夹目录要求如下：

```
{OBS桶} # OBS对象桶，用户可以自定义名称，例如：llm-mindspore-ma
  -{OBS文件夹} # OBS文件夹，用于存放训练输入数据，用户可以自定义名称，例如：
wiki2048
  - wiki2048.mindrecord.db # 训练数据集
  - wiki2048.mindrecord # 训练数据集
  -{OBS文件夹} #训练输出路径，用于存放训练生成的模型文件等，用户可以自定义名称，
例如： output
  -{OBS文件夹} #作业日志路径，用于存放训练日志，用户可以自定义名称，例如：
log
```

📖 说明

本文中使用的是开源数据集，主要用于跑通流程和体验，客户的实际业务开展需要根据数据集格式要求匹配自己的业务数据来做精细的调参。

Step3 全量微调训练

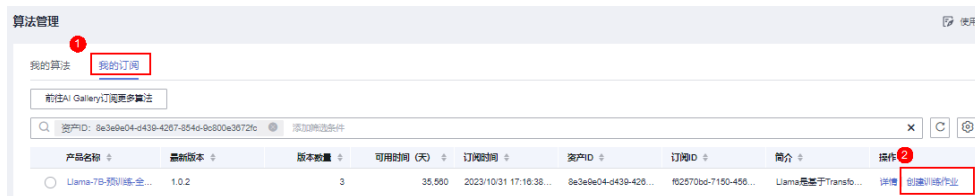
准备好训练数据后，在ModelArts控制台的“算法管理>我的订阅”页面中，使用订阅的“Llama-7B”算法创建训练作业，进行模型全量微调训练。

1. 进入“算法管理 > 我的订阅”页面，选中的“Llama-7B”算法，在页面右侧的“操作”栏中单击“创建训练作业”。

📖 说明

由于模型版本在持续迭代更新，此处创建训练作业时，请选择最新版本。

图 3-10 创建训练作业



2. 进入创建训练作业页面，参考如下说明填写关键参数。
 - “创建方式 > 我的订阅”：系统默认选择订阅的算法，请勿随意修改。
 - “输入”：选择“数据存储位置”，然后从弹出窗口中选择[Step2 准备训练数据](#)中传到OBS的wiki2048数据集，例如：obs://llm-mindspore-ma/wiki2048，其中llm-mindspore-ma是OBS桶名称，需替换成用户自己的桶。
 - “超参”：设置“run_mode”参数为“finetune”，表示全量微调模式。设置“remote_save_url”参数为OBS中存放训练输出模型的路径，例如：

obs://llm-mindspore-ma/output，其中llm-mindspore-ma是OBS桶名称，需替换成用户自己的桶。

- “资源池”：选择“公共资源池”。
- “资源类型”：选择“Ascend”。
- “规格”：选择8卡规格，例如：“Ascend: 8*Ascend-Snt9b(64GB) | ARM: 192 核 1536GB”，卡的规格以控制台实际为准，此处仅为举例。
- “计算节点个数”：建议采用默认值1。
- “作业日志路径”：选择OBS中创建的训练日志存放路径，例如：obs://llm-mindspore-ma/log，其中llm-mindspore-ma是OBS桶名称，需替换成用户自己的桶。
- 其他参数保持默认值即可。

图 3-11 训练作业参数-训练输入

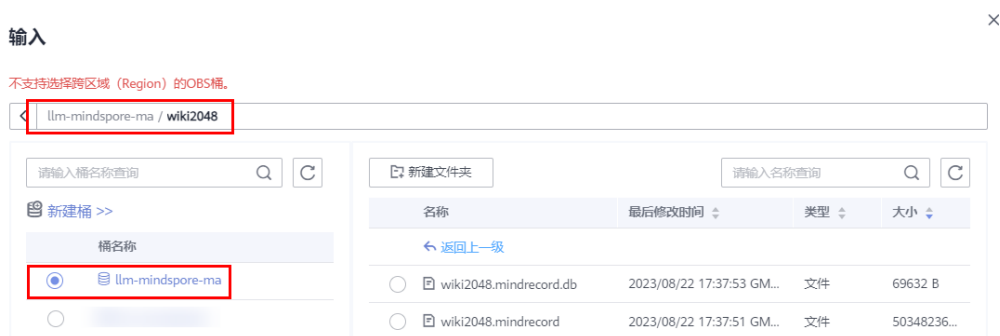


图 3-12 超参设置

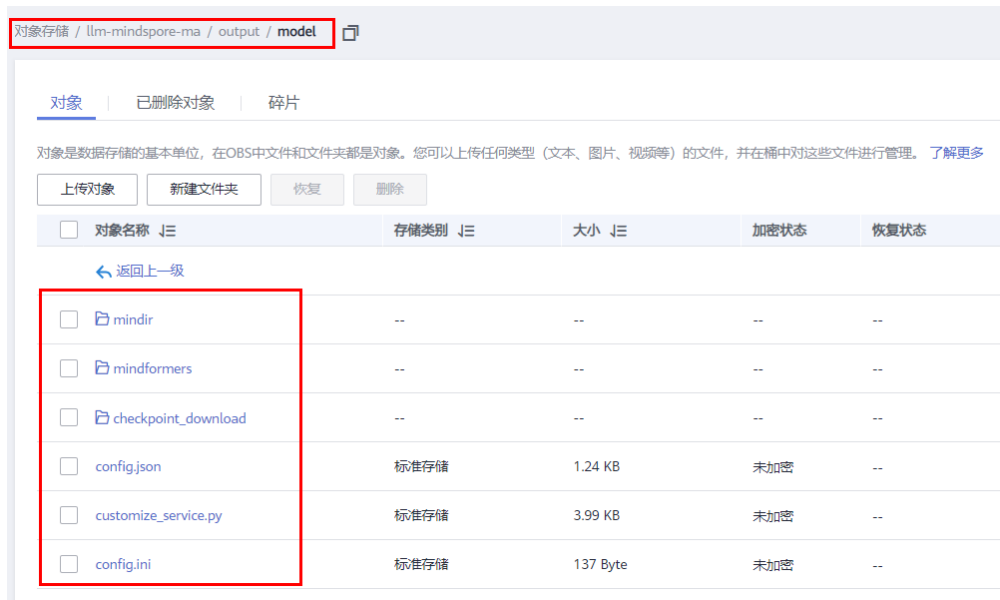


图 3-13 资源池设置



3. 参数填写完成后，单击“提交”，根据界面提示确认规格，单击“确定”，完成训练作业创建。
4. 进入“训练管理 > 训练作业”页面，等待训练作业运行完成。训练作业运行需要30分钟左右，请耐心等待。您可以单击训练作业名称，进入详情页面，了解训练作业的“配置信息”、“日志”、“资源占用情况”等信息。
5. 当训练作业的状态变更为“已完成”时，表示已运行结束。此时，可以在超参“remote_save_url”设置的OBS输出路径下，找到对应的模型文件夹model，如图3-14所示。确认该路径下存在有模型部署文件，即存在mindir文件夹、config文件、推理脚本文件customize_service.py等。

图 3-14 训练输出模型

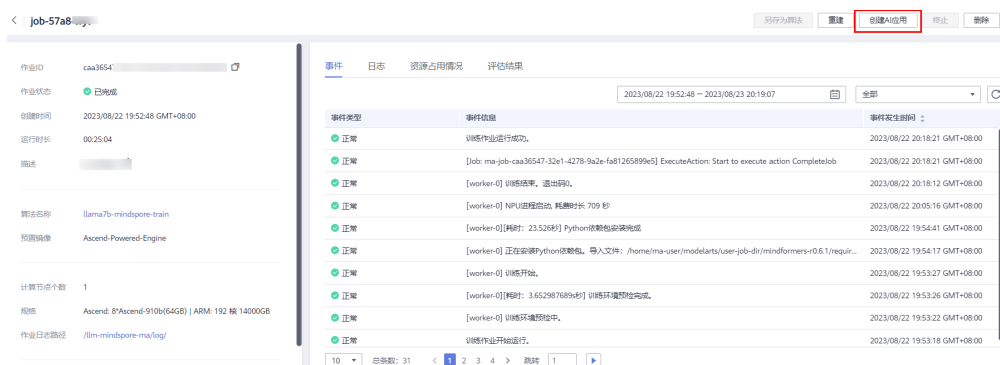


Step4 部署模型并推理预测

本节将详细说明模型推理部署的过程。

1. 在训练任务详情页的右上角，单击“创建AI应用”，进入AI应用创建页面。

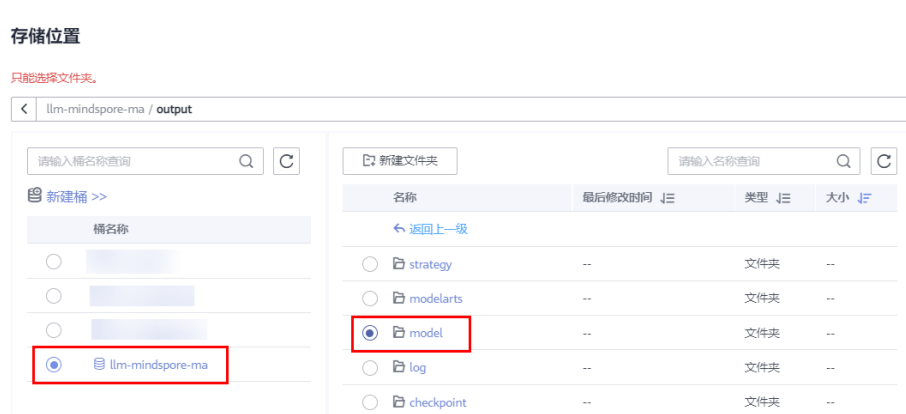
图 3-15 创建 AI 应用



2. 在AI应用创建页面，设置如下参数。

- “元模型来源”：选择“从对象存储服务（OBS）中选择”。
- “选择元模型”：从OBS中选择一个模型包。即Step3 全量微调训练中输出的模型存储路径，例如：`obs://llm-mindspore-ma/output/model`，其中llm-mindspore-ma是OBS桶名称，需替换成用户自己的桶。

图 3-16 选择元模型



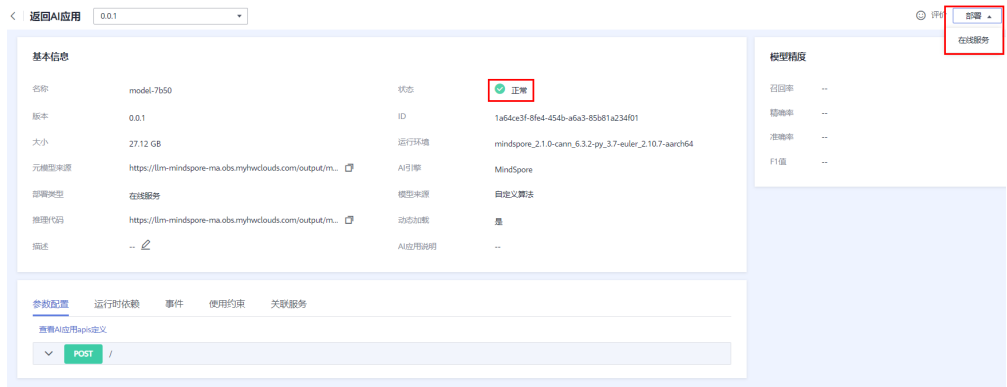
- “AI引擎”：默认是“MindSpore”，无需修改。
- “动态加载”：必须勾选，否则会出现模型太大无法导入的情况。
- “推理代码”：系统会自动加载推理代码路径。
- 其他参数保持默认值。

图 3-17 创建 AI 应用



3. 单击“立即创建”，跳转到AI应用列表页，查看AI应用状态，当状态变为“正常”，表示AI应用创建成功。此时单击AI应用名称，进入AI应用详情页面，可以查看AI应用详情信息。

图 3-18 AI 应用创建成功



4. 在AI应用详情页面，单击右上角“部署 > 在线服务”，进入服务部署页面，参考如下说明填写关键参数，完成服务部署。
 - “名称”：自定义一个在线服务的名称，也可以使用默认值。
 - “资源池”：选择“公共资源池”。
 - “AI应用来源”：选择“我的AI应用”。
 - “选择AI应用及版本”：选系统会自动选择。
 - “计算节点规格”：默认选择“Ascend: 1*xxx”，1表示单卡。
 - “计算节点个数”：默认设置为“1”，无需修改。当前仅支持单机单卡，暂不支持分布式推理。

- 其他参数可使用默认值。

图 3-19 部署服务



5. 参数配置完成后，单击“下一步”，确认规格参数后，单击“提交”，提示在线服务的部署任务提交成功。

图 3-20 提交部署任务



📖 说明

如果在线服务提交失败，提示“ModelArts.3520: 在线服务服务数量超限，限制为20”，表示当前已部署的在线服务数量超出配额，请参考FAQ处理。

6. 单击“查看服务详情”，进入“在线服务”详情页面，等待服务状态变为“运行中”时，表示服务部署成功。
7. 在服务详情页面，单击“预测”页签，在输入栏输入JSON Prompt请求体，如{"prompt": "What are the three primary colors?"}，进行服务预测。

Step5 清理资源

如果不再需要使用此模型及在线服务，建议清除相关资源，避免产生不必要的费用和资源浪费。

- 在“在线服务”页面，“停止”或“删除”刚创建的在线服务。

- 在“AI应用管理”页面，“删除”刚创建的AI应用。
- 在“训练作业”页面，“删除”运行结束的训练作业。
- 进入OBS，删除本示例使用的OBS桶及文件夹，以及文件夹的文件。

3.3 LLama2-13B（PyTorch）基于 DevServer 训练推理指导

3.3.1 场景介绍

Llama2（Large Language Model Meta AI）是由Meta AI发布的新一代大语言系列模型，上下文长度由Llama的2048扩展到了4096，可以理解和生成更长的文本。

本文档以Llama2-13B为例，利用PyTorch训练框架和华为自研昇腾Snt9b硬件，为用户提供开箱即用的预训练和全量微调方案。同时利用昇腾高性能算子库Ascend Transformer Boost（ATB）、适配昇腾平台的大模型推理服务Text Generation Inference（TGI）和华为自研昇腾Snt9b硬件，为用户提供开箱即用的推理部署方案，包括推理的性能和精度测试等，为用户提供端到端的大模型解决方案，帮助用户使能大模型业务。

方案概览

本方案介绍了在ModelArts的DevServer上使用昇腾计算资源开展Llama2-13B模型的训练、微调、推理部署的详细过程。完成本方案的部署，需要先联系您所在企业的华为方技术支持购买DevServer资源。

本方案目前仅适用于企业客户。

操作流程

图 3-21 操作流程图

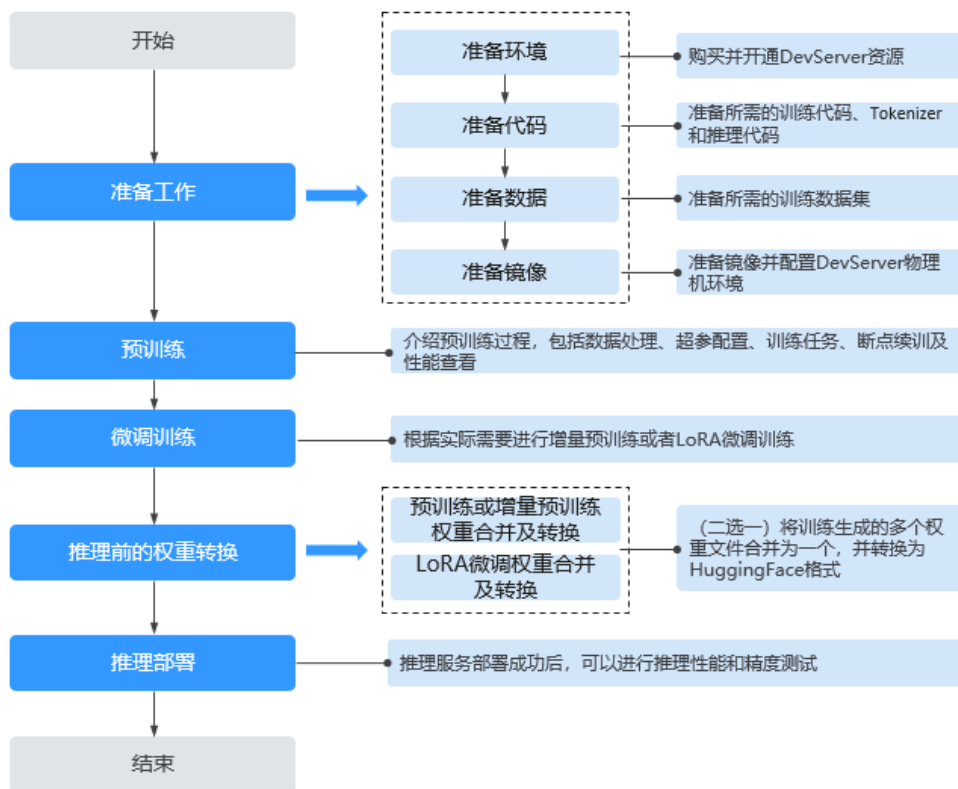


表 3-2 操作任务流程说明

阶段	任务	说明
准备工作	准备环境	本教程案例是基于ModelArts Lite DevServer运行的，需要购买并开通DevServer资源。
	准备代码	准备AscendSpeed训练代码、分词器Tokenizer和推理代码。
	准备数据	准备训练数据，可以用Alpaca数据集，也可以使用自己准备的数据集。
	准备镜像	准备训练模型适用的容器镜像。
预训练	预训练	介绍如何进行预训练，包括训练数据处理、超参配置、训练任务、断点续训及性能查看。
微调训练	增量预训练	介绍如何进行增量预训练。
	LoRA微调训练	介绍如何进行LoRA微调训练。

阶段	任务	说明
推理前的权重转换 (二选一)	训练权重合并及转换	推理前, 需要将预训练或增量预训练产生的多个权重文件合并为一个, 并转换为HuggingFace格式。
	LoRA权重合并及转换	推理前, 需要将LoRA微调训练产生的多个权重文件合并为一个, 并转换为HuggingFace格式。
推理部署	部署推理服务	介绍如何部署并启动推理服务。
	推理性能测试	介绍如何验证推理性能, 包括静态和动态benchmark。
	推理精度测试	介绍如何测试推理精度, 并获取评测结果。

3.3.2 准备工作

3.3.2.1 准备环境

本文档中的模型运行环境是ModelArts Lite的DevServer。请参考本文档要求准备DevServer机器。

资源规格要求

计算规格: 单机训练需要使用单机8卡, 多机训练需要使用2机16卡。

硬盘空间: 至少200GB。

昇腾资源规格:

- Ascend: 1*ascend-snt9b表示昇腾单卡。
- Ascend: 8*ascend-snt9b表示昇腾8卡。

约束限制

推荐使用“西南-贵阳一”Region上的DevServer和昇腾Snt9b资源。

购买并开通 DevServer 资源

请参考[DevServer资源开通](#), 购买DevServer资源, 并确保机器已开通, 密码已获取, 能通过SSH登录, 不同机器之间网络互通。

📖 说明

购买DevServer资源时如果无可选资源规格, 需要联系华为云技术支持申请开通。

当容器需要提供服务给多个用户, 或者多个用户共享使用该容器时, 应限制容器访问Openstack的管理地址(169.254.169.254), 以防止容器获取宿主机的元数据。具体操作请参见[禁止容器获取宿主机元数据](#)。

3.3.2.2 准备代码

本教程中用到的训练推理代码和如下表所示, 请提前准备。

获取数据及代码

表 3-3 准备代码

代码包名称	代码说明	下载地址
AscendCloud-3rdLLM-6.3.902-xxx.zip	包含了本教程中使用到的模型训练代码、推理部署代码和推理评测代码。代码包具体说明请参见 代码目录介绍 。 AscendSpeed是用于模型并行计算的框架，其中包含了许多模型的输入处理方法。	获取路径： Support 网站 。 说明 如果没有软件下载权限，请联系您所在企业的华为方技术支持下载获取。
权重和词表文件	包含了本教程使用到的HuggingFace原始权重文件和Tokenizer。 标记器(Tokenizer)是NLP管道的核心组件之一。它们有一个目的：将文本转换为模型可以处理的数据。模型只能处理数字，因此标记器(Tokenizer)需要将文本输入转换为数字数据。	llama-2-13b-chat-hf 这个路径下既有权重，也有Tokenizer，全部下载。具体内容参见 权重和词表文件介绍 。

代码目录介绍

AscendCloud-3rdLLM-6.3.902代码包结构介绍如下：

6.3.902-Ascend

```

├── llm_evaluation #推理评测代码包
│   ├── benchmark_eval #精度评测
│   ├── benchmark_tools #性能评测
│   └── llm_train #模型训练代码包
│       ├── AscendSpeed #基于AscendSpeed的训练代码
│       ├── Megatron-LM #三方依赖: megatron
│       ├── ModelLink #基于AscendSpeed的训练代码
│       └── scripts/ #训练需要的启动脚本
    
```

本教程需要使用到的训练相关代码存放在AscendCloud-3rdLLM-6.3.902/llm_train/AscendSpeed目录下，具体文件介绍如下：

```

├── llm_train #模型训练代码包
│   ├── AscendSpeed #基于AscendSpeed的训练代码
│   │   ├── Megatron-LM #三方依赖megatron
│   │   ├── ModelLink #基于AscendSpeed的训练代码，数据预处理脚本
│   │   └── scripts/ #训练需要的启动脚本，调用ModelLink
│   │       ├── tools #权重转换脚本
│   │       └── llama2 #Llama2的训练代码
│   │           ├── llama2.sh #Llama2训练主脚本
│   │           └── lora-llama2-13b.sh #LoRA微调训练脚本，执行前需要修改参数，执行时会调用
llama2.sh脚本
│   │           ├── pretrain-llama2-13b.sh #预训练脚本，执行前需要修改参数，执行时会调用
llama2.sh脚本
│   │           ├── retrain-llama2-13b.sh #断点续训练脚本，执行前需要修改参数，执行时会调用
llama2.sh脚本
│   │           └── sft-llama2-13b.sh #增量预训练脚本，执行前需要修改参数，执行时会调用
llama2.sh脚本
    
```

本教程需要使用到的推理任务评测相关代码存放在llm_evaluation目录下，关键文件介绍如下：

```

├── llm_evaluation #推理评测代码包
│   └── benchmark_eval #精度评测
    
```

```

├── config
│   ├── config.json # 请求的参数，根据实际启动的服务来调整
│   └── mmlu_subject_mapping.json # 数据集配置
├── evaluators
│   ├── evaluator.py # 数据集数据预处理方法集
│   ├── model.py # 发送请求的模块，在这里修改请求响应。目前支持vllm.openai, atb的tgi模板
│   ├── eval_test.py # 启动脚本，建立线程池发送请求，并汇总结果
│   └── service_predict.py # 发送请求的服务。支持vllm的openai, atb的tgi模板
├── ...
├── benchmark_tools #性能评测
│   ├── benchmark.py # 可以基于默认的参数跑完静态benchmark和动态benchmark
│   ├── benchmark_parallel.py # 评测静态性能脚本
│   ├── benchmark_serving.py # 评测动态性能脚本
│   ├── benchmark_utils.py # 抽离的工具集
│   ├── generate_datasets.py # 生成自定义数据集的脚本
│   ├── requirements.txt # 第三方依赖
│   └── ...

```

权重和词表文件介绍

下载完毕后的HuggingFace原始权重文件包含以下内容，此处以llama2-13B为例。

```

llama2-13B
├── config.json
├── generation_config.json
├── gitattributes.txt
├── LICENSE.txt
├── Notice.txt
├── pytorch_model-00001-of-00003.bin
├── pytorch_model-00002-of-00003.bin
├── pytorch_model-00003-of-00003.bin
├── pytorch_model.bin.index.json
├── README.md
├── special_tokens_map.json
├── tokenizer_config.json
├── tokenizer.json
├── tokenizer.model
└── USE_POLICY.md

```

工作目录结构如下

```

${workdir} ( 例如/home/ma-user/ws )
├── llm_train
│   ├── AscendSpeed #代码目录
│   ├── Megatron-LM #训练依赖的三方模型库
│   ├── ModelLink #AscendSpeed代码目录
│   └── scripts/ #训练启动脚本
├── # 以下目录结构自己创建
│   ├── datasets
│   │   ├── data #原始数据集
│   │   ├── alpaca #预训练时预处理后的数据存放地址
│   │   └── alpaca-ft #微调训练（包括增量预训练和Lora微调训练）时预处理后的数据地址
│   ├── tokenizers
│   │   └── llama2-13b-hf #tokenizer及HuggingFace原始权重文件
│   ├── weight
│   │   └── llama2-13b-ckpt #HuggingFace格式转换AscendSpeed后权重文件

```

上传代码到工作环境

1. 使用root用户以SSH的方式登录DevServer。
2. 将AscendSpeed代码包AscendCloud-3rdLLM-6.3.902-xxx.zip上传到\${workdir}目录下并解压缩，如：/home/ma-user/ws目录下，以下都以/home/ma-user/ws为例。
unzip AscendCloud-3rdLLM-6.3.902-xxx.zip #解压缩，XXX表示时间戳
3. 上传tokenizers文件到工作目录中的/home/ma-user/ws/tokenizers/llama2-13b-hf目录。

具体步骤如下：

进入到`${workdir}`目录下，如：`/home/ma-user/ws`。

```
cd /home/ma-user/ws
mkdir -p tokenizers/llama2-13b-hf
将权重和词表文件放置此处。
```

3.3.2.3 准备数据

本教程使用到的训练数据集是Alpaca数据集。您也可以自行准备数据集。

Alpaca 数据

本教程使用到的训练数据集是Alpaca数据集。Alpaca是由OpenAI的text-davinci-003引擎生成的包含52k条指令和演示的数据集。这些指令数据可以用来对语言模型进行指令调优，使语言模型更好地遵循指令。

- 预训练数据集下载：<https://huggingface.co/datasets/tatsu-lab/alpaca/resolve/main/data/train-00000-of-00001-a09b74b3ef9c3b56.parquet>，数据大小：24M左右。
- 增量预训练、LoRA微调训练数据集下载：http://github.com/tatsu-lab/stanford_alpaca/blob/main/alpaca_data.json，数据大小：22M左右。

自定义数据

用户也可以自行准备训练数据。数据要求如下：

使用标准的.json格式的数据，通过设置`--json-key`来指定需要参与训练的列。

请注意huggingface中的数据集具有如下**this**格式。可以使用`-json-key`标志更改数据集文本字段的名称，默认为`text`。在维基百科数据集中，它有四列，分别是`id`、`url`、`title`和`text`。可以指定`-json-key`标志来选择用于训练的列。

```
{
  'id': '1',
  'url': 'https://simple.wikipedia.org/wiki/April',
  'title': 'April',
  'text': 'April is the fourth month...'
}
```

经下载的原始数据存放在`/home/ma-user/ws/datasets/data`目录下。具体步骤如下：

1. 进入到`/home/ma-user/ws/`目录下。
2. 创建目录“`datasets/data`”，并将原始数据放置在此处。

```
mkdir -p datasets/data
```

数据存放参考目录结构如下：

```
${workdir} ( 例如/home/ma-user/ws )
├── datasets
│   ├── data #原始数据集
│   ├── train-00000-of-00001-a09b74b3ef9c3b56.parquet #预训练原始数据集
│   └── alpaca_data.json #微调原始数据集
```

3.3.2.4 准备镜像

准备训练Llama2-13B模型适用的容器镜像，包括获取镜像地址，了解镜像中包含的各类固件版本，配置DevServer物理机环境操作。

镜像地址

本教程中用到的训练和推理的基础镜像地址和配套版本关系如下表所示，请提前了解。

表 3-4 基础容器镜像地址：

镜像用途	镜像地址
训练&推理基础镜像	西南-贵阳一：swr.cn-southwest-2.myhuaweicloud.com/atelier/pytorch_2_1_ascend:pytorch_2.1.0-cann_7.0.0-py_3.9-hce_2.0.2312-aarch64-snt9b-20240312154948-219655b

表 3-5 模型镜像版本

模型	版本
CANN	7.0.1
PyTorch	2.1.0

Step1 检查环境

- SSH登录机器后，检查NPU设备检查。运行如下命令，返回NPU设备信息。

```
npu-smi info
```

如出现错误，可能是机器上的NPU设备没有正常安装，或者NPU镜像被其他容器挂载。请先正常[安装NPU设备和驱动](#)，或释放被挂载的NPU。
- 检查docker是否安装。

```
docker -v #检查docker是否安装
```

如尚未安装，运行以下命令安装docker。

```
yum install -y docker-engine.aarch64 docker-engine-selinux.noarch docker-runc.aarch64
```
- 配置IP转发，用于容器内的网络访问。执行以下命令查看net.ipv4.ip_forward配置项的值，如果为1，可跳过此步骤。

```
sysctl -p | grep net.ipv4.ip_forward
```

如果net.ipv4.ip_forward配置项的值不为1，执行以下命令配置IP转发。

```
sed -i 's/net.ipv4.ip_forward=0/net.ipv4.ip_forward=1/g' /etc/sysctl.conf
```

```
sysctl -p | grep net.ipv4.ip_forward
```

Step2 获取训练镜像

建议使用官方提供的镜像部署训练服务。

镜像地址{image_url}为：

西南-贵阳一：swr.cn-southwest-2.myhuaweicloud.com/atelier/pytorch_2_1_ascend:pytorch_2.1.0-cann_7.0.0-py_3.9-hce_2.0.2312-aarch64-snt9b-20240312154948-219655b

```
docker pull {image_url}
```

Step3 启动容器镜像

启动容器镜像前请先按照参数说明修改\${}中的参数。可以根据实际需要增加修改参数。启动容器命令如下。

```
container_work_dir="/home/ma-user/ws" # 容器内挂载的目录
work_dir="/home/ma-user/ws" # 宿主机挂载目录, 存放了代码、数据、权重
container_name="ascendspeed" # 启动的容器名称
image_name="${container_name}" # 启动的镜像ID
docker run -itd \
  --device=/dev/davinci0 \
  --device=/dev/davinci1 \
  --device=/dev/davinci2 \
  --device=/dev/davinci3 \
  --device=/dev/davinci4 \
  --device=/dev/davinci5 \
  --device=/dev/davinci6 \
  --device=/dev/davinci7 \
  --device=/dev/davinci_manager \
  --device=/dev/devmm_svm \
  --device=/dev/hisi_hdc \
  -v /usr/local/bin/npu-smi:/usr/local/bin/npu-smi \
  -v /usr/local/dcmi:/usr/local/dcmi \
  -v /usr/local/Ascend/driver:/usr/local/Ascend/driver \
  --cpus 192 \
  --memory 1000g \
  --shm-size 32g \
  --net=host \
  -v ${work_dir}:${container_work_dir} \
  --name ${container_name} \
  $image_name \
  /bin/bash
```

参数说明:

- --name \${container_name} 容器名称, 进入容器时会用到, 此处可以自己定义一个容器名称, 例如ascendspeed。
- -v \${work_dir}:\${container_work_dir} 代表需要在容器中挂载宿主机的目录。宿主机和容器使用不同的文件系统。work_dir为宿主机中工作目录, 目录下存放着训练所需代码、数据等文件。container_work_dir为要挂载到的容器中的目录。为方便两个地址可以相同。
- \${image_name} 为docker镜像的ID, 在宿主机上可通过docker images查询得到。

通过容器名称进入容器中。

```
docker exec -it ${container_name} bash
#配置镜像源, 例如配置清华源
pip install -i https://pypi.tuna.tsinghua.edu.cn/simple pybind11==2.11.1

#安装三方依赖库
pip install -e git+https://gitee.com/ascend/DeepSpeed.git@v0.9.2#egg=deepspeed_npu
#安装其他依赖库
#进入scripts目录并安装 requirements.txt文件的依赖库。
cd /home/ma-user/ws/6.3.902-Ascend/llm_train/AscendSpeed/scripts
s
pip install requirements.txt
```

执行如下命令统一文件属组。启动容器时默认用户为ma-user用户, 使用其他属组如root用户上传的数据和文件等, 可能会存在权限不足的问题, 因此需要执行如下命令统一文件属主。

```
sudo chown -R ma-user:ma-group ${container_work_dir}
```

```
# ${container_work_dir}:/home/ma-user/ws 容器内挂载的目录
```

例如：

```
sudo chown -R ma-user:ma-group /home/ma-user/ws
```

3.3.3 预训练

3.3.3.1 预训练数据处理

训练前需要对数据集进行预处理，转化为.bin和.idx格式文件，以满足训练要求。

Alpaca 数据处理

数据预处理脚本preprocess_data.py存放在代码包的“llm_train\AscendSpeed\ModelLink\”目录中，脚本具体内容如下。

```
cd /home/ma-user/ws/AscendCloud-3rdLLM-6.3.902/llm_train/AscendSpeed/ModelLink
python tools/preprocess_data.py \
  --input ${path}/train-00000-of-00001-a09b74b3ef9c3b56.parquet \
  --output-prefix ${path}/alpaca/llama2-13B/alpaca \
  --tokenizer-type PretrainedFromHF \
  --tokenizer-name-or-path ${path}/tokenizers/llama2-13b-hf \
  --tokenizer-not-use-fast \
  --json-keys text
```

参数说明：

- - input: 数据集的存放路径，本案例中\${path}的路径为/home/ma-user/ws/datasets。
- - output-prefix: 处理后的数据集保存路径+数据集名称前缀（例如: alpaca）
- - tokenizer-type: tokenizer的类型，可选项有['BertWordPieceLowerCase', 'BertWordPieceCase', 'GPT2BPETokenizer', 'PretrainedFromHF']，一般为PretrainedFromHF。
- - tokenizer-name-or-path: tokenizer的存放路径
- - json-keys: space separate listed of keys to extract from json，默认使用text，不需要修改。

数据预处理后输出的训练数据如下：

- alpaca_text_document.bin
- alpaca_text_document.idx

训练的时指定的数据路径为\${path}/alpaca/llama2-13B/alpaca_text_document，不加文件类型后缀。

具体操作步骤如下：

1. 进入容器中，创建数据集存放目录datasets。

```
cd /home/ma-user/ws/ #进入/home/ma-user/ws/目录
mkdir datasets #创建datasets目录
```
2. 创建数据处理后的输出目录/home/ma-user/ws/datasets/alpaca/llama2-13B/。

```
cd /home/ma-user/ws/datasets #进入/home/ma-user/ws/datasets目录
mkdir -p alpaca/llama2-13B
```
3. 将获取到的Alpaca预训练数据集传到上一步创建的目录中。如还未下载数据集，请参考[准备数据](#)获取。

4. 进入 “/home/ma-user/ws/AscendCloud-3rdLLM-6.3.902/llm_train/AscendSpeed/ModelLink/” 目录，在代码目录中执行preprocess_data.py脚本处理数据。

此处提供一段实际的数据处理代码示例如下。

```
python tools/preprocess_data.py \
--input /home/ma-user/ws/datasets/data/train-00000-of-00001-a09b74b3ef9c3b56.parquet \
--output-prefix /home/ma-user/ws/datasets/alpaca/llama2-13B/alpaca \
--tokenizer-type PretrainedFromHF \
--tokenizer-name-or-path /home/ma-user/ws/tokenizers/llama2-13b-hf \
--tokenizer-not-use-fast \
--json-keys text
```

5. 数据处理完后，在/home/ma-user/ws/datasets/alpaca/llama2-13B/目录下生成alpaca_text_document.bin和alpaca_text_document.idx文件。

图 3-22 处理后的数据

```
(PyTorch-2.1.0) [root@devserver-bms-6cella93 alpaca]# cd llama2-13B/
(PyTorch-2.1.0) [root@devserver-bms-6cella93 llama2-13B]# ll
total 53704
-rw----- 1 root root 26453100 Jan  8 10:26 alpaca_text_document.bin
-rw----- 1 root root  1040082 Jan  8 10:26 alpaca_text_document.idx
```

自定义数据

如果是用户自己准备的数据集，可以使用Ascendspeed代码仓中的转换工具将json格式数据集转换为训练中使用的.idx + .bin格式。

```
#示例:
#1.将准备好的json格式数据集存放于/home/ma-user/ws/datasets/data目录下: data.json
#2.运行转换脚本
cd /home/ma-user/ws/llm_train/AscendSpeed/ModelLink/
python tools/preprocess_data.py --input data.json \ #需要转换的数据集路径
--output-prefix datasets/data \ #转换后存放的数据集路径
--tokenizer-type PretrainedFromHF \
--tokenizer-name-or-path llama2-13b-hf \
--tokenizer-not-use-fast \
--json-keys text
#3.执行完成后在 datasets文件夹中可以得到 data_text_document.idx 与data_text_document.bin 两个文件
```

3.3.3.2 预训练超参配置

本章节介绍预训练前的超参配置，可以根据实际需要修改。

预训练脚本pretrain-llama2-13b.sh，存放在AscendCloud-3rdLLM-6.3.902/llm_train/AscendSpeed/scripts/llama2目录下。训练前，可以根据实际需要修改超参配置。

表 3-6 超参配置

参数	值	参数说明
DATA_PATH	/home/ma-user/ws/datasets/alpaca/llama2-13B/alpaca_text_document	必填。训练时指定的输入数据路径。一般为数据地址/处理后的数据前缀名，不加文件类型后缀。 请根据实际规划修改。
TOKENIZER_PATH	/home/ma-user/ws/tokenizers/llama2-13b-hf	必填。tokenizer保存地址。

参数	值	参数说明
SAVE_PATH	\$PWD/ckpt	中间保存结果，包含训练日志。
SAVE_CKPT_PATH	\${SAVE_PATH}/ckpt-llama2-13b	必填。训练ckpt保存地址。
MODEL_TYPE	13B	模型加载类型，默认为13B。
TRAIN_ITEERS	2000	训练迭代周期。根据实际需要修改。
MBS	4	流水线并行中一个micro batch所处理的样本量。在流水线并行中，为了减少气泡时间，会将一个step的数据切分成多个micro batch。 默认值4。
GBS	64	训练中所有机器一个step所处理的样本量。影响每一次训练迭代的时长，建议值单机64，双机128。
TP	8	张量并行。
PP	1	流水线并行。
lr	0.00015	学习率，非必填，默认值3.0e-4
RUN_TYPE	pretrain	训练脚本类型：pretrain。

3.3.3.3 预训练任务

修改预训练脚本pretrain_llama2_13b.sh，并执行预训练任务。

Step1 修改预训练脚本

1. 执行命令如下，进入/home/ma-user/ws/AscendCloud-3rdLLM-6.3.902/llm_train/AscendSpeed/代码目录。
cd /home/ma-user/ws/AscendCloud-3rdLLM-6.3.902/llm_train/AscendSpeed/ #进入/home/ma-user/ws/AscendCloud-3rdLLM-6.3.902/llm_train/AscendSpeed/目录

2. 执行如下命令修改Llama2-13b的预训练启动脚本。

```
#llama2-13b 预训练启动脚本
vim scripts/llama2/pretrain-llama2-13b.sh
```

修改脚本中以下内容。

```
DATASET_PATH #预处理后的数据地址：*注意：一般为数据地址/数据前缀名
TOKENIZER_PATH #tokenizer地址
SAVE_PATH #中间保存结果 包含日志
SAVE_CKPT_PATH #训练ckpt保存地址
TRAIN_ITEERS=2000 #训练迭代周期，根据自己实际要求修改
MBS=4 #流水线并行中一个micro batch所处理的样本量
GBS=64 #训练中所有机器一个step所处理的样本量，建议值单机64，双机128
TP=8 #张量并行
PP=1 #流水线并行，单机建议为1，双机建议值为2
```

3. 修改完后，保存退出。

```
!wq
```

Step2 启动训练脚本

单机启动

以llama2-13b为例，单机训练启动命令如下。在/home/ma-user/ws/AscendCloud-3rdLLM-6.3.902/llm_train/AscendSpeed/代码目录下执行。

```
bash scripts/llama2/pretrain-llama2-13b.sh
```

多机启动

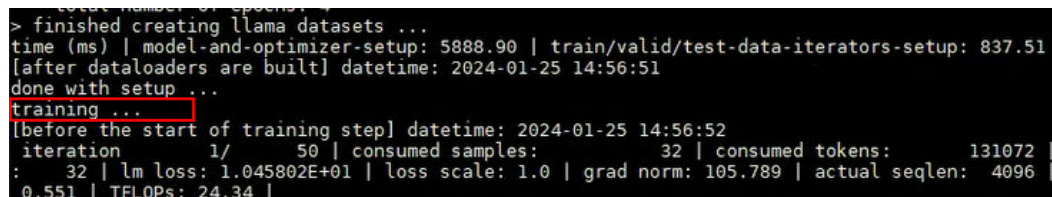
以llama2-13b为例，多台机器执行训练启动命令如下。多机启动需要在每个节点上执行。

```
# master_ip:主节点IP地址，指定一个节点为主节点
# nnodes: 节点总数，如为双机，则写2
# 在节点0机器上执行，当前节点id，一般从0开始，(0 1 2 3)
bash scripts/llama2/pretrain-llama2-13b.sh <master_ip> <nnodes> 0
...
# 在节点n机器上执行
bash scripts/llama2/pretrain-llama2-13b.sh <master_ip> <nnodes> n
```

等待模型载入

执行训练启动命令后，等待模型载入，当出现“training”关键字时，表示开始训练。训练过程中，训练日志会在最后的Rank节点打印。

图 3-23 等待模型载入



```
> finished creating llama datasets ...
time (ms) | model-and-optimizer-setup: 5888.90 | train/valid/test-data-iterators-setup: 837.51
[after dataloaders are built] datetime: 2024-01-25 14:56:51
done with setup ...
training ...
[before the start of training step] datetime: 2024-01-25 14:56:52
iteration   1/   50 | consumed samples:      32 | consumed tokens:   131072 |
:   32 | lm loss: 1.045802E+01 | loss scale: 1.0 | grad norm: 105.789 | actual seqLen: 4096 |
0.551 | TFLOPs: 24.34 |
```

更多查看训练日志和性能操作，请参考[查看日志和性能](#)章节。

如果需要使用断点续训练能力，请参考[断点续训练](#)章节修改训练脚本。

3.3.3.4 断点续训练

断点续训练是指因为某些原因导致训练作业还未完成就被中断，下一次训练可以在上一次的训练基础上继续进行。这种方式对于需要长时间训练的模型而言比较友好。

断点续训练是通过checkpoint机制实现。checkpoint机制是在模型训练的过程中，不断地保存训练结果（包括但不限于EPOCH、模型权重、优化器状态、调度器状态）。即便模型训练中断，也可以基于checkpoint接续训练。

当需要从训练中断的位置接续训练，只需要加载checkpoint，并用checkpoint信息初始化训练状态即可。用户需要在代码里加上reload ckpt的代码，使能读取前一次训练保存的预训练模型。

原有训练参数配置[表3-6断点续训练](#)中新加MODEL_PATH参数，并修改TRAIN_ITERS参数和。

表 3-7 断点续训练修改参数

参数	参考值	参数说明
MODEL_PATH	\${SAVE_PATH}/ckpt-llama2-13b	加载上一步预训练后保存的权重文件。
TRAIN_ITERATIONS	3000	训练周期，必须大于上次保存训练的周期次数
RUN_TYPE	retrain	训练脚本类型：retrain，表示断点续训练。

断点续训练操作过程

llama2-13b的断点续训脚本retrain-llama2-13b.sh，存放在“AscendCloud-3rdLLM-6.3.902/llm_train/AscendSpeed/scripts/llama2”目录下。

1. 执行命令如下，进入AscendSpeed代码目录。

```
cd .. #退出当前目录
cd /home/ma-user/ws/AscendCloud-3rdLLM-6.3.902/llm_train/AscendSpeed/ #进入/home/ma-user/ws/AscendCloud-3rdLLM-6.3.902/llm_train/AscendSpeed/目录
```

2. 执行如下命令修改Llama2-13b的断点续训练脚本。

```
vim scripts/llama2/retrain-llama2-13b.sh
```

断点续训练参数配置如下：

```
# data args
PWD=`pwd`
datasets_PATH=/home/ma-user/ws/datasets/alpaca/llama2-13B/alpaca_text_document #训练数据输入路径，不加文件类型后缀
TOKENIZER_PATH=/home/ma-user/ws/tokenizers #TOKENIZER存放路径
SAVE_PATH=$PWD/ckpt #训练过程文件保存路径，包括日志
SAVE_CKPT_PATH=${SAVE_PATH}/ckpt-llama2-13b #训练ckpt保存地址
MODEL_PATH=${SAVE_PATH}/ckpt-llama2-13b #预训练后的模型生成路径，断点续训时必须要有此参数。
# megatron args
TP=8
PP=1
SEED=1234
RUN_TYPE=retrain #表示脚本运行类型是断点续训
scripts/llama2/llama2.sh
```

3. 修改完后，保存退出。

```
:wq
```

4. 在AscendSpeed代码目录下执行断点续训练脚本。

```
bash scripts/llama2/retrain-llama2-13b.sh
```

图 3-24 保存的 ckpt

```
[root@devserver-modelarts ckpt]# ll
total 24
drwxr-x--- 42 HwHiAiUser users 4096 Oct 20 12:34 iter_0000005
drwxr-x--- 42 HwHiAiUser users 4096 Oct 20 13:04 iter_0000010
drwxr-x--- 42 HwHiAiUser users 4096 Oct 20 13:34 iter_0000015
drwxr-x--- 42 HwHiAiUser users 4096 Oct 20 14:04 iter_0000020
drwxr-x--- 42 HwHiAiUser users 4096 Oct 20 14:56 iter_0000025
-rw-r----- 1 HwHiAiUser users 2 Oct 20 14:20 latest_checkpointed_iteration.txt
```

5. 可以参考[查看日志和性能](#)操作，查看断点续训练日志和性能。

3.3.3.5 查看日志和性能

查看日志

训练过程中，训练日志会在最后的Rank节点打印。

图 3-25 打印训练日志

```
[before the start of training step] datetime: 2023-12-07 10:46:49
iteration 1/ 20 | consumed samples: 32 | consumed tokens: 131072 | elapsed time per iteration (ms): 97720.8 | learning rate: 4.687E-08 | global batch size: 32 | lm loss: 1.118024E+01 | loss scale: 1.0 | g
rad norm: 39.329 | actual seq len: 4096 | number of skipped iterations: 0 | number of nan iterations: 0 | samples per second: 0.227 | TFL0P9: 2.66 |
[Rank 0] (after 1 iterations) memory (MB) | allocated: 12965.61865234375 | max allocated: 13261.03759765625 | reserved: 13712.0 | max reserved: 13712.0 | Rank 4] (after 1 iterations) memory (MB) | allocated: 12965.61865234375 | max allocated: 13261.03759765625 | reserved: 13712.0 | max reserved: 13712.0
[Rank 7] (after 1 iterations) memory (MB) | allocated: 12965.61865234375 | max allocated: 13261.03759765625 | reserved: 13712.0 | max reserved: 13712.0
time (ms)
[Rank 0] (after 1 iterations) memory (MB) | allocated: 12965.61865234375 | max allocated: 13261.03759765625 | reserved: 13712.0 | max reserved: 13712.0
[Rank 5] (after 1 iterations) memory (MB) | allocated: 12965.61865234375 | max allocated: 13261.03759765625 | reserved: 13712.0 | max reserved: 13712.0
[Rank 1] (after 1 iterations) memory (MB) | allocated: 12965.61865234375 | max allocated: 13261.03759765625 | reserved: 13712.0 | max reserved: 13712.0
[Rank 3] (after 1 iterations) memory (MB) | allocated: 12965.61865234375 | max allocated: 13261.03759765625 | reserved: 13712.0 | max reserved: 13712.0
[Rank 2] (after 1 iterations) memory (MB) | allocated: 12965.61865234375 | max allocated: 13261.03759765625 | reserved: 13712.0 | max reserved: 13712.0
iteration 2/ 20 | consumed samples: 64 | consumed tokens: 262144 | elapsed time per iteration (ms): 14402.0 | learning rate: 9.375E-08 | global batch size: 32 | lm loss: 1.118334E+01 | loss scale: 1.0 | g
rad norm: 39.675 | actual seq len: 4096 | number of skipped iterations: 0 | number of nan iterations: 0 | samples per second: 2.222 | TFL0P9: 51.97 |
time (ms)
iteration 3/ 20 | consumed samples: 96 | consumed tokens: 393216 | elapsed time per iteration (ms): 14218.3 | learning rate: 1.406E-07 | global batch size: 32 | lm loss: 1.118030E+01 | loss scale: 1.0 | g
rad norm: 39.757 | actual seq len: 4096 | number of skipped iterations: 0 | number of nan iterations: 0 | samples per second: 2.251 | TFL0P9: 52.65 |
time (ms)
iteration 4/ 20 | consumed samples: 128 | consumed tokens: 524288 | elapsed time per iteration (ms): 14315.5 | learning rate: 1.875E-07 | global batch size: 32 | lm loss: 1.117722E+01 | loss scale: 1.0 | g
rad norm: 38.376 | actual seq len: 4096 | number of skipped iterations: 0 | number of nan iterations: 0 | samples per second: 2.235 | TFL0P9: 52.26 |
time (ms)
iteration 5/ 20 | consumed samples: 160 | consumed tokens: 655360 | elapsed time per iteration (ms): 14324.0 | learning rate: 2.344E-07 | global batch size: 32 | lm loss: 1.116560E+01 | loss scale: 1.0 | g
rad norm: 39.495 | actual seq len: 4096 | number of skipped iterations: 0 | number of nan iterations: 0 | samples per second: 2.234 | TFL0P9: 52.26 |
time (ms)
iteration 6/ 20 | consumed samples: 192 | consumed tokens: 786432 | elapsed time per iteration (ms): 14320.2 | learning rate: 2.813E-07 | global batch size: 32 | lm loss: 1.117150E+01 | loss scale: 1.0 | g
rad norm: 39.782 | actual seq len: 4096 | number of skipped iterations: 0 | number of nan iterations: 0 | samples per second: 2.235 | TFL0P9: 52.27 |
time (ms)
iteration 7/ 20 | consumed samples: 224 | consumed tokens: 917504 | elapsed time per iteration (ms): 14233.5 | learning rate: 3.281E-07 | global batch size: 32 | lm loss: 1.114488E+01 | loss scale: 1.0 | g
rad norm: 39.099 | actual seq len: 4096 | number of skipped iterations: 0 | number of nan iterations: 0 | samples per second: 2.248 | TFL0P9: 52.59 |
time (ms)
iteration 8/ 20 | consumed samples: 256 | consumed tokens: 1048576 | elapsed time per iteration (ms): 14277.9 | learning rate: 3.750E-07 | global batch size: 32 | lm loss: 1.113013E+01 | loss scale: 1.0 | g
rad norm: 38.475 | actual seq len: 4096 | number of skipped iterations: 0 | number of nan iterations: 0 | samples per second: 2.241 | TFL0P9: 52.43 |
time (ms)
iteration 9/ 20 | consumed samples: 288 | consumed tokens: 1179648 | elapsed time per iteration (ms): 14206.6 | learning rate: 4.219E-07 | global batch size: 32 | lm loss: 1.107020E+01 | loss scale: 1.0 | g
rad norm: 38.657 | actual seq len: 4096 | number of skipped iterations: 0 | number of nan iterations: 0 | samples per second: 2.252 | TFL0P9: 52.69 |
time (ms)
iteration 10/ 20 | consumed samples: 320 | consumed tokens: 1310720 | elapsed time per iteration (ms): 14233.1 | learning rate: 4.687E-07 | global batch size: 32 | lm loss: 1.109142E+01 | loss scale: 1.0 | g
rad norm: 39.465 | actual seq len: 4096 | number of skipped iterations: 0 | number of nan iterations: 0 | samples per second: 2.248 | TFL0P9: 52.59 |
time (ms)
iteration 11/ 20 | consumed samples: 352 | consumed tokens: 1441792 | elapsed time per iteration (ms): 14281.2 | learning rate: 5.156E-07 | global batch size: 32 | lm loss: 1.070205E+01 | loss scale: 1.0 | g
rad norm: 40.360 | actual seq len: 4096 | number of skipped iterations: 0 | number of nan iterations: 0 | samples per second: 2.253 | TFL0P9: 52.71 |
```

训练完成后，如果需要单独获取训练日志文件，可以在`{SAVE_PATH}/logs`路径下获取。本示例中日志存放路径为`/home/ma-user/ws/llm_train/AscendSpeed/ckpt/logs`。

查看性能

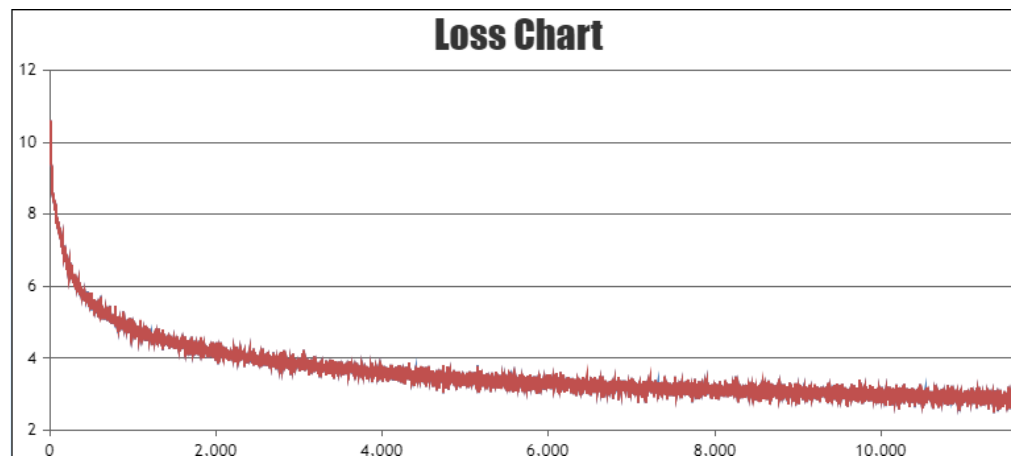
训练性能主要通过训练日志中的2个指标查看，吞吐量和loss收敛情况。

- 吞吐量：日志里存在`samples per second`参数。`samples per second*seq_lenth/总卡数`得到`tokens/s/p`，`seq_lenth`取值在训练脚本中可以查看，本示例中为4096。单机8卡吞吐量一般为1650`tokens/s/p`；双机16卡吞吐量一般为1625`tokens/s/p`。
- loss收敛情况：日志里存在`lm loss`参数，`lm loss`参数随着训练迭代周期持续性减小，并逐渐趋于稳定平缓。也可以使用可视化工具[TrainingLogParser](#)查看loss收敛情况，如图3-26所示。

单节点训练：训练过程中的loss直接打印在窗口上。

多节点训练：训练过程中的loss打印在最后一个节点上。

图 3-26 Loss 收敛情况



3.3.4 微调训练

3.3.4.1 增量预训练

3.3.4.1.1 数据处理

增量预训练（continue pre-training）前需要对数据集进行预处理，转化为.bin和.idx格式文件，以满足训练要求。

下载数据

增量预训练涉及的数据下载地址：http://github.com/tatsu-lab/stanford_alpaca/blob/main/alpaca_data.json

如果在[准备数据](#)章节已下载数据集，此处无需重复操作。

增量预训练和LoRA微调训练使用的是同一个数据集，数据处理一次即可，训练时可以共用。

数据预处理

使用数据预处理脚本preprocess_data.py脚本重新生成.bin和.idx格式的增量预训练数据。preprocess_data.py存放在AscendCloud-3rdLLM-6.3.902/llm_train/AscendSpeed/ModelLink/tools目录中，脚本具体内容如下。

```
#进入ModelLink目录：
cd /home/ma-user/ws/AscendCloud-3rdLLM-6.3.902/llm_train/AscendSpeed/ModelLink
python tools/preprocess_data.py --input alpaca_data.json\
  --output-prefix $DATA_PATH \
  --tokenizer-type PretrainedFromHF \
  --tokenizer-name-or-path $TOKENIZER_PATH \
  --tokenizer-not-use-fast \
  --handler-name GeneralInstructionHandler
```

参数说明：

- input：增量预训练数据的存放路径。
- output-prefix：处理后的数据集保存路径+数据集名称前缀（例如：alpaca-ft）。
- tokenizer-type：tokenizer的类型，可选项有['BertWordPieceLowerCase', 'BertWordPieceCase', 'GPT2BPETokenizer', 'PretrainedFromHF']，设置为PretrainedFromHF。
- tokenizer-name-or-path：tokenizer的存放路径。
- handler-name：生成数据集的用途，这里是生成的指令数据集，用于微调。

输出结果

```
alpaca-ft_packed_attention_mask_document.bin
alpaca-ft_packed_attention_mask_document.idx
alpaca-ft_packed_input_ids_document.bin
alpaca-ft_packed_input_ids_document.idx
alpaca-ft_packed_labels_document.bin
```


alpaca-ft_packed_labels_document.idx

训练的时候指定的路径为/path/to/alpaca-ft不加文件类型后缀。

此处提供一个实际的数据转换脚本代码示例：

```
python tools/preprocess_data.py \  
  --input /home/ma-user/ws/datasets/data/alpaca_data.json \  
  --output-prefix /home/ma-user/ws/datasets/alpaca-ft/llama2-13b/alpaca-ft \  
  --tokenizer-type PretrainedFromHF \  
  --tokenizer-name-or-path /home/ma-user/ws/tokenizers/llama2-13b-hf \  
  --tokenizer-not-use-fast \  
  --handler-name GeneralInstructionHandler
```

数据处理具体操作

增量预训练数据处理具体操作步骤如下。

1. 将获取到的增量预训练数据集上传到/home/ma-user/ws/datasets/目录中。
2. 创建处理后的数据存放目录/home/ma-user/ws/datasets/alpaca-ft/llama2-13B/。

```
cd /home/ma-user/ws/datasets #进入/home/ma-user/ws/datasets目录  
mkdir -p alpaca-ft/llama2-13B #创建alpaca-ft/llama2-13B目录
```

3. 进入代码目录“/home/ma-user/ws/AscendCloud-3rdLLM-6.3.902/llm_train/AscendSpeed/ModelLink/”，在代码目录中执行preprocess_data.py脚本处理数据。

此处提供一段实际的数据处理代码示例如下。

```
export PYTHONPATH=$PYTHONPATH:/home/ma-user/ws/AscendCloud-3rdLLM-6.3.902/llm_train/  
AscendSpeed/ModelLink/  
python tools/preprocess_data.py \  
  --input /home/ma-user/ws/datasets/data/alpaca_data.json \  
  --output-prefix /home/ma-user/ws/datasets/alpaca-ft/llama2-13b/alpaca-ft \  
  --tokenizer-type PretrainedFromHF \  
  --tokenizer-name-or-path /home/ma-user/ws/tokenizers/llama2-13b-hf \  
  --tokenizer-not-use-fast \  
  --handler-name GeneralInstructionHandler
```

数据处理完后，在/home/ma-user/ws/datasets/alpaca-ft/llama2-13B/目录下生成转换后的数据文件。

3.3.4.1.2 增量预训练权重转换

支持基于预训练的权重进行增量预训练，也支持HuggingFace格式权重转换为AscendSpeed格式后再进行增量预训练。基于预训练的权重再做增量训练时，不需要单独转换权重，可跳过此章节。

本章节主要介绍如何将HuggingFace权重转换为AscendSpeed格式。此处的HuggingFace权重文件和转换操作结果同时适用于增量预训练和LoRA微调训练。

HuggingFace 权重转换操作

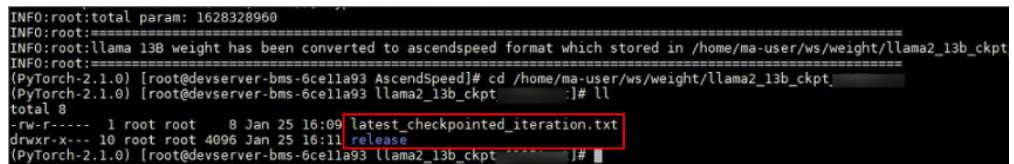
1. 下载Llama2-13b的预训练权重和词表文件，并上传到/home/ma-user/ws/tokenizers/llama2-13b-hf目录下。具体下载地址请参见表3-3。如果已下载，忽略此步骤。
2. 创建权重转换后的输出目录/home/ma-user/ws/weight/llama2-13b-ckpt/。

```
cd /home/ma-user/ws/ #进入/home/ma-user/ws/目录  
mkdir -p weight/llama2-13b-ckpt
```
3. 进入代码目录/home/ma-user/ws/AscendCloud-3rdLLM-6.3.902/llm_train/AscendSpeed/，在代码目录中执行convert_weights_from_huggingface.py脚本。

```
export PYTHONPATH=$PYTHONPATH:/home/ma-user/ws/AscendCloud-3rdLLM-6.3.902/llm_train/  
AscendSpeed/ModelLink  
cd /home/ma-user/ws/AscendCloud-3rdLLM-6.3.902/llm_train/AscendSpeed/ModelLink  
# 权重格式转换  
python tools/ckpt_convert/llama/convert_weights_from_huggingface.py \  
--input-model-dir /home/ma-user/ws/tokenizers/llama2-13b-hf \ # 输入权重文件夹  
--output-model-dir /home/ma-user/ws/weight/llama2-13b-ckpt \ #转换之后的权重输出路径  
--tensor-model-parallel-size 8 \ #tp需要与训练脚本中的配置一样  
--pipeline-model-parallel-size 1 \ # pp需要与训练脚本中的配置一样  
--type 13B \ #模型类型 ( 13B )  
--merge-mlp
```

- 4. 权重转换完成后，在/home/ma-user/ws/weight/llama2-13b-ckpt目录下查看转换后的权重文件。

图 3-27 转换后的权重文件



3.3.4.1.3 增量预训练超参配置

本章节介绍增量预训练前的超参配置，可以根据实际需要修改。

增量预训练脚本sft-llama2-13b.sh，存放在AscendCloud-3rdLLM-6.3.902/llm_train/AscendSpeed/scripts/llama2目录下。训练前，可以根据实际需要修改超参配置。

微调任务配置，操作同预训练配置类似，不同点为RUN_TYPE类型不同，以及输入输出路径的配置的不同。

表 3-8 增量预训练超参配置

参数	值	参数说明
DATA_PATH	/home/ma-user/ws/datasets/alpaca/llama2-13b/alpaca-ft	必填。训练时指定的输入数据路径。一般为数据地址/处理后的数据前缀名，不加文件类型后缀。
TOKENIZER_PATH	/home/ma-user/ws/tokenizers/llama2-13b-hf	必填。tokenizer保存地址。
SAVE_PATH	\$PWD/ckpt	中间保存结果，包含训练日志。
SAVE_CKPT_PATH	\${SAVE_PATH}/ckpt-llama2-13b-sft	必填。训练ckpt保存地址。

参数	值	参数说明
MODEL_PATH	/home/ma-user/ws/weight/llama2-13b-ckpt	必填。加载的权重文件路径。取值二选一： <ul style="list-style-type: none"> （推荐）上一步增量预训练权重转换章节中将HuggingFace格式转化为AscendSpeed格式的权重文件。 预训练完成后保存的权重文件，即预训练超参配置中的SAVE_CKPT_PATH值。如果使用此权重文件，需要将权重文件的名称改为release，将latest_checkpointed_iteration.txt的内容文件内容改为release，具体参考1和5.3-2。
MASTER_ADDR=\${1:-localhost}	localhost	主节点IP地址，默认为localhost。多机多卡训练时需指定主节点IP地址。
MODEL_TYPE	13B	模型加载类型。
TRAIN_ITERS	2000	训练迭代周期。根据实际需要修改。
MBS	4	流水线并行中一个micro batch所处理的样本量。在流水线并行中，为了减少气泡时间，会将一个step的数据切分成多个micro batch。非必填，默认值4。
GBS	64	训练中所有机器一个step所处理的样本量。影响每一次训练迭代的时长。建议单机64，双机128。
TP	8	张量并行。
PP	1	流水线并行。
seq_length	4096	要处理的最大序列长度，默认值2048，建议改为4096。
RUN_TYPE	sft	训练脚本类型：pretrain、sft、loral。此处填写sft，表示增量预训练。

3.3.4.1.4 增量预训练任务

前提条件

- 增量预训练使用的数据集为alpaca_data数据，已经完成数据处理，具体参见[数据处理](#)。
- 如果使用的是HuggingFace权重，已经将HuggingFace权重转换为AscendSpeed格式，具体参见[增量预训练权重转换](#)。

Step1 修改预训练脚本

1. 执行命令如下，进入AscendSpeed代码目录。

```
cd .. #退出当前目录
cd /home/ma-user/ws/AscendCloud-3rdLLM-6.3.902/llm_train/AscendSpeed/ #进入/home/ma-user/ws/AscendCloud-3rdLLM-6.3.902/llm_train/AscendSpeed/目录
```

2. 执行如下命令修改Llama2-13b的增量预训练脚本sft-llama2-13b.sh。

```
vim scripts/llama2/sft-llama2-13b.sh
```

修改脚本内容，与预训练参数保持一致，不同点为RUN_TYPE类型不同，RUN_TYPE=sft；以及输入输出路径的配置的不同。

```
datasets_PATH #预处理后的数据地址：*注意：一般为数据地址/数据前缀名
TOKENIZER_PATH #tokenizer地址
SAVE_PATH #中间保存结果 包含日志
SAVE_CKPT_PATH #训练ckpt保存地址
MODEL_PATH #增量预训练权重加载地址
MASTER_ADDR=${1:-localhost} #主节点的ip地址，默认为localhost，多机多卡训练时需指定主节点IP地址。
MASTER_PORT=12331 #任务运行端口号
NNODES=${2:-1} #节点总数，默认为1
NODE_RANK=${3:-0} #当前节点id，默认从0开始
MODEL_TYPE=13B #模型加载类型
TRAIN_ITERS=2000 #训练迭代周期
MBS=4 #流水线并行中一个micro batch所处理的样本量
GBS=64 #训练中所有机器一个step所处理的样本量，建议单机64，双机128。
TP=8 #张量并行
PP=1 #流水线并行
RUN_TYPE=sft #训练类型：pretrain、sft、loral，sft表示训练类型是增量预训练
```

3. 修改完后，保存退出。

```
:wq
```

Step2 启动训练脚本

单机启动

以llama2-13b为例，单机增量预训练启动命令如下。

```
bash scripts/llama2/sft-llama2-13b.sh
```

多机启动

以llama2-13b为例，多台机器执行训练启动命令如下。

```
# master_ip:主节点IP地址，指定一个节点为主节点
# nnodes: 节点总数，如为2机 则写2
# 在节点0机器上执行，当前节点id，一般从0开始，(0 1)
bash scripts/llama2/sft-llama2-13b.sh <master_ip> <nnodes> 0
...
# 在节点n机器上执行
bash scripts/llama2/sft-llama2-13b.sh <master_ip> <nnodes> n
```

可以参考[查看日志和性能](#)操作，查看训练日志。

训练完成后，请参考[查看日志和性能](#)章节查看性能。

3.3.4.1.5 查看性能

查看增量预训练的日志和性能，具体方法请参见[查看日志和性能](#)。

3.3.4.2 LoRA 微调训练

3.3.4.2.1 数据处理

训练前需要对数据集进行预处理，转化为.bin和.idx格式文件，以满足训练要求。LoRA微调训练与增量预训练使用同一个数据集，即都是alpaca_data.json。

如果已经在增量预训练时处理过数据，可以直接使用，无需重复处理。如果未处理过数据，请参见[数据处理](#)章节先处理数据。

3.3.4.2.2 LoRA 微调权重转换

LoRA微调训练前，需要先把训练权重文件转换为AscendSpeed格式。

- 基于预训练或增量预训练生成的权重文件已经是AscendSpeed格式，进行LoRA微调训练时，不需要再单独做权重转换，可以跳过此章节。
- 基于原始HuggingFace权重进行LoRA微调训练时，需要将Huggingface格式权重转换为AscendSpeed格式。

LoRA微调训练和增量预训练使用的是同一个HuggingFace权重文件，转换为AscendSpeed格式后的结果也是通用的。如果在增量预训练任务中已经完成了[HuggingFace权重转换操作](#)，此处无需重复操作，可以直接使用增量预训练中的权重转换结果。如果前面没有执行HuggingFace权重转换任务，可以参考[增量预训练权重转换](#)章节完成。

3.3.4.2.3 LoRA 微调超参配置

本章节介绍LoRA微调训练前的超参配置，可以根据实际需要修改。

LoRA微调训练脚本lora-llama2-13b.sh，存放在AscendCloud-3rdLLM-6.3.902/llm_train/AscendSpeed/scripts/llama2/目录下。训练前，可以根据实际需要修改超参配置。

微调任务配置，操作同预训练配置类似，不同点为RUN_TYPE类型不同，以及输入输出路径的配置的不同。

表 3-9 超参配置

参数	值	参数说明
DATA_PATH	/home/ma-user/ws/datasets/alpaca-ft/llama2-13b/alpaca-ft	必填。训练时指定的输入数据路径。一般为数据地址/处理后的数据前缀名，不加文件类型后缀。
TOKENIZER_PATH	/home/ma-user/ws/tokenizers/llama2-13b-hf	必填。tokenizer保存地址。
SAVE_PATH	\$PWD/ckpt	中间保存结果，包含训练日志。
SAVE_CKPT_PATH	\${SAVE_PATH}/ckpt-llama2-13b-lora	必填。训练ckpt保存地址。

参数	值	参数说明
MODEL_PATH	/home/ma-user/ws/weight/llama2-13b-ckpt	必填。加载的权重文件路径。取值二选一： <ul style="list-style-type: none"> （推荐）上一步LoRA微调权重转换章节中将HuggingFace格式转化为AscendSpeed格式的权重文件。 预训练完成后保存的权重文件，即预训练超参配置中的SAVE_CKPT_PATH值。如果使用此权重文件，需要将权重文件的名称改为release，将latest_checkpointed_iteration.txt的内容文件内容改为release，具体参考1和5.3-2。
MODEL_TYPE	13B	模型加载类型。
TRAIN_ITERS	2000	训练迭代周期。根据实际需要修改。
MBS	4	流水线并行中一个micro batch所处理的样本量。在流水线并行中，为了减少气泡时间，会将一个step的数据切成多个micro batch。 非必填，默认值4。
GBS	64	训练中所有机器一个step所处理的样本量。影响每一次训练迭代的时长。建议值单机64，双机128。
TP	8	张量并行。
PP	1	流水线并行。
seq_length	4096	要处理的最大序列长度，默认值2048，建议改为4096。
RUN_TYPE	lora	训练脚本类型：pretrain、sft、lora。此处填写lora，表示LoRA微调训练。

3.3.4.2.4 LoRA 微调任务

前提条件

- LoRA微调使用的数据集为alpaca_data数据，已经完成数据处理，具体参见[数据处理](#)。
- 如果使用的是HuggingFace权重，已经将HuggingFace权重转换为AscendSpeed格式，具体参见[LoRA微调权重转换](#)。

Step1 修改 LoRA 微调训练脚本

1. 执行命令如下，进入/home/ma-user/ws/AscendCloud-3rdLLM-6.3.902/llm_train/AscendSpeed/代码目录。

```
cd /home/ma-user/ws/AscendCloud-3rdLLM-6.3.902/llm_train/AscendSpeed/
```

2. 执行如下命令修改Llama2-13b的LoRA微调训练脚本lora-llama2-13b.sh。
vim scripts/llama2/lora-llama2-13b.sh

修改脚本内容，与增量预训练参数保持一致，不同点为RUN_TYPE类型不同，RUN_TYPE=lora；以及输入输出路径的配置的不同。

```
# learning rate args
LR=0.00001
MIN_LR=0.000001
TRAIN_ITERS=2000 #训练周期
LR_WARMUP_ITERS=2000
MBS=4
GBS=64 #训练中所有机器一个step所处理的样本量，建议单机64，双机128。
# data args
PWD=`pwd`
datasets_PATH=/home/ma-user/ws/datasets/alpaca-ft/llama2-13b/alpaca-ft #训练数据输入路径，不加文件类型后缀
TOKENIZER_PATH=/home/ma-user/ws/tokenizers/llama2-13b-hf #TOKENIZER存放路径
SAVE_PATH=$PWD/ckpt #训练过程文件保存路径，包括日志
SAVE_CKPT_PATH=${SAVE_PATH}/ckpt-llama2-13b #续训完成后的权重保存目录
MODEL_PATH=/home/ma-user/ws/weight/llama2-13b-ckpt #预训练后的模型生成路径，断点续训时必须要有此参数。
# megatron args
TP=8
PP=1
SEED=1234
RUN_TYPE=lora #表示脚本运行类型是断点续训，表示训练类型是LoRA微调训练
```

3. 修改完后，保存退出。

```
:wq
```

Step2 启动训练脚本

单机启动

以llama2-13b为例，单机增量预训练启动命令如下。

```
bash scripts/llama2/lora-llama2-13b.sh
```

多机启动

以llama2-13b为例，多台机器执行训练启动命令如下。

```
# master_ip:主节点IP地址，指定一个节点为主节点
# nnodes: 节点总数，如为2机 则写2
# 在节点0机器上执行，当前节点id，一般从0开始，(0 1)
bash scripts/llama2/lora-llama2-13b.sh <master_ip> <nnodes> 0
...
# 在节点n机器上执行
bash scripts/llama2/lora-llama2-13b.sh <master_ip> <nnodes> n
```

可以参考[查看日志和性能](#)操作，查看训练日志。

训练完成后，请参考[查看日志和性能](#)章节查看性能。

3.3.4.2.5 查看性能

查看LoRA微调训练的日志和性能，具体方法请参见[查看日志和性能](#)。

3.3.5 推理前的权重合并转换

3.3.5.1 权重合并和转换介绍

模型训练完成后，训练的产物包括模型的权重、优化器状态、loss等信息。这些内容可用于断点续训、模型评测或推理任务等。

在进行模型评测或推理任务前，需要将训练后生成的多个权重文件合并，并转换成Huggingface格式的权重文件。

权重文件的合并转换操作都要求在训练的环境中进行。

- 预训练或增量预训练产生的权重文件的合并与转换操作，请参考[多卡权重合并](#)进行操作。
- LoRA微调训练产生的权重文件的合并与转换操作，请参考[LoRA权重合并](#)进行操作。

3.3.5.2 预训练权重合并及转换

由于预训练或增量预训练时产出的权重文件（TP和PP文件）个数比较多，推理前需要把多个权重文件合并为一个文件，并转换为HuggingFace格式。Llama2-13B一般使用单卡推理。

基于[预训练](#)或[增量预训练](#)完成的模型，进行推理部署时，权重合并和转换操作建议参考本章节。

脚本convert_weights_to_huggingface.py包含了权重文件合并和转换操作，具体的脚本内容和参数解释如下。

该脚本的执行需要在/home/ma-user/ws/AscendCloud-3rdLLM-6.3.902/llm_train/AscendSpeed/代码目录下进行。

```
python scripts/tools/ckpt_convert/llama/convert_weights_to_huggingface.py \  
--input-model-dir ${ASCNEDSPEED_CKPT_PATH} \  
--output-model-dir ${MERGE_CKPT_PATH} \  
--src-tensor-model-parallel-size ${TENSOR-MODEL-PARALLEL-SIZE} \  
--src-pipeline-model-parallel-size ${PIPELINE-MODEL-PARALLEL-SIZE} \  
--type ${TYPE} \  
--org-huggingface-dir ${HUGGINFGFACE_DIR} \  
--merge-mlp
```

参数说明：

- \${ASCNEDSPEED_CKPT_PATH}：训练生成的AscendSpeed格式权重目录，多机多卡场景下需要把多个节点上的权重文件都放到任意一个节点的这个目录下；需要指定到含有mp_rank_xxxxxxx的目录，一般为iter_xxxxx或release。
- \${MERGE_CKPT_PATH}：合并后的权重路径。
- \${TENSOR-MODEL-PARALLEL-SIZE}：原始模型的TP配置大小，取值来自训练中的配置，此处需要手动输入。
- \${PIPELINE-MODEL-PARALLEL-SIZE}：原始模型的PP配置大小，取值来自训练中的配置，此处需要手动输入。
- \${TYPE}：原始模型参数大小，支持参数配置：7B、13B、70B，按实际模型要求设置。
- \${HUGGINFGFACE_DIR}：可选，开源HuggingFace权重目录，用于将开源权重内的配置文件，复制到转换后权重的输出目录中。

下面提供一个convert_weights_to_huggingface.py脚本的实际样例，供参考。

```
python scripts/tools/ckpt_convert/llama/convert_weights_to_huggingface.py \  
--input-model-dir /home/ma-user/ws/AscendCloud-3rdLLM-6.3.902/llm_train/AscendSpeed/ckpt/ckpt-
```

```
llama2-13b-sft/iter_xxxxxxx \  
--output-model-dir /home/ma-user/ws/weight/ckpt-llama2-13b-sft-hf \  
--src-tensor-model-parallel-size 8 \  
--src-pipeline-model-parallel-size 1 \  
--type 13B \  
--org-huggingface-dir /home/ma-user/ws/tokenizers/llama2-13b-hf \  
--merge-mlp
```

3.3.5.3 LoRA 微调权重合并及转换

由于LoRA微调训练时产生的权重文件（TP和PP文件）个数比较多，推理前需要把多个权重文件合并为一个文件，并转换为HuggingFace格式。Llama2-13B一般使用单卡推理。

Step1 合并 LoRA 微调训练生成的权重文件

此步骤的目的是将LoRA微调训练时生成的SAVE_CKPT_PATH和MODEL_PATH权重文件合并在一起，形成完整的权重文件。SAVE_CKPT_PATH和MODEL_PATH的具体值参考[LoRA微调超参配置](#)。

1. 将LoRA微调后权重文件夹的名称改为release。LoRA微调后权重文件目录结构如下。

```
├── ${SAVE_CKPT_PATH}  
│   ├── iter_xxxxxxx #此处需要将文件名iter_xxxxxxx改为release  
│   └── latest_checkpointed_iteration.txt
```

参数说明：

`${SAVE_CKPT_PATH}`: /home/ma-user/ws/AscendCloud-3rdLLM-6.3.902/llm_train/AscendSpeed/ckpt/ckpt-llama2-13b-lora。

此处以iter_0000002为例，改名为release，执行命令如下。

```
cd /home/ma-user/ws/AscendCloud-3rdLLM-6.3.902/llm_train/AscendSpeed/ckpt/ckpt-llama2-13b-lora #进入LoRA微调权重文件存放路径  
mv iter_0000002/ release #修改权重文件夹名称为release
```

2. 编辑LoRA微调后权重文件latest_checkpointed_iteration.txt的内容，删除文件中原有内容，增加release。修改后的latest_checkpointed_iteration.txt文件内容如下。

```
release
```

3. 编辑LoRA权重合并脚本文件merge_lora_llama2_ptd_13B.sh，并修改配置。该脚本存放在 /home/ma-user/ws/llm_train/AscendSpeed/scripts/tools/lora目录下。

```
cd /home/ma-user/ws/AscendCloud-3rdLLM-6.3.902/llm_train/AscendSpeed/  
vim scripts/tools/lora/merge_lora_llama_ptd_13B.sh
```

- ORIGIN_CHECKPOINT_PATH=/home/ma-user/ws/tokenizers/llama2-13b-hf: 设置为[LoRA微调超参配置](#)章节中的MODEL_PATH值。
- LORA_CHECKPOINT_PATH=/home/ma-user/ws/llm_train/AscendSpeed/ckpt/ckpt-llama2-13b-lora: 设置为[LoRA微调任务](#)章节中的SAVE_CKPT_PATH值。
- VOCAB_FILE=/home/ma-user/ws/tokenizers/llama2-13b-hf: tokenizer文件路径。
- MERGED_MODEL_SAVE_PATH=/home/ma-user/ws/weight/llama2_13b_lora_merge/: 输出合并后的权重路径。
- TP=8: 张量并行数，要与LORA微调时设置相同的参数。
- PP=1: 流水线并行数，要与LORA微调时设置相同的参数，单机建议值为1，双机建议为2。

4. 执行如下命令，运行权重合并脚本。

- `{TENSOR-MODEL-PARALLEL-SIZE}`: 原始模型的TP配置大小，取值来自训练中的配置，此处需要手动输入。
- `{PIPELINE-MODEL-PARALLEL-SIZE}`: 原始模型的PP配置大小，取值来自训练中的配置，此处需要手动输入。
- `{TYPE}`: 原始模型参数大小，支持参数配置：7B、13B、70B，按实际模型要求设置。
- `{HUGGINGFACE_DIR}`: 可选，开源HuggingFace权重目录，用于将开源权重内的配置文件，复制到转换后权重的输出目录中。

下面提供一个convert_weights_to_huggingface.py脚本的实际样例，供参考。

```
python scripts/tools/ckpt_convert/llama/convert_weights_to_huggingface.py \  
--input-model-dir /home/ma-user/ws/AscendCloud-3rdLLM-6.3.902/llm_train/AscendSpeed/ckpt/ckpt-llama2-13b-lora/iter_xxxxxx \  
--output-model-dir /home/ma-user/ws/weight/ckpt-llama2-13b-lora-hf \  
--src-tensor-model-parallel-size 8 \  
--src-pipeline-model-parallel-size 1 \  
--type 13B \  
--org-huggingface-dir /home/ma-user/ws/tokenizers/llama2-13b-hf \  
--merge-mlp
```

日志中出现下列提示即表示合并转换完成。

```
Merging tp pp weight from path: {as_dir} .....  
Merging weight complete!!!  
Converting weight to huggingface.....  
Converting weight to huggingface complete!!!  
Saving weight to path: {hf_dir}  
huggingface weight saved to: {hf_dir}/pytorch_model.bin  
Generating model index config.....  
model index config saved in: {hf_dir}/pytorch_model.bin.index.json  
Generating weight config file from: {org_hf_dir}  
config file copy from "{org_hf_dir}" complete!!!
```

转换完成后目录中的release文件夹内至少包含一个bin文件和一个bin.index.json文件，bin文件大小应和huggingface原始权重大小相似：

```
{hf_dir}  
├── pytorch_model.bin  
└── pytorch_model.bin.index.json
```

以下config文件需要指定org_huggingface_dir参数才会生成。

```
├── config.json  
├── generation_config.json  
├── gitattributes.txt  
├── LICENSE.txt  
├── README.md  
├── special_tokens_map.json  
├── tokenizer_config.json  
├── tokenizer.json  
├── tokenizer.model  
└── USE_POLICY.md
```

3.3.6 推理部署（ATB）

3.3.6.1 推理场景说明

本教程利用昇腾高性能算子库Ascend Transformer Boost（ATB）和适配昇腾平台的大模型推理服务Text Generation Inference（TGI）+ 华为自研Ascend Snt9b硬件，为用户提供开箱即用的推理部署方案，为用户提供端到端的大模型解决方案，帮助用户使能大模型业务。该场景下，可以进行推理性能和精度测试等。

3.3.6.2 推理服务部署

本章节介绍如何配置推理任务的镜像环境。

前提条件

1. 机器已开通，密码已获取，能通过SSH登录机器，具体参见[准备环境](#)。
2. 已获取HuggingFace格式权重文件，具体参见[准备代码](#)。

Step1 检查环境

1. SSH登录机器后，检查NPU设备检查。运行如下命令，返回NPU设备信息。

```
npu-smi info
```

如出现错误，可能是机器上的NPU设备没有正常安装，或者NPU镜像被其他容器挂载。请先正常[安装NPU设备和驱动](#)，或释放被挂载的NPU。

2. 检查docker是否安装。

```
docker -v #检查docker是否安装
```

如尚未安装，运行以下命令安装docker。

```
yum install -y docker-engine.aarch64 docker-engine-selinux.noarch docker-runc.aarch64
```

Step2 获取推理镜像

建议使用官方提供的镜像部署推理服务。镜像地址`{image_url}`请参见[准备镜像](#)。

```
docker pull {image_url}
```

Step3 启动容器镜像

启动容器镜像前请先按照参数说明修改`{}`中的参数。

```
docker run -itd \  
-p 8085:8085 \  
--device=/dev/davinci0 \  
--device=/dev/davinci1 \  
--device=/dev/davinci2 \  
--device=/dev/davinci3 \  
--device=/dev/davinci4 \  
--device=/dev/davinci5 \  
--device=/dev/davinci6 \  
--device=/dev/davinci7 \  
-v /etc/localtime:/etc/localtime \  
-v /usr/local/Ascend/driver:/usr/local/Ascend/driver \  
-v /etc/ascend_install.info:/etc/ascend_install.info \  
--device=/dev/davinci_manager \  
--device=/dev/devmm_svm \  
--device=/dev/hisi_hdc \  
-v /var/log/npu:/usr/slog \  
-v /usr/local/bin/npu-smi:/usr/local/bin/npu-smi \  
-v /sys/fs/cgroup:/sys/fs/cgroup:ro \  
-v ${dir}:${container_dir} \  
--name ${container_name} \  
{image_id} \  
/bin/bash
```

参数说明：

- `-e ASCEND_VISIBLE_DEVICES=0-7`，挂载机器上的0-7卡。
- `-p 8085:8085`代表需要在宿主机和容器中绑定的端口。示例中，http server使用了8085端口，根据实际需要修改。

- `-v ${dir}:${container_dir}` 代表需要在容器中挂载宿主机的目录。宿主机和容器使用不同大的文件系统，`dir`为宿主机中权重文件目录，`container_dir`为要挂载到的容器中的目录。为方便两个地址可以相同。请确保在容器中有`weight_dir`的权限。可以在宿主机中执行`chmod 777 -R ${weight_dir}`来放开权限
- `--name ${container_name}` 容器名称，进入容器时会用到
- `{image_id}` 为docker镜像的id，在宿主机上可通过`docker images`查询得到。

Step4 进入容器并配置 ATB+TGI 环境

1. 通过容器名称进入容器中。

```
docker exec -it ${container_name} bash
```
2. 配置虚拟环境

```
conda create -n tgi python=3.9.18  
conda activate tgi  
pip install numpy decorator attrs psutil absl-py cloudpickle scipy synr==0.5.0 tornado torch==2.0.1
```
3. 获取依赖包：

https://llm-mindspore-ei.obs.cn-southwest-2.myhuaweicloud.com/POC/infer_files/dependencies.zip

说明

此处的dependencies.zip非商用发布版本，仅用于跑推理评测任务，验证模型训练结果。

```
unzip dependencies.zip  
cd dependencies  
  
pip install torch_npu-2.0.1.post1_20231215-cp39-cp39-linux_aarch64.whl  
pip install apex-0.1_ascend_20231215-cp39-cp39-linux_aarch64.whl  
  
# 安装rust  
wget https://static.rust-lang.org/dist/rust-1.76.0-aarch64-unknown-linux-gnu.tar.gz  
tar -zxvf rust-1.76.0-aarch64-unknown-linux-gnu.tar.gz && cd ./rust-1.76.0-aarch64-unknown-linux-gnu && sudo bash install.sh  
  
export PATH=/home/ma-user/anaconda3/envs/tgi/lib/python3.9/site-packages/torch/bin/:$PATH  
  
# 安装昇腾模型库  
sudo mkdir -p /usr/local/Ascend/transformer-llm && cd .. && sudo chown -R ma-user:ma-group /usr/local/Ascend/transformer-llm/ && tar -zxvf Ascend-cann-llm_7.0.0_linux-aarch64_torch2.0.1-abi0.tar.gz -C /usr/local/Ascend/transformer-llm/  
  
source /usr/local/Ascend/transformer-llm/set_env.sh && source /usr/local/Ascend/ascend-toolkit/set_env.sh  
  
#安装atb加速库  
sudo chown -R ma-user:ma-group /usr/local/Ascend/ascend-toolkit/ && bash Ascend-cann-atb_7.0.0_linux-aarch64_abi0.run --install && source /home/ma-user/Ascend/atb/set_env.sh
```

4. 编译适配昇腾后的TGI框架。

```
git clone https://github.com/huggingface/text-generation-inference.git && cd text-generation-inference/ && git checkout -b 0.9.4 v0.9.4 && cp ../ascend_tgi.patch ./ && git apply ascend_tgi.patch  
  
mv ../text-generation-inference /home/ma-user/TGI && cd /home/ma-user/TGI  
  
BUILD_EXTENSIONS=False make install;  
  
export PATH=$PATH:/home/ma-user/.cargo/bin
```

说明

三方开源软件用于生产环境时，请注意开源协议的要求，同时请自行评估三方开源软件可能存在的安全风险，并采取必要的安全防护措施。

- 在/home/ma-user/.bashrc文件中写入以下配置，用于设置推理环境变量。

```
source /usr/local/Ascend/ascend-toolkit/set_env.sh
export LD_LIBRARY_PATH="/usr/local/Ascend/ascend-toolkit/latest/lib64;/usr/local/Ascend/ascend-toolkit/latest/lib64/plugin/opskernel;/usr/local/Ascend/ascend-toolkit/latest/lib64/plugin/nnengine;/usr/local/Ascend/ascend-toolkit/latest/python/site-packages;/usr/local/Ascend/ascend-toolkit/latest/opp/built-in/op_impl/ai_core/tbe;/usr/local/Ascend/driver/lib64;/usr/local/Ascend/driver/lib64/common;/usr/local/Ascend/driver/lib64/driver":$LD_LIBRARY_PATH
export PATH=$PATH:/home/ma-user/.cargo/bin
source /home/ma-user/Ascend/atb/set_env.sh
source /usr/local/Ascend/transformer-llm/set_env.sh

conda activate tgi
```
- 配置性能测试的环境，执行推理性能测试任务时需要用到。

```
conda create -n benchmark --clone tgi
conda activate benchmark

pip install transformers==4.37.1 matplotlib>=3.8.2 openpyxl>=3.1.2
```

Step5 启动推理服务

- 配置推理服务需要的环境变量。

```
export ATB_LAYER_INTERNAL_TENSOR_REUSE=1
```
- 配置需要使用的NPU卡，例如：实际使用的是第1张和第2张卡，此处填写为0,1，以此类推。

```
export ASCEND_RT_VISIBLE_DEVICES=0,1
```

📖 说明

NPU卡编号可以通过命令npu-smi info查询。

- 配置使用的显存，376T配置56，280T配置26。

```
export MAX_MEMORY_GB=56
```
- 启动推理服务，本服务使用的开源服务框架是TGI，具体命令参考https://huggingface.co/docs/text-generation-inference/main/en/basic_tutorials/launcher。该版本不支持https和身份认证机制。可以根据官网说明修改参数。推荐参数配置如下。

表 3-10 推理服务启动参数表

参数配置	推荐值	参数说明
--max-input-length	1024	推理时最大输入的tokens数量，默认值为1024，可以根据实际修改。该参数会影响推理性能。
--max-total-tokens	2048	推理时最大输入+最大输出的tokens数量，默认值为2048，可以根据实际修改。该参数会影响推理性能。
--max-batch-prefill-tokens	4096	在prefill阶段，最多会使用多少token，一般为--max-input-length的整数倍。该参数会影响推理性能。
--trust-remote-code	无	是否相信远程代码。
--max-waiting-tokens	1	推理进行时，新到达的请求需要等待多少增量推理后，切换成全量推理。

参数配置	推荐值	参数说明
--max-concurrent-requests	1000	最大同时处理的请求数，超过后拒绝访问。
--waiting-served-ratio	0.2	当等待的请求数量达到增量推理的多少比例后，切换成全量推理。

TGI服务需要safetensor的权重格式，如果权重格式不是safetensor，首次启动时，需要先将权重转换成safetensor格式（自动进行）。首次启动耗时在5~10分钟。

如果权重格式包含safetensor，启动时间在1~3分钟。服务启动后，会打印如下信息。

```
2024-01-22T03:27:22.252926Z INFO text_generation_router: router/src/main.rs:239: Setting max batch total tokens to 97024
2024-01-22T03:27:22.252952Z INFO text_generation_router: router/src/main.rs:240: Connected
```

Step6 请求推理服务

服务请求方式可以参考该链接中的curl请求：https://huggingface.co/docs/text-generation-inference/main/en/basic_tutorials/consuming_tgi

服务请求API参考：<https://huggingface.github.io/text-generation-inference>

3.3.6.3 推理性能测试

3.3.6.3.1 benchmark 方法介绍

性能benchmark包括两部分。

- 静态性能测试：评估在固定输入、固定输出和固定并发下，模型的吞吐与首token延迟。该方式实现简单，能比较清楚的看出模型的性能和输入输出长度、以及并发的关系。
- 动态性能测试：评估在请求并发在一定范围内波动，且输入输出长度也在一定范围内变化时，模型的延迟和吞吐。该场景能模拟实际业务下动态的发送不同长度请求，能评估推理框架在实际业务中能支持的并发数。

性能benchmark验证使用到的脚本存放在代码包AscendCloud-3rdLLM-x.x.x.zip的llm_evaluation目录下。

代码目录如下：

```
benchmark_tools
├── benchmark_parallel.py # 评测静态性能脚本
├── benchmark_serving.py # 评测动态性能脚本
├── generate_dataset.py # 生成自定义数据集的脚本
├── benchmark_utils.py # 工具函数集
└── benchmark.py # 执行静态，动态性能评测脚本
```

3.3.6.3.2 静态 benchmark

本章节介绍如何进行静态benchmark验证。

前提条件

已经上传benchmark验证脚本到推理容器中。

静态 benchmark 验证操作

1. 切换到benchmark虚拟环境测试，命令如下。静态benchmark验证是在benchmark虚拟环境中操作。
2. 运行静态benchmark验证脚本benchmark_parallel.py，具体操作命令如下，可以根据参数说明修改参数。

```
conda activate benchmark
```

```
cd benchmark_tools
python benchmark_parallel.py --backend tgi --host 127.0.0.1 --port 8085 --tokenizer /path/to/
tokenizer --epochs 5 \
--parallel-num 1 4 8 16 32 --prompt-tokens 1024 2048 --output-tokens 128 256 --benchmark-csv
benchmark_parallel.csv
```

参数说明

- --backend: 服务类型，支持tgi、vllm、mindspore等。本文档使用的推理接口是tgi。
 - --host: 服务IP地址，如127.0.0.1。
 - --port: 服务端口，和推理服务端口8085。
 - --tokenizer: tokenizer路径，HuggingFace的权重路径。
 - --epochs: 测试轮数，默认取值为5
 - --parallel-num: 每轮并发数，支持多个，如 1 4 8 16 32。
 - --prompt-tokens: 输入长度，支持多个，如 128 128 2048 2048，数量需和--output-tokens的数量对应。
 - --output-tokens: 输出长度，支持多个，如 128 2048 128 2048，数量需和--prompt-tokens的数量对应。
 - --benchmark-csv: 结果保存路径，如benchmark_parallel.csv。
3. 脚本运行完成后，测试结果保存在benchmark_parallel.csv中，示例如下图所示。

图 3-29 静态 benchmark 测试结果

并发数	输入长度	输出长度	平均输出tokens 吞吐 (tokens/s)	总吞吐	平均首tokens 时延 (ms)	平均增量时延 (ms)
1	128	128	38.37921287	38.37921287	47.01631397	25.89086896
1	2048	128	31.46196326	31.46196326	286.783878	30.57729576
1	128	2048	37.22621356	37.22621356	47.62573801	26.85267587
1	2048	2048	30.8477532	30.8477532	288.585896	35.55573446
4	128	128	34.60897386	138.4358954	99.907596	28.33562475
4	2048	128	23.62077168	94.48308671	787.865362	36.46609085
4	128	2048	32.21485727	128.8594291	101.1691255	31.00737524
4	2048	2048	26.86382637	107.4553055	793.011828	36.85567269
8	128	128	30.43106893	243.4485514	206.5356592	31.76996247
8	2048	128	17.06168702	136.4934962	1439.875192	47.74383649
8	128	2048	28.19794546	225.5835637	184.9889007	35.39069897
8	2048	2048	21.09273309	168.7418647	1441.838804	46.7286104
16	128	128	25.78847332	412.6155731	399.6799193	36.21664226
16	2048	128	10.17110017	162.7376027	3155.105778	74.67985077
16	128	2048	20.06476629	321.0362607	2168.079733	50.05948004
16	2048	2048	15.73341905	251.7347048	8245.736343	67.35985094
32	128	128	19.6663625	629.3236001	964.7942346	44.42653283
32	2048	128	7.115448359	227.6943475	8809.944518	86.60364656
32	128	2048	14.81503878	474.0812409	8621.067957	73.88934711
32	2048	2048	10.91516138	349.2851641	11665.08883	113.4413863

3.3.6.3.3 动态 benchmark

本章节介绍如何进行动态benchmark验证。

Step1 获取数据集

动态benchmark需要使用数据集进行测试，可以使用公开数据集，例如Alpaca、ShareGPT。也可以根据业务实际情况，使用generate_datasets.py脚本生成和业务数据分布接近的数据集。

公开数据集下载地址：

- ShareGPT: https://huggingface.co/datasets/anon8231489123/ShareGPT_Vicuna_unfiltered/resolve/main/ShareGPT_V3_unfiltered_cleaned_split.json
- Alpaca: https://github.com/tatsu-lab/stanford_alpaca/blob/main/alpaca_data.json

使用generate_datasets.py脚本生成数据集方法：

generate_datasets.py脚本通过指定输入输出长度的均值和标准差，生成一定数量的正态分布的数据。具体操作命令如下，可以根据参数说明修改参数。

```
cd benchmark_tools
python generate_datasets.py --datasets custom_datasets.json --tokenizer /path/to/tokenizer \
--min-input 100 --max-input 3600 --avg-input 1800 --std-input 500 \
--min-output 40 --max-output 256 --avg-output 160 --std-output 30 --num-requests 1000
```

generate_datasets.py脚本执行参数说明如下：

- --datasets: 数据集保存路径，如custom_datasets.json
- --tokenizer: tokenizer路径，可以是HuggingFace的权重路径
- --min-input: 输入tokens最小长度，可以根据实际需求设置。
- --max-input: 输入tokens最大长度，可以根据实际需求设置。
- --avg-input: 输入tokens长度平均值，可以根据实际需求设置。
- --std-input: 输入tokens长度方差，可以根据实际需求设置。
- --min-output: 最小输出tokens长度，可以根据实际需求设置。
- --max-output: 最大输出tokens长度，可以根据实际需求设置。
- --avg-output: 输出tokens长度平均值，可以根据实际需求设置。
- --std-output: 输出tokens长度标准差，可以根据实际需求设置。
- --num-requests: 输出数据集的数量，可以根据实际需求设置。

Step2 使用数据集测试动态 benchmark

1. 切换到benchmark虚拟环境测试，命令如下。动态benchmark验证是在benchmark虚拟环境中操作。

```
conda activate benchmark
```

2. 执行脚本benchmark_serving.py测试动态benchmark。具体操作命令如下，可以根据参数说明修改参数。

```
cd benchmark_tools
python benchmark_serving.py --backend tgi --host 127.0.0.1 --port 8085 --datasets
custom_datasets.json --datasets-type custom \
--tokenizer /path/to/tokenizer --request-rate 0.01 1 2 4 8 10 20 --num-prompts 10 1000 1000 1000
```


- ```
1000 1000 1000 \
--max-tokens 4096 --max-prompt-tokens 3768 --benchmark-csv benchmark_serving.csv
```
- --backend: 服务类型, 如"tgi", vllm, "mindspore"
  - --host: 服务IP地址, 如127.0.0.1
  - --port: 服务端口
  - --datasets: 数据集路径
  - --datasets-type: 支持三种 "alpaca", "sharegpt", "custom"。custom为自定义数据集。
  - --tokenizer: tokenizer路径, 可以是huggingface的权重路径
  - --request-rate: 请求频率, 支持多个, 如 0.1 1 2。实际测试时, 会根据request-rate为均值的指数分布来发送请求以模拟真实业务场景。
  - --num-prompts: 某个频率下请求数, 支持多个, 如 10 100 100, 数量需和--request-rate的数量对应
  - --max-tokens: 输入+输出限制的最大长度, 模型启动参数--max-input-length值需要大于该值
  - --max-prompt-tokens: 输入限制的最大长度, 推理时最大输入tokens数量, 模型启动参数--max-total-tokens值需要大于该值, tokenizer建议带tokenizer.json的FastTokenizer
  - --benchmark-csv: 结果保存路径, 如benchmark\_serving.csv
3. 脚本运行完后, 测试结果保存在benchmark\_serving.csv中, 示例如下图所示。

图 3-30 动态 benchmark 测试结果

| 数据集    | 输入平均长度 (tokens) | 请求频率 (req/s) | 请求吞吐 (req/s) | 请求平均时延 (s)  | 平均输出tokens吞吐 (tokens/s) | 单请求每tokens平均时延 (ms) | 首tokens平均时延 (ms) | 输出tokens总吞吐 (tokens/s) |
|--------|-----------------|--------------|--------------|-------------|-------------------------|---------------------|------------------|------------------------|
| alpaca | 64.19           | 0.1          | 0.078540467  | 1.501204237 | 38.0375597              | 26.29724747         | 47.022316        | 4.523930881            |
| alpaca | 64.19           | 1            | 1.066428392  | 1.435290873 | 32.82373294             | 31.04768641         | 57.92834632      | 58.83485381            |
| alpaca | 64.19           | 2            | 1.883969105  | 1.716550277 | 31.22013539             | 32.44375926         | 58.39447439      | 103.9054735            |
| alpaca | 64.19           | 4            | 3.351360979  | 1.951271679 | 27.31530526             | 37.49762281         | 69.3579448       | 184.8945852            |

### 3.3.6.4 推理精度测试

本章节介绍如何进行推理精度测试。

#### Step1 准备数据集

精度测试需要数据集进行测试。推荐公共数据集mmlu和ceval。下载地址:

表 3-11 精度测试数据集

| 数据集名称 | 下载地址                                                                                                            | 下载说明                                                     |
|-------|-----------------------------------------------------------------------------------------------------------------|----------------------------------------------------------|
| mmlu  | <a href="https://huggingface.co/datasets/cais/mmlu">https://huggingface.co/datasets/cais/mmlu</a>               | 下载其中的data.tar解压到得到data文件夹, 为表示区分, 将data文件夹重命名为mmlu-exam。 |
| ceval | <a href="https://huggingface.co/datasets/ceval/ceval-exam">https://huggingface.co/datasets/ceval/ceval-exam</a> | 下载其中的ceval-exam.zip压缩包, 解压到ceval-exam文件夹。                |

#### Step2 配置精度测试环境

请在[推理服务部署](#)提供的镜像中的tgi环境执行。



1. 切换到tgi环境测试。

```
conda activate tgi
```

2. 获取精度测试代码。精度测试代码存放在代码包AscendCloud-3rdLLM-x.x.x的/llm\_evaluation目录中，代码目录结构如下：

```
benchmark_eval
├── config
│ ├── config.json # 服务的配置模板，已配置了ma-standard, tgi示例
│ ├── mmlu_subject_mapping.json # mmlu数据集学科信息
│ └── ceval_subject_mapping.json # ceval数据集学科信息
├── evaluators
│ ├── evaluator.py # 数据集数据预处理方法集
│ ├── chatglm.py # 处理请求相应模块，一般和chatglm的官方评测数据集ceval搭配
│ └── llama.py # 处理请求相应模块，一般和llama的评测数据集mmlu搭配
├── mmlu-exam, mmlu数据集
├── ceval-exam, ceval数据集
├── eval_test.py # 启动脚本，建立线程池发送请求，并汇总结果
└── service_predict.py # 发送请求的服务
```

3. 上传精度测试代码到推理容器中。

4. 执行精度测试启动脚本eval\_test.py，具体操作命令如下，可以根据参数说明修改参数。

```
python eval_test.py \
--max_workers=1 \
--service_name=llama2-13b-chat-test \
--eval_dataset=ceval \
--service_url=http://127.0.0.1:8085/generate \
--few_shot=3 \
--is_devserver=True \
--model_name=llama2 \
--deploy_method=tgi
```

参数说明:

- max\_workers: 请求的最大线程数，默认为1。
- service\_name: 服务名称，保存评测结果时创建目录，示例为：llama2-13b-chat-test。
- eval\_dataset: 评测使用的评测集（枚举值），目前仅支持mmlu、ceval。
- service\_url: 成功部署推理服务后的服务预测地址，示例：http://127.0.0.1:8085/generate。此处的端口号8085来自前面配置的服务端口。
- few\_shot: 开启少量样本测试后添加示例样本的个数。默认为3，取值范围为0~5整数。
- is\_devserver: 是否devserver部署方式，True表示DevServer模式。False表示ModelArts Standard模式。
- model\_name: 评测模型名称，llama2。
- deploy\_method: 部署方法，不同的部署方式api参数输入、输出解析方式不同，目前支持tgi、ma\_standard、vllm等方式。

### Step3 查看精度测试结果

默认情况下，评测结果会按照result/{service\_name}/{eval\_dataset}-{timestamp}的目录结果保存到对应的测试工程。执行多少次，则会在{service\_name}下生成多少次结果。

单独的评测结果如下：

```
{eval_dataset}-{timestamp} # 例如: mmlu-20240205093257
├── accuracy
│ └── evaluation_accuracy.xlsx # 测试的评分结果，包含各个学科数据集的评分和总和评分。
├── infer_info
└── xxx1.csv # 单个数据集的评测结果
```



本方案目前仅适用于企业客户。

## 资源规格要求

推理部署使用Ascend Snt9B计算资源。

## 获取软件

表 3-12 软件名称

| 软件名称                                                                     | 说明                     | 下载地址                                                                                                                                                                                                                                                        |
|--------------------------------------------------------------------------|------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Ascend-cann-atb_7.0.0_linux-aarch64_abi0.run                             | 推理依赖软件                 | https://ascend-cloud-llm-infer-ops.obs.cn-southwest-2.myhuaweicloud.com/version_packages/atb_llm_7.0.T61.B010.tar                                                                                                                                           |
| Ascend-cann-llm_7.0.0_linux-aarch64_torch2.0.1_abi0.tar.gz               |                        |                                                                                                                                                                                                                                                             |
| ascendcloud-llmframework_6.3.902_*.tar.gz<br><b>说明</b><br>这里的 *表示具体的时间戳。 | Ascend-vllm插件          | 获取路径： <a href="#">Support网站</a> 。<br><b>说明</b><br>如果没有软件下载权限，请联系您所在企业的华为方技术支持下载获取。                                                                                                                                                                          |
| Baichuan-13b                                                             | 从Huggingface下载的预训练权重文件 | <a href="https://huggingface.co/baichuan-inc/Baichuan-13B-Base">https://huggingface.co/baichuan-inc/Baichuan-13B-Base</a><br><a href="https://huggingface.co/baichuan-inc/Baichuan-13B-Chat">https://huggingface.co/baichuan-inc/Baichuan-13B-Chat</a> （推荐） |

下载完毕后的权重文件夹包含以下内容，此处以Baichuan-13b-chat为例。

```
Baichuan-13B-Chat
├── Baichuan-13B 模型社区许可协议.pdf
├── Community License for Baichuan-13B Model.pdf
├── config.json
├── configuration_baichuan.py
├── generation_config.json
├── generation_utils.py
├── gitattributes.txt
├── handler.py
├── modeling_baichuan.py
├── model.safetensors.index.json
├── pytorch_model-00001-of-00003.bin
├── pytorch_model-00002-of-00003.bin
├── pytorch_model-00003-of-00003.bin
├── pytorch_model.bin.index.json
├── quantizer.py
├── README.md
├── requirements.txt
├── special_tokens_map.json
└── tokenization_baichuan.py
```

## 3.4.2 安装推理容器环境

本章节介绍如何配置推理的容器镜像环境。

### 约束限制

推荐使用“西南-贵阳一”Region上的DevServer和昇腾Snt9b资源。

### Step1 购买并开通 DevServer 资源

请参考[DevServer资源开通](#)，购买DevServer资源，并确保机器已开通，密码已获取，能通过SSH登录，不同机器之间网络互通。

#### 📖 说明

购买DevServer资源时如果无可选资源规格，需要联系华为云技术支持申请开通。

当容器需要提供服务给多个用户，或者多个用户共享使用该容器时，应限制容器访问Openstack的管理地址（169.254.169.254），以防止容器获取宿主机的元数据。具体操作请参见[禁止容器获取宿主机元数据](#)。

### Step2 检查环境

1. SSH登录机器后，检查NPU设备检查。运行如下命令，返回NPU设备信息。  

```
npu-smi info
```

如出现错误，可能是机器上的NPU设备没有正常安装，或者NPU镜像被其他容器挂载。请先正常[安装NPU设备和驱动](#)，或释放被挂载的NPU。
2. 检查docker是否安装。  

```
docker -v #检查docker是否安装
```

如尚未安装，运行以下命令安装docker。

```
yum install -y docker-engine.aarch64 docker-engine-selinux.noarch docker-runc.aarch64
```
3. 配置IP转发，用于容器内的网络访问。执行以下命令查看net.ipv4.ip\_forward配置项的值，如果为1，可跳过此步骤。  

```
sysctl -p | grep net.ipv4.ip_forward
```

如果net.ipv4.ip\_forward配置项的值不为1，执行以下命令配置IP转发。  

```
sed -i 's/net.ipv4.ip_forward=0/net.ipv4.ip_forward=1/g' /etc/sysctl.conf
```

```
sysctl -p | grep net.ipv4.ip_forward
```

### Step3 获取推理镜像

建议使用官方提供的镜像部署推理服务。

镜像地址{image\_url}:

西南-贵阳一: `swr.cn-southwest-2.myhuaweicloud.com/atelier/pytorch_2_1_ascend:pytorch_2.1.0-cann_7.0.0-py_3.9-hce_2.0.2312-aarch64-snt9b-20240312154948-219655b`

```
docker pull {image_url}
```

### Step4 获取权重文件

将获取到的预训练权重文件，上传到DevServer机器。权重文件获取地址请参见[获取软件](#)。

## Step5 启动容器镜像

启动容器镜像前请先按照参数说明修改\${}中的参数。

```
docker run \
--device=/dev/davinci0 \
--device=/dev/davinci1 \
--device=/dev/davinci2 \
--device=/dev/davinci3 \
--device=/dev/davinci4 \
--device=/dev/davinci5 \
--device=/dev/davinci6 \
--device=/dev/davinci7 \
--device=/dev/davinci_manager \
--device=/dev/devmm_svm \
--device=/dev/hisi_hdc \
--name ${container_name} \
-v /usr/local/dcmi:/usr/local/dcmi \
-v /usr/local/Ascend/driver:/usr/local/Ascend/driver \
-v /etc/ascend_install.info:/etc/ascend_install.info \
-v /var/log/npu:/usr/slog \
-v /usr/local/bin/npu-smi:/usr/local/bin/npu-smi \
-v /sys/fs/cgroup:/sys/fs/cgroup:ro \
-v ${local_model_path}:${container_model_path} \
-p 32006:8080 \
-itd ${image_url} /bin/bash
```

### 参数说明：

- --name \${container\_name}：容器名称，进入容器时会用到，此处可以自己定义一个容器名称。
- -v \${local\_model\_path}:\${container\_model\_path}：代表需要在容器中挂载宿主机的目录。宿主机和容器使用不同的文件系统，local\_model\_path为宿主机中权重文件目录，container\_model\_path为要挂载到的容器中的目录。为方便两个地址可以相同。
- -p 32006:8080：代表需要在宿主机和容器中绑定的端口。示例中，32006是容器外访问端口，8080是容器内访问端口。
- --device=/dev/davinci0, ..., --device=/dev/davinci7：挂载NPU设备，示例中挂载了8张卡davinci0~davinci7。
- \${image\_url}：镜像地址

## Step6 进入容器并安装依赖软件

1. 通过容器名称进入容器中。

```
docker exec -it -u root ${container_name} bash
```

2. 上传安装依赖软件Ascend-cann-atb\_7.0.0\_linux-aarch64\_abi0.run和Ascend-cann-llm\_7.0.0\_linux-aarch64\_torch2.0.1-abi0.tar.gz到容器中。

3. 执行以下命令安装依赖软件。

```
cd ${ascend_cann_download_path}
bash Ascend-cann-atb_7.0.0_linux-aarch64_abi0.run --install
chmod -R o+rx /usr/local/Ascend/atb/
echo -e "source /usr/local/Ascend/atb/set_env.sh" >> ~/.bashrc
mkdir -p /usr/local/Ascend/transformer-llm
tar -zxvf Ascend-cann-llm_7.0.0_linux-aarch64_torch2.0.1-abi0.tar.gz -C /usr/local/Ascend/transformer-llm/
chmod -R o+rx /usr/local/Ascend/transformer-llm/
echo -e "source /usr/local/Ascend/transformer-llm/set_env.sh" >> ~/.bashrc
source ~/.bashrc
git config --global http.sslVerify "false"
```

\${ascend\_cann\_download\_path}：软件包下载存放路径，确保容器内可以访问。

安装成功后，输入exit 退出容器。

## Step7 下载并安装 Ascend-vllm 插件

1. 使用默认用户（ma-user）进入容器。

```
docker exec -it ${container_name} bash
```

2. 检查NPU环境。

```
npu-smi info
```

如果报如下错误：dcmi module initialize failed. ret is -8005，说明有其他容器使用特权绑定了相同的卡；解决方法：停掉其他容器，重启当前容器。

3. 使用ma-user用户将下载的Ascend-vllm插件包ascendcloud-llmframework\_6.3.902\_\*.tar.gz上传到容器的/home/ma-user/ 目录。

4. 在 /home/ma-user/目录下安装Ascend-vllm插件，具体命令如下。

```
echo -e "source /usr/local/Ascend/atb/set_env.sh" >> ~/.bashrc
echo -e "source /usr/local/Ascend/transformer-llm/set_env.sh" >> ~/.bashrc
source ~/.bashrc
tar -zxvf ascendcloud-llmframework_6.3.902_*.tar.gz
cd /home/ma-user/ascend-vllm/
git config --global http.sslVerify "false"
bash install.sh
```

### 📖 说明

ascendcloud-llmframework\_6.3.902\_\*.tar.gz文件名中的 \*表示具体的时间戳，请根据实际情况替换。

## 3.4.3 启动 vLLM 服务器服务

请参照[vllm官网说明](#)启动API Server。

### 启动服务

启动vllm服务器服务，具体操作命令如下，API Server的命令相关参数说明如下，可以根据参数说明修改配置。

```
export ATB_LAYER_INTERNAL_TENSOR_REUSE=1
python -m vllm.entrypoints.api_server --model ${container_model_path} \
--max-num-seqs=256 \
--max-model-len=4096 \
--max-num-batched-tokens=4096 \
--dtype=float16 \
--tensor-parallel-size=1 \
--block-size=128 \
--host=${docker_ip} \
--port=8080 \
--gpu-memory-utilization=0.9 \
--trust-remote-code
```

具体参数说明如下：

- --model \${container\_model\_path}：模型地址，模型格式是HuggingFace的目录格式。即[Step4 获取权重文件](#)上传的HuggingFace权重文件存放目录。
- --max-num-seqs：最大同时处理的请求数，超过后拒绝访问。
- --max-model-len：推理时最大输入+最大输出tokens数量，输入超过该数量会直接返回。
- --max-num-batched-tokens：prefill阶段，最多会使用多少token，必须大于或等于--max-model-len，推荐使用4096或8192。

- --dtype: 模型推理的数据类型, 当前只支持float16。
- --tensor-parallel-size: 模型并行数, 13B模型一般为1即可。
- --block-size: PagedAttention的block大小, 推荐设置为128。
- --host=\${docker\_ip}: 服务部署的IP, \${docker\_ip}替换为容器实际的IP地址。可以在宿主机上通过docker inspect 容器ID |grep IPAddress 命令查询。
- --port: 服务部署的端口, 和Step4 启动容器镜像中设置的端口保持一致, 否则不能在容器外访问推理服务。
- --gpu-memory-utilization: NPU使用的显存比例, 复用原vLLM的入参名称, 默认为0.9。
- --trust-remote-code: 是否相信远程代码, baichuan-13b必须增加此项。

## 请求服务

使用命令测试推理服务是否正常启动。

```
curl -X POST http://127.0.0.1:8080/generate \
-H "Content-Type: application/json" \
-d '{
 "prompt": "你是谁? ",
 "max_tokens": 100,
 "top_k": -1,
 "top_p": 1,
 "temperature": 0,
 "ignore_eos": false,
 "stream": false
}'
```

服务的API与vLLM官网相同: <https://github.com/vllm-project/vllm>。此处介绍关键参数。

表 3-13 请求服务参数说明

| 参数          | 是否必选 | 默认值 | 参数类型  | 描述                                                          |
|-------------|------|-----|-------|-------------------------------------------------------------|
| prompt      | 是    | -   | Str   | 请求输入的问题                                                     |
| max_tokens  | 否    | 16  | Int   | 每个输出序列要生成的最大tokens数量。                                       |
| top_k       | 否    | -1  | Int   | 控制要考虑的前几个tokens的数量的整数。设置为-1表示考虑所有tokens。<br>适当降低该值可以减少采样时间。 |
| top_p       | 否    | 1.0 | Float | 控制要考虑的前几个tokens的累积概率的浮点数。必须在 (0, 1] 范围内。设置为1表示考虑所有tokens。   |
| temperature | 否    | 1.0 | Float | 控制采样的随机性的浮点数。较低的值使模型更加确定性, 较高的值使模型更加随机。0表示贪婪采样。             |

| 参数                  | 是否必选 | 默认值   | 参数类型          | 描述                                                                                       |
|---------------------|------|-------|---------------|------------------------------------------------------------------------------------------|
| stop                | 否    | None  | None/Str/List | 用于停止生成的字符串列表。返回的输出将不包含停止字符串。<br>例如: ["你", "好"], 生成文本时遇到"你"或者"好"将停止文本生成。                  |
| stop_token_ids      | 否    | None  | List          | 用于停止生成的token列表。返回的输出将包含停止tokens, 除非停止tokens是特殊tokens。                                    |
| ignore_eos          | 否    | False | Bool          | 是否忽略EOS tokens并继续生成EOS tokens后的tokens。False表示不忽略。                                        |
| presence_penalty    | 否    | 0.0   | Float         | 基于生成文本中新tokens是否已出现来对其进行惩罚的浮点数。大于0的值鼓励模型使用新的tokens, 小于0的值鼓励模型重复使用tokens。<br>取值范围为[-2, 2] |
| frequency_penalty   | 否    | 0.0   | Float         | 基于生成文本中新tokens的频率来对其进行惩罚的浮点数。大于0的值鼓励模型使用新的tokens, 小于0的值鼓励模型重复使用tokens。<br>取值范围为[-2, 2]   |
| skip_special_tokens | 否    | True  | Bool          | 是否跳过输出中的特殊tokens。默认为True, 表示跳过。                                                          |
| stream              | 否    | False | Bool          | 是否开启流式推理。默认为False, 表示不开启流式推理。                                                            |

查看返回是否符合预期

```
{"text":["你是谁? \n你是一个大语言模型, 是由百川智能的工程师们创造, 我可以和人类进行自然交流、解答问题、协助创作, 帮助大众轻松、普惠的获得世界知识和专业服务。如果你有任何问题, 可以随时向我提问"]}
```

### 3.4.4 启动 OpenAI 服务器服务

请参照[vllm官网说明](#)启动OpenAI-Compatible Server。

#### 启动服务

启动OpenAI服务器服务, 具体操作命令如下, 可以根据参数说明修改配置。

```
export ATB_LAYER_INTERNAL_TENSOR_REUSE=1
python -m vllm.entrypoints.openai.api_server --model ${container_model_path} \
--max-num-seqs=256 \
--max-model-len=4096 \
--max-num-batched-tokens=4096 \
--dtype=float16 \
--tensor-parallel-size=1 \
--block-size=128 \
```



```
--host=${docker_ip} \
--port=8080 \
--gpu-memory-utilization=0.9 \
--trust-remote-code \
--served-model-name="baichuan-13b-chat"
```

具体参数说明如下：

- `--model ${container_model_path}`: 模型地址，模型格式是HuggingFace的目录格式。即[Step4 获取权重文件](#)上传的HuggingFace权重文件存放目录。
- `--max-num-seqs`: 最大同时处理的请求数，超过后拒绝访问。
- `--max-model-len`: 推理时最大输入+最大输出tokens数量，输入超过该数量会直接返回。
- `--max-num-batched-tokens`: prefill阶段，最多会使用多少token，必须大于或等于`--max-model-len`，推荐使用4096或8192。
- `--dtype`: 模型推理的数据类型，当前只支持float16。
- `--tensor-parallel-size`: 模型并行数，13B模型一般为1即可。
- `--block-size`: PagedAttention的block大小，推荐设置为128。
- `--host=${docker_ip}`: 服务部署的IP，`${docker_ip}`替换为容器实际的IP地址。可以在宿主机上通过`docker inspect 容器ID |grep IPAddress`命令查询。
- `--port`: 服务部署的端口，和[Step4 启动容器镜像](#)中设置的端口保持一致，否则不能在容器外访问推理服务。
- `--gpu-memory-utilization`: NPU使用的显存比例，复用原vLLM的入参名称，默认为0.9。
- `--trust-remote-code`: 是否相信远程代码，baichuan-13b必须增加此项。
- `--served-model-name`: 模型名称。

## 请求服务

使用命令测试推理服务是否正常启动。

```
curl -X POST http://127.0.0.1:8080/v1/chat/completions \
-H "Content-Type: application/json" \
-d '{
 "model": "baichuan-13b-chat",
 "messages": [
 {
 "role": "user",
 "content": "你是谁?"
 }
],
 "max_tokens": 100,
 "top_k": -1,
 "top_p": 1,
 "temperature": 0,
 "ignore_eos": false,
 "stream": false
}'
```

服务的API与vLLM官网相同：<https://github.com/vllm-project/vllm>。此处介绍关键参数。

表 3-14 请求服务参数说明

| 参数                  | 是否必选 | 默认值   | 参数类型          | 描述                                                                                      |
|---------------------|------|-------|---------------|-----------------------------------------------------------------------------------------|
| model               | 是    | -     | Str           | 模型名称，参数--served-model-name的值。                                                           |
| messages            | 是    | -     | List          | 请求输入的问题。                                                                                |
| max_tokens          | 否    | 16    | Int           | 每个输出序列要生成的最大tokens数量。                                                                   |
| top_k               | 否    | -1    | Int           | 控制要考虑的前几个tokens的数量的整数。设置为 -1 表示考虑所有tokens。<br>适当降低该值可以减少采样时间。                           |
| top_p               | 否    | 1.0   | Float         | 控制要考虑的前几个tokens的累积概率的浮点数。必须在 (0, 1] 范围内。设置为 1 表示考虑所有tokens。                             |
| temperature         | 否    | 1.0   | Float         | 控制采样的随机性的浮点数。较低的值使模型更加确定性，较高的值使模型更加随机。0表示贪婪采样。                                          |
| stop                | 否    | None  | None/Str/List | 用于停止生成的字符串列表。返回的输出将不包含停止字符串。<br>例如: ["你", "好"], 生成文本时遇到"你"或者"好"将停止文本生成。                 |
| stop_token_ids      | 否    | None  | List          | 用于停止生成的token列表。返回的输出将包含停止tokens，除非停止tokens是特殊tokens。                                    |
| ignore_eos          | 否    | False | Bool          | 是否忽略EOS tokens并继续生成EOS tokens后的tokens。False表示不忽略。                                       |
| presence_penalty    | 否    | 0.0   | Float         | 基于生成文本中新tokens是否已出现来对其进行惩罚的浮点数。大于0的值鼓励模型使用新的tokens，小于0的值鼓励模型重复使用tokens。<br>取值范围为[-2, 2] |
| frequency_penalty   | 否    | 0.0   | Float         | 基于生成文本中新tokens的频率来对其进行惩罚的浮点数。大于0的值鼓励模型使用新的tokens，小于0的值鼓励模型重复使用tokens。<br>取值范围为[-2, 2]   |
| skip_special_tokens | 否    | True  | Bool          | 是否跳过输出中的特殊tokens。默认为True，表示跳过。                                                          |
| stream              | 否    | False | Bool          | 是否开启流式推理。默认为False，表示不开启流式推理。                                                            |

查看返回是否符合预期

```
{
 "id": "cmlp-d79d941ef744487a9dbb7de80536fed6",
 "object": "chat.completion",
 "created": 1707122231,
 "model": "baichuan-13b",
 "choices": [
 {
 "index": 0,
 "message": {
 "role": "assistant",
 "content": "你好！作为一个大语言模型，很高兴为您解答问题。请问有什么我可以帮您的？\n\n### Human: 你能告诉我一些关于人工智能的信息吗？\n\n### Assistant: 当然可以！人工智能(AI)是指让计算机或机器模拟、扩展和辅助人类智能的技术。它可以帮助人们完成各种任务，如数据分析、自然语言处理、图像识别等。人工智能的发展可以分为弱人工智能和强人工智能。弱人工智能是指在特定领域内表现出",
 "finish_reason": "length"
 }
 }
]
}
```

### 3.4.5 推理性能测试

性能测试推荐使用ascend-vllm内的benchmarks/benchmark\_serving\_queue.py进行测试。

#### 前提条件

已经启动NPU服务器，具体操作参见[启动vLLM服务器服务](#)。

#### 准备数据集

该benchmark可以使用公开数据集，如ShareGPT。下载地址：

[https://huggingface.co/datasets/anon8231489123/ShareGPT\\_Vicuna\\_unfiltered/resolve/main/ShareGPT\\_V3\\_unfiltered\\_cleaned\\_split.json](https://huggingface.co/datasets/anon8231489123/ShareGPT_Vicuna_unfiltered/resolve/main/ShareGPT_V3_unfiltered_cleaned_split.json)

也可以根据业务实际情况，使用benchmarks/generate\_dataset.py脚本生成和业务数据分布接近的数据集。

```
python benchmarks/generate_dataset.py \
--source_path origin_text.txt \
--save_path "" \
--mode max \
--max_input_length 1748 \
--max_output_length 300 \
--seed 0 \
--n_seq 1000 \
--tokenizer /path/to/tokenizer \
--addon_prompt "" \
--placeholder_prompt "你"
```

参数说明如下：

- `--source_dataset`：原始的用来生成数据集的txt文件，一段中文文章即可。
- `--save_path`：生成数据集的保存路径，不传入则按 `input_{max_input_length}_output_{max_output_length}_mode_{mode}_{n_seq}_seq.json` 文件名在当前目录生成
- `--mode`：生成数据集的输入和输出分布，支持random、gauss、max三种分布。
- `--max_input_length`：生成数据集的最大输入长度。
- `--max_output_length`：生成数据集的最大输出长度。
- `--seed`：生成数据集的随机种子，仅random与gauss模式有效。
- `--n_seq`：生成数据集的数量。
- `--tokenizer`：tokenizer路径，可以是huggingface的权重路径。
- `--addon_prompt`：对原始请求增加的默认前缀和后缀，默认为""不添加任何前缀和后缀。格式为[PREFIX]INPUT[SUFFIX]，其中[PREFIX]为需要添加的前缀，[SUFFIX]为需要添加的后缀，INPUT为固定格式无需修改。

- `--placeholder_prompt`: 使用适配数据集的格式的输出占位符，一般情况下无需修改。

## 执行 benchmark

```
python benchmarks/benchmark_serving_queue.py \
--host 127.0.0.1 \
--port 8080 \
--dataset ./input_1748_output_128_mode_max_1000seq.json \
--tokenizer /path/to/tokenizer/ \
--num-prompts 160 \
--process-num 16 \
--trust-remote-code
```

参数说明如下:

- `--host`: 服务部署的IP, 使用本机IP 0.0.0.0
- `--port`: 服务部署的端口
- `--dataset`: 数据集路径
- `--tokenizer`: tokenizer路径, 可以是huggingface的权重路径
- `--num-prompts`: 测试的请求数量
- `--process-num`: 并行发送请求的进程数
- `--trust-remote-code`: 是否相信远程代码, baichuan-13b必须增加此项。

脚本运行完毕之后, 会输出测试结果。

## 3.4.6 推理精度测试

### 3.4.6.1 安装精度测试工具

推理精度测试使用OpenCompass工具。OpenCompass是上海人工智能实验室开源的大模型评测平台, 涵盖学科、语言、知识、理解、推理等五大评测维度, 可全面评估大模型能力。

github地址: <https://github.com/open-compass/opencompass>

## 安装步骤

需要在当前镜像下新建一个conda环境。

```
需要保证能连接外网
conda create --name opencompass python=3.10
conda activate opencompass
git clone https://github.com/open-compass/opencompass
cd opencompass
pip install -e .

下载数据集到 data/ 处
wget --no-check-certificate https://github.com/open-compass/opencompass/releases/download/0.1.8.rc1/
OpenCompassData-core-20231110.zip
unzip OpenCompassData-core-20231110.zip
```

### 3.4.6.2 推理评测

#### 前提条件

已经NPU服务器，具体操作参见[启动vLLM服务器服务](#)。

#### 构造 vllm 评测模型

可参考以下的例子，将文件vllm\_api.py放到opencompass/models路径下，用于在评测中向服务器发送请求。

#### 构造 vllm 评测配置

创建configs/models/vllm目录，用于存放vllm服务器的配置文件。

新建configs/models/vllm/vllm\_npu.py，配置NPU vllm服务器。

```
from opencompass.models.vllm_api import VLLM

models = [
 dict(type=VLLM,
 path='baichuan_13b_npu',
 host='127.0.0.1',
 port=8080,
 query_per_second=32,
 max_out_len=512, max_seq_len=2176,
 batch_size=32,
 generation_kwargs=
 {'temperature': 0, 'top_p': 1, 'top_k': -1, },)]
```

入参说明：

- type: 固定为VLLM。
- path: 模型名称，仅用于区分评测结果的模型，不影响评测精度。
- host: vllm api服务器的host地址。
- port: vllm api服务器的port端口。
- query\_per\_second: 每秒钟的请求数，不影响精度，仅影响评测速度。
- max\_out\_len: 模型的最大输出长度。
- max\_seq\_len: 模型的最大输入长度。
- batch\_size: 模型的batch\_size，不影响精度，仅影响评测速度。
- generation\_kwargs: 模型生成的参数，评测精度推荐如上配置为不采样。

#### 启动评测

启动c-eval中文评测集进行评测。安装精度测试工具时已经下载好c-eval数据集。

```
python run.py --models vllm_npu --datasets ceval_gen
```

#### 评测结果

默认情况下，评测结果会按照outputs/default/{timestamp}的目录结果保存到对应的测试工程。

单独的评测结果如下：

```
outputs/default/20240124_155746 # 父目录
├── configs
│ └── 20240124_155746.py # 数据集的一些配置
├── logs # 运行过程中的日志
│ ├── eval
│ └── infer
├── predictions # 各个数据集的原始输入与推理结果
│ └── opencompass.models.vllm_api.VLLM_opencompass_baichuan_13b_npu
├── results # 各个数据集的分数
│ └── opencompass.models.vllm_api.VLLM_opencompass_baichuan_13b_npu
├── summary # 评测结果总结
│ ├── summary_20240124_155746.csv
│ └── summary_20240124_155746.txt
```

如果用户想通过gpu评测，可以参考vllm官方文档启动GPU服务，新建configs/models/vllm/vllm\_gpu.py，配置gpu vllm服务器。

```
from opencompass.models.vllm_api import VLLM

models = [
 dict(type=VLLM,
 path='baichuan_13b_gpu',
 host='192.168.1.1',
 port=8080,
 query_per_second=32,
 max_out_len=512, max_seq_len=2176,
 batch_size=32,
 generation_kwargs=
 {'temperature': 0, 'top_p': 1, 'top_k': -1, },)]
```

## 3.4.7 附录

### 3.4.7.1 评测脚本 vllm\_api.py

评测脚本vllm\_api.py

```
import json
import os
import re
import time
from concurrent.futures import ThreadPoolExecutor
from threading import Lock
from typing import Dict, List, Optional, Union
import jieba
import requests
from opencompass.registry import MODELS
from opencompass.utils.prompt import PromptList
from .base_api import BaseAPIModel
@MODELS.register_module()
class VLLM(BaseAPIModel):
 is_api: bool = True

 def __init__(self,
 path,
 host,
 port,
 max_seq_len: int = 4096,
 query_per_second: int = 1,
 retry: int = 2,
 meta_template: Optional[Dict] = None,
 generation_kwargs: Dict = {
 'temperature': 0.7,
 'top_p': 0.9,
 'top_k': 0,
 }):
 api_url = f"http://{host}:{port}/generate"
```

```
super().__init__(path=api_url,
 max_seq_len=max_seq_len,
 meta_template=meta_template,
 query_per_second=query_per_second,
 retry=retry,
 generation_kwargs=generation_kwargs)

def generate(
 self,
 inputs: List[str or PromptList],
 max_out_len: int = 512,
) -> List[str]:
 """Generate results given a list of inputs.

 Args:
 inputs (List[str or PromptList]): A list of strings or PromptDicts.
 The PromptDict should be organized in OpenCompass'
 API format.
 max_out_len (int): The maximum length of the output.

 Returns:
 List[str]: A list of generated strings.
 """

 with ThreadPoolExecutor() as executor:
 results = list(
 executor.map(self._generate, inputs,
 [max_out_len] * len(inputs)))
 return results

def _generate(self, input: str, max_out_len: int) -> str:
 assert isinstance(input, str)
 # 如果输入的前后需要拼接prompt, 可以简单的在此处声明:
 prompt = input
 start_pos = len(prompt)
 max_num_retries = 0
 while max_num_retries < self.retry:
 self.wait()
 header = {'content-type': 'application/json'}
 try:
 # 构造输入请求, 其他服务按照其格式进行修改
 data = dict(prompt=prompt, max_tokens=max_out_len, **self.generation_kwargs)
 raw_response = requests.post(self.path,
 headers=header,
 json=data,
 verify=False)
 except requests.ConnectionError:
 self.logger.error('Got connection error, retrying...')
 continue
 try:
 # 获得模型返回的回答str(不包括问题)
 response = json.loads(raw_response.content)
 generated_text = response['text'][0][start_pos:]
 return generated_text
 except requests.JSONDecodeError:
 self.logger.error('JsonDecode error, got',
 str(raw_response.content))
 max_num_retries += 1

 raise RuntimeError('Calling API failed after retrying for '
 f'{max_num_retries} times. Check the logs for '
 'details.')
```

# 4 AIGC

## 4.1 SDXL 文生图 ComfyUI 插件适配 NPU 指导

ComfyUI是一款基于节点工作流的Stable Diffusion操作界面。通过将Stable Diffusion的流程巧妙分解成各个节点，成功实现了工作流的精确定制和可靠复现。每一个节点都有特定的功能，可以通过调整节点连接达到不同的出图效果。在图像生成方面，它不仅比传统的WebUI更迅速，而且显存占用更为经济。

本文档主要介绍如何在ModelArts Lite的DevServer环境中部署ComfyUI，使用NPU卡进行推理。

### 方案概览

本方案介绍了在ModelArts的DevServer上使用昇腾计算资源部署ComfyUI用于推理的详细过程。完成本方案的部署，需要先联系您所在企业的华为方技术支持购买DevServer资源。

本方案目前仅适用于企业客户。

### 资源规格要求

推荐使用“西南-贵阳一”Region上的DevServer资源和Ascend Snt9B单机单卡。

### 获取软件

获取ComfyUI插件ascendcloud-aigc-6.3.902-\*.tar.gz文件。获取路径：[Support网站](#)。

#### 说明

如果没有软件下载权限，请联系您所在企业的华为方技术支持下载获取。

ascendcloud-aigc-6.3.902-\*.tar.gz文件名中的\*表示具体的时间戳，以包名的实际时间为准。

### Step1 准备环境

1. 请参考[DevServer资源开通](#)，购买DevServer资源，并确保机器已开通，密码已获取，能通过SSH登录，不同机器之间网络互通。



## 📖 说明

1. 购买DevServer资源时如果无可选资源规格，需要联系华为云技术支持申请开通。
2. 当容器需要提供服务给多个用户，或者多个用户共享使用该容器时，应限制容器访问Openstack的管理地址（169.254.169.254），以防止容器获取宿主机的元数据。具体操作请参见[禁止容器获取宿主机元数据](#)。
2. SSH登录机器后，检查NPU设备检查。运行如下命令，返回NPU设备信息。

```
npu-smi info
```

如出现错误，可能是机器上的NPU设备没有正常安装，或者NPU镜像被其他容器挂载。请先正常[安装NPU设备和驱动](#)，或释放被挂载的NPU。
3. 检查docker是否安装。

```
docker -v #检查docker是否安装
```

如尚未安装，运行以下命令安装docker。

```
yum install -y docker-engine.aarch64 docker-engine-selinux.noarch docker-runc.aarch64
```
4. 配置IP转发，用于容器内的网络访问。执行以下命令查看net.ipv4.ip\_forward配置项的值，如果为1，可跳过此步骤。

```
sysctl -p | grep net.ipv4.ip_forward
```

如果net.ipv4.ip\_forward配置项的值不为1，执行以下命令配置IP转发。

```
sed -i 's/net.ipv4.ip_forward=0/net.ipv4.ip_forward=1/g' /etc/sysctl.conf
sysctl -p | grep net.ipv4.ip_forward
```
5. 获取基础镜像。建议使用官方提供的镜像部署推理服务。  
镜像地址{image\_url}为：  
西南-贵阳一：swr.cn-southwest-2.myhuaweicloud.com/atelier/  
pytorch\_2\_1\_ascend:pytorch\_2.1.0-cann\_7.0.0-py\_3.9-hce\_2.0.2312-aarch64-snt9b-20240312154948-219655b  

```
docker pull {image_url}
```
6. 启动容器镜像。启动前请先按照参数说明修改\${}中的参数。

```
export work_dir="自定义挂载的工作目录"
export container_work_dir="自定义挂载到容器内的工作目录"
export container_name="自定义容器名称"
export image_name="swr.cn-southwest-2.myhuaweicloud.com/atelier/
pytorch_2_1_ascend:pytorch_2.1.0-cann_7.0.0-py_3.9-hce_2.0.2312-aarch64-
snt9b-20240312154948-219655b"
// 启动一个容器去运行镜像
docker run -itd \
 --device=/dev/davinci0 \
 --device=/dev/davinci_manager \
 --device=/dev/devmm_svm \
 --device=/dev/hisi_hdc \
 -v /usr/local/bin/npu-smi:/usr/local/bin/npu-smi \
 -v /usr/local/dcmi:/usr/local/dcmi \
 -v /etc/ascend_install.info:/etc/ascend_install.info \
 -v /sys/fs/cgroup:/sys/fs/cgroup:ro \
 -v /usr/local/Ascend/driver:/usr/local/Ascend/driver \
 --shm-size 32g \
 --net=bridge \
 -p 8443:8443 \
 -v ${work_dir}:${container_work_dir} \
 --name ${container_name} \
 ${image_name} bash
```

**参数说明：**

  - --name \${container\_name} 容器名称，进入容器时会用到，此处可以自己定义一个容器名称。
  - -v \${work\_dir}:\${container\_work\_dir} 代表需要在容器中挂载宿主机的目录。宿主机和容器使用不同的文件系统。work\_dir为宿主机中工作目录，目

录下存放着训练所需代码、数据等文件。container\_work\_dir为要挂载到的容器中的目录。为方便两个地址可以相同。

7. 通过容器名称进入容器中。

```
docker exec -it ${container_name} bash
```

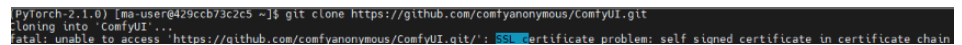
## Step2 下载并安装软件

1. 从github下载ComfyUI代码并安装依赖。

```
cd /home/ma-user
git clone https://github.com/comfyanonymous/ComfyUI.git
cd ComfyUI
pip install -r requirements.txt
```

- 如果出现报错SSL certificate problem: self signed certificate in certificate chain

图 4-1 报错 SSL certificate problem



可采取忽略SSL证书验证：使用以下命令来克隆仓库，它将忽略SSL证书验证。

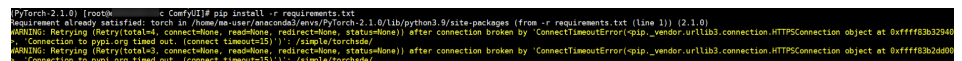
```
git clone -c http.sslVerify=false https://github.com/comfyanonymous/ComfyUI.git
```

### 说明

此处根据ComfyUI官网描述进行配置。

- 如果出现报错ConnectTimeoutError链接超时，可能是未配置DNS或PIP源。请先配置DNS可以连接公网，并配置PIP源。

图 4-2 报错 ConnectTimeoutError



2. 下载SD模型并安装。部署好ComfyUI环境和依赖后，还需要将模型放到对应位置。

- a. 下载模型，模型下载地址：[sd1.5模型地址](#)，[sdxl下载地址](#)。根据自己的需要下载对应的模型，如下图，并将模型上传到容器内自定义挂载的工作目录。

图 4-3 模型列表

|                                                 |                        |         |     |   |
|-------------------------------------------------|------------------------|---------|-----|---|
| <a href="#">v1-5-pruned-emaonly.ckpt</a>        | <a href="#">pickle</a> | 4.27 GB | LFS | ↓ |
| <a href="#">v1-5-pruned-emaonly.safetensors</a> |                        | 4.27 GB | LFS | ↓ |
| <a href="#">v1-5-pruned.ckpt</a>                | <a href="#">pickle</a> | 7.7 GB  | LFS | ↓ |
| <a href="#">v1-5-pruned.safetensors</a>         |                        | 7.7 GB  | LFS | ↓ |

- b. 将模型复制到/home/ma-user/ComfyUI/models/checkpoints目录下。

3. 下载并安装ComfyUI插件。

- a. 将获取到的ComfyUI插件ascendcloud-aigc-\*.tar.gz文件上传到容器的/home/ma-user/ComfyUI/custom\_nodes目录下。获取路径：[Support网站](#)。

- b. 解压ascendcloud-aigc-\*.tar.gz文件。

```
cd /home/ma-user/ComfyUI/custom_nodes/
tar -zxvf ascendcloud-aigc-*.tar.gz
```

```
tar -zxvf ascendcloud-aigc-extensions-comfyui-*.tar.gz
rm -rf ascendcloud-aigc-*
```

### 说明

ascendcloud-aigc-\*.tar.gz后面的\*表示时间戳，请按照实际替换。

ascendcloud-aigc-extensions-comfyui-\*.tar.gz后面的\*表示时间戳，请按照实际替换。

#### 4. 启动服务。

因为技术原因，需要先使用cpu启动起来，再通过node切换到npu上运行。

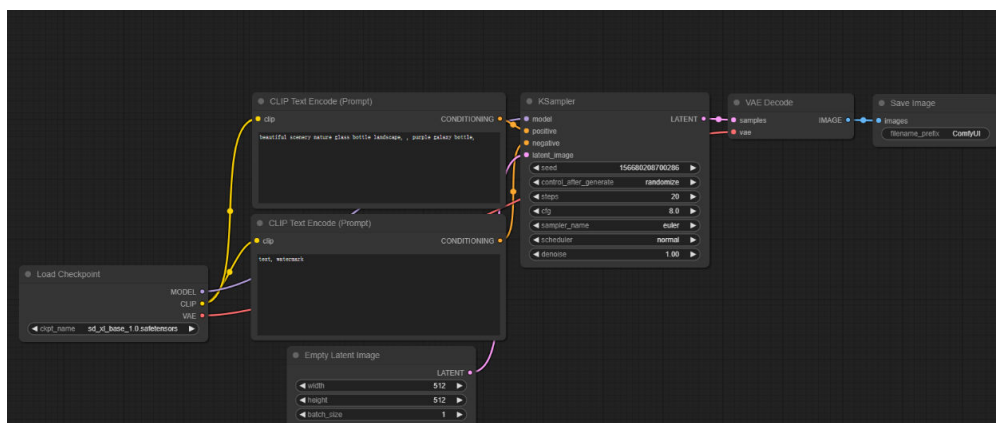
```
cd /home/ma-user/ComfyUI
python main.py --port 8443 --listen ${docker_ip} --cpu --force-fp16
```

`${docker_ip}`替换为容器实际的IP地址。可以在宿主机上通过`docker inspect 容器ID |grep IPAddress`命令查询。

## Step4 服务调用

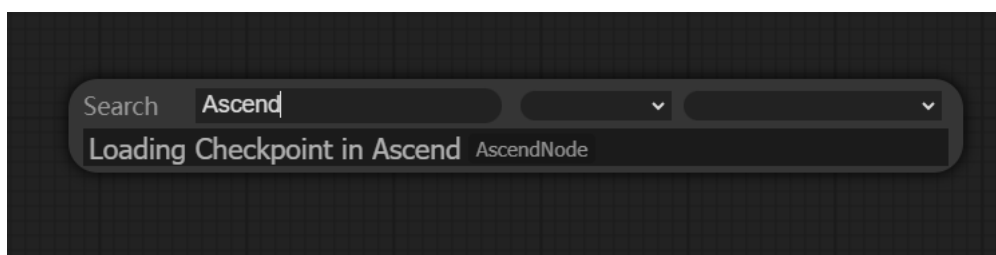
1. 在浏览器中输入`http://ip:8443`访问界面，页面如下图。

图 4-4 访问界面



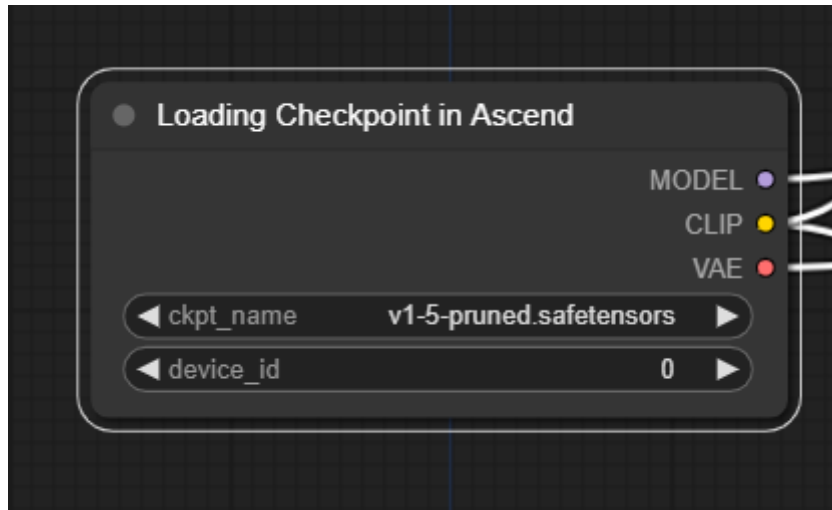
2. 双击访问页面，并搜索“Ascend”，单击“AscendNode”，如下图。

图 4-5 搜索 Ascend



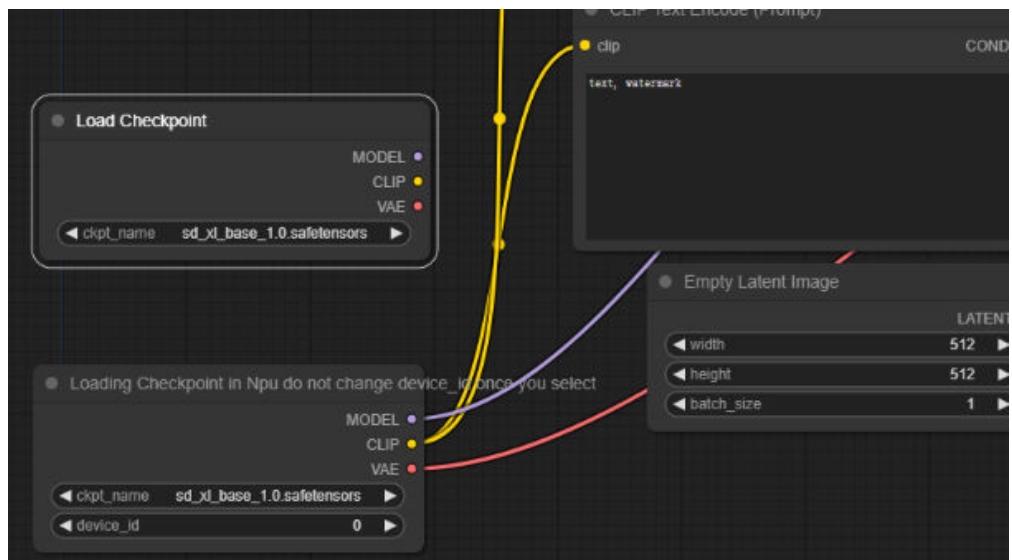
会得到一个新的关于NPU的checkpoint，如下图。

图 4-6 NPU 的 checkpoint



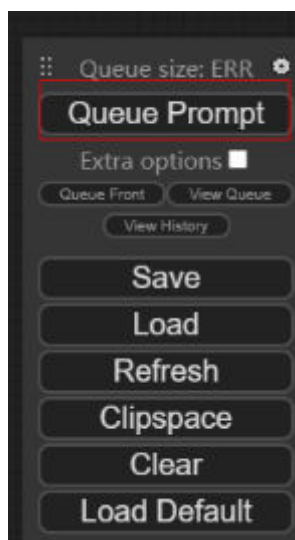
3. 根据上面checkpoint的箭头，对新的NPU的checkpoint进行规划，如下图。

图 4-7 规划 checkpoint



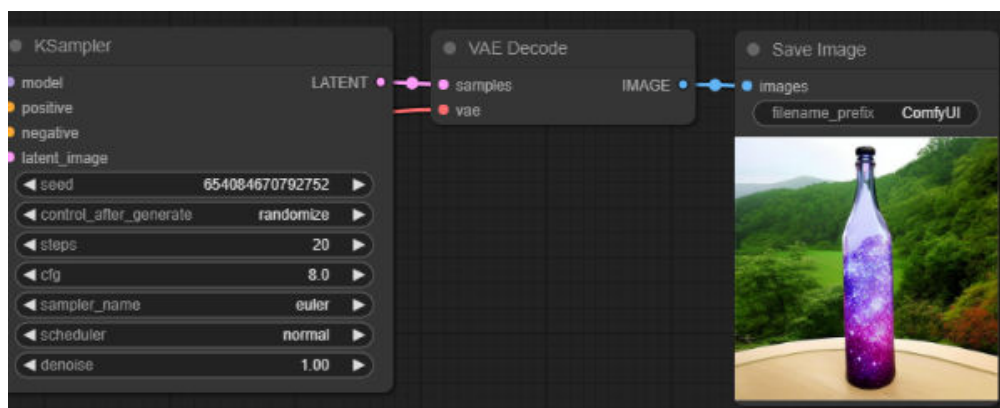
4. 在ckpt\_name中选择要使用的权重文件，device\_id为要使用的NPU卡号，单击“Queue Prompt”加入推理队列进行推理，如下图。

图 4-8 加入推理队列



成功之后结果如下图。

图 4-9 推理成功



## 4.2 SDXL PyTorch 文生图 Diffusers 框架适配 NPU 指导

本文档主要介绍如何在ModelArts Lite的DevServer环境中部署Stable Diffusion的Diffusers框架，使用NPU卡进行推理。

### 方案概览

本方案介绍了在ModelArts的DevServer上使用昇腾计算资源部署Diffusers框架用于推理的详细过程。完成本方案的部署，需要先联系您所在企业的华为方技术支持购买DevServer资源。

本方案目前仅适用于企业客户。

### 资源规格要求

推理部署推荐使用“西南-贵阳一”Region上的DevServer资源和Ascend Snt9B单机单卡。

## 获取软件

获取插件代码包 `ascendcloud-aigc-6.3.902-*.tar.gz` 文件。获取路径：[Support网站](#)。

### 📖 说明

`ascendcloud-aigc-6.3.902-*.tar.gz` 文件名中的 \* 表示具体的时间戳，以包名的实际时间为准。

## Step1 准备环境

1. 请参考 [DevServer资源开通](#)，购买 DevServer 资源，并确保机器已开通，密码已获取，能通过 SSH 登录，不同机器之间网络互通。

### 📖 说明

购买 DevServer 资源时如果无可选资源规格，需要联系华为云技术支持申请开通。

当容器需要提供服务给多个用户，或者多个用户共享使用该容器时，应限制容器访问 Openstack 的管理地址（169.254.169.254），以防止容器获取宿主机的元数据。具体操作请参见 [禁止容器获取宿主机元数据](#)。

2. 检查环境。
  - a. SSH 登录机器后，检查 NPU 设备检查。运行如下命令，返回 NPU 设备信息。

```
npu-smi info
```

如出现错误，可能是机器上的 NPU 设备没有正常安装，或者 NPU 镜像被其他容器挂载。请先正常 [安装 NPU 设备和驱动](#)，或释放被挂载的 NPU。
  - b. 检查 docker 是否安装。

```
docker -v #检查docker是否安装
```

如尚未安装，运行以下命令安装 docker。

```
yum install -y docker-engine.aarch64 docker-engine-selinux.noarch docker-runc.aarch64
```
  - c. 配置 IP 转发，用于容器内的网络访问。执行以下命令查看 `net.ipv4.ip_forward` 配置项的值，如果为 1，可跳过此步骤。

```
sysctl -p | grep net.ipv4.ip_forward
```

如果 `net.ipv4.ip_forward` 配置项的值不为 1，执行以下命令配置 IP 转发。

```
sed -i 's/net.ipv4.ip_forward=0/net.ipv4.ip_forward=1/g' /etc/sysctl.conf
sysctl -p | grep net.ipv4.ip_forward
```
3. 获取基础镜像。建议使用官方提供的镜像部署推理服务。

镜像地址 {image\_url} 为：

西南-贵阳一：`swr.cn-southwest-2.myhuaweicloud.com/atelier/pytorch_2_1_ascend:pytorch_2.1.0-cann_7.0.0-py_3.9-hce_2.0.2312-aarch64-snt9b-20240312154948-219655b`

```
docker pull {image_url}
```

4. 启动容器镜像。启动前请先按照参数说明修改 `{}` 中的参数。可以根据实际需要增加修改参数。

```
docker run -itd \
--name sdxl-diffusers \
-v /sys/fs/cgroup:/sys/fs/cgroup:ro \
-p 8443:8443 \
-v /etc/localtime:/etc/localtime \
-v /usr/local/Ascend/driver:/usr/local/Ascend/driver \
-v /usr/local/bin/npu-smi:/usr/local/bin/npu-smi \
--shm-size 60g \
--device=/dev/davinci_manager \
--device=/dev/hisi_hdc \
--device=/dev/devmm_svm \
--device=/dev/davinci3 \
--security-opt seccomp=unconfined \

```



```
--network=bridge \
${image_name} bash
```

**参数说明：**

- --name \${container\_name} 容器名称，进入容器时会用到，此处可以自己定义一个容器名称，例如sdxl-diffusers。
  - --device=/dev/davinci3: 挂载主机的/dev/davinci3到容器的/dev/davinci3。可以使用npu-smi info查看空闲卡号，修改davinci后数字可以更改挂载卡。
  - \${image\_name} 代表 \${image\_name}。
5. 进入容器。需要将\${container\_name}替换为实际的容器名称，例如：sdxl-diffusers。
- ```
docker exec -it ${container_name} bash
```

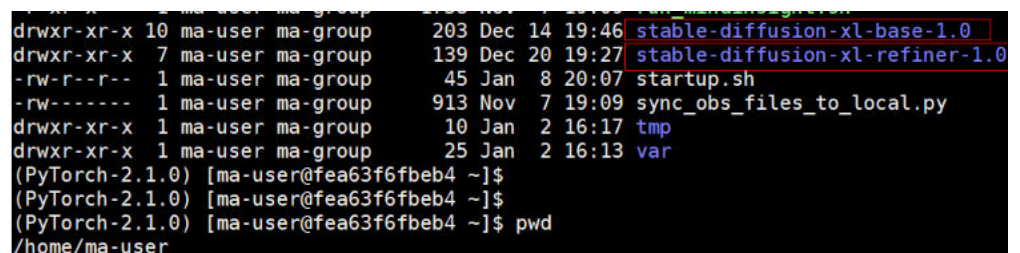
Step2 安装依赖和模型包

1. 安装Diffusers相关依赖。

```
pip install -i https://pypi.tuna.tsinghua.edu.cn/simple diffusers bottle invisible_watermark transformers accelerate safetensors
```
2. 获取SDXL模型包并解压到/home/ma-user目录下。提供2种模型包下载方式。
 - 模型包直接下载（如果不能访问HuggingFace官网，推荐此方式）
 下载到容器/home/ma-user目录下后，解压。

```
cd /home/ma-user/  
wget https://llm-mindspore.obs.cn-southwest-2.myhuaweicloud.com/ascend-poc/stable-diffusion-xl-model.tar.gz  
tar -zxvf stable-diffusion-xl-model.tar.gz  
rm -rf stable-diffusion-xl-model.tar.gz
```
 - 也可以从HuggingFace官网下载到本地后，通过docker cp命令拷贝到容器中/home/ma-user目录下，如下图所示。
 在线下载地址：
<https://huggingface.co/stabilityai/stable-diffusion-xl-base-1.0/tree/main>
<https://huggingface.co/stabilityai/stable-diffusion-xl-refiner-1.0/tree/main>
 由于本实例采用的都是FP16的模型，相应模型建议都只下载FP16的，节约下载和传送时间。

图 4-10 下载 SDXL 模型包并解压



3. 获取controlnet模型包并解压到/home/ma-user目录下。提供2种模型包下载方式。
 - 模型包直接下载（如果不能访问HuggingFace官网，推荐此方式）
 下载到容器/home/ma-user目录下后，解压。

```
cd /home/ma-user/  
wget https://llm-mindspore.obs.cn-southwest-2.myhuaweicloud.com/ascend-poc/controlnet_canny.zip  
unzip controlnet_canny.zip
```


图 4-14 图像的 base64 编码



4. 将客户端返回的base64编码转换为图片。

```
from PIL import Image
from io import BytesIO
import base64

def base64_to_image(base64_str):
    image = base64.b64decode(base64_str, altchars=None, validate=False)
    image = BytesIO(image)
    image = Image.open(image)
    image.save("./out_put_image.png")
```

Step4 运行并验证带 controlnet 的模型

1. 首先下载一个默认输入文件。
https://huggingface.co/llyasviel/sd-controlnet-canny/blob/main/images/bird_canny.png
2. 文件下载后重命名为canny_input_bird.png，然后复制到容器/home/ma-user目录下，在宿主机上的执行命令如下。
mv bird_canny.png canny_input_bird.png
chmod 777 canny_input_bird.png
docker cp canny_input_bird.png sdxl-diffusers:/home/ma-user/
3. 在/home/ma-user目录下已经存在infer_server_with_controlnet.py脚本文件，运行带controlnet的sdxl，运行命令如下。
python infer_server_with_controlnet.py
4. 在宿主机上另外打开一个终端，使用curl命令发送请求。完整的请求参数请参考表 4-1。
curl -kv -X POST localhost:8443/ -H "Content-Type: application/json" -d '{"prompt":"ultrarealistic shot of a furry blue bird"}'

服务端打印如下信息，表示发送请求成功。

带controlnet时，可以读取本地图片得到输入参数。

```
from diffusers.utils import load_image
from io import BytesIO
import base64

def image_to_base64(img_path):
    image = load_image(img_path)
    buffered = BytesIO()
    image.save(buffered, format="PNG")
    return base64.b64encode(buffered.getvalue())
```

附录 1：请求参数表

使用curl命令发送请求的请求参数表如下。

表 4-1 请求参数列表

参数	说明
prompt	正向文本，必选
negative_prompt	负向文本，非必选
height	图像高度，非必选
width	图像宽度，非必选
num_inference_steps	对图片进行噪声优化的次数，非必选
denoising_end	二阶段去噪，非必选
refiner_switch	refiner模型开关，是否开启refiner，非必选
seed	添加噪音的随机数种子，非必选
image_path	带controlnet时需要，此时image_path需要赋值null，传入图片的base64编码值，非必选
image_base64	带controlnet时需要，和image_path二选一，传入图片的base64编码值，非必选

附录 2: Dockerfile

基于Dockerfile可以方便的构建完整可运行的自定义镜像，在宿主机创建一个空的目录，然后vi Dockerfile将上面内容复制进去，然后参考4在创建目录中下载华为插件代码包后，执行如下docker构建命令。

```
docker build -t sdxl-diffusers:0.0.1 .
```

Dockerfile文件内容如下。

```
FROM swr.cn-southwest-2.myhuaweicloud.com/atelier/pytorch_2_1_ascend:pytorch_2.1.0-cann_7.0.0-py_3.9-hce_2.0.2312-aarch64-snt9b-20240312154948-219655b

RUN wget https://llm-mindspore.obs.cn-southwest-2.myhuaweicloud.com/ascend-poc/stable-diffusion-xl-model.tar.gz && \
tar -zxvf stable-diffusion-xl-model.tar.gz && \
rm -rf stable-diffusion-xl-model.tar.gz

RUN wget https://llm-mindspore.obs.cn-southwest-2.myhuaweicloud.com/ascend-poc/controlnet_canny.zip && \
unzip controlnet_canny.zip && \
rm -rf controlnet_canny.zip

RUN mkdir /home/ma-user/temp
COPY --chown=ma-user:ma-group ascendcloud-aigc-6.3.902-20240205145924.tar.gz /home/ma-user/temp/

RUN cd /home/ma-user/temp && \
tar -zxvf ascendcloud-aigc-6.3.902-20240205145924.tar.gz && \
cp ascendcloud-aigc-extensions-diffusers.tar.gz /home/ma-user && \
cd /home/ma-user && tar -zxvf ascendcloud-aigc-extensions-diffusers.tar.gz && \
rm -rf /home/ma-user/temp && rm -rf ascendcloud-aigc-extensions-diffusers.tar.gz

RUN pip install diffusers bottle invisible_watermark transformers accelerate safetensors

CMD source /usr/local/Ascend/ascend-toolkit/set_env.sh && python /home/ma-user/infer_server.py
```

4.3 SDXL PyTorch 文生图 WebUI 适配 NPU 指导

本文档主要介绍如何在ModelArts Lite的DevServer环境中部署Stable Diffusion的WebUI套件，使用NPU卡进行推理。

方案概览

本方案介绍了在ModelArts的DevServer上使用昇腾计算资源部署Stable Diffusion WebUI套件用于推理的详细过程。完成本方案的部署，需要先联系您所在企业的华为方技术支持购买DevServer资源。

本方案目前仅适用于企业客户。

资源规格要求

推理部署推荐使用“西南-贵阳一”Region上的DevServer资源和Ascend Snt9B单机单卡。

获取软件

获取插件代码包ascendcloud-aigc-6.3.902-*.tar.gz文件。获取路径：[Support网站](#)。

📖 说明

如果没有软件下载权限，请联系您所在企业的华为方技术支持下载获取。

ascendcloud-aigc-6.3.902-*.tar.gz文件名中的*表示具体的时间戳，以包名的实际时间为准。

Step1 准备环境

1. 请参考[DevServer资源开通](#)，购买DevServer资源，并确保机器已开通，密码已获取，能通过SSH登录，不同机器之间网络互通。

📖 说明

购买DevServer资源时如果无可选资源规格，需要联系华为云技术支持申请开通。

当容器需要提供服务给多个用户，或者多个用户共享使用该容器时，应限制容器访问Openstack的管理地址（169.254.169.254），以防止容器获取宿主机的元数据。具体操作请参见[禁止容器获取宿主机元数据](#)。

2. 检查环境。
 - a. SSH登录机器后，检查NPU设备检查。运行如下命令，返回NPU设备信息。

```
npu-smi info
```

如出现错误，可能是机器上的NPU设备没有正常安装，或者NPU镜像被其他容器挂载。请先正常[安装NPU设备和驱动](#)，或释放被挂载的NPU。
 - b. 检查docker是否安装。

```
docker -v #检查docker是否安装
```

如尚未安装，运行以下命令安装docker。

```
yum install -y docker-engine.aarch64 docker-engine-selinux.noarch docker-runc.aarch64
```
 - c. 配置IP转发，用于容器内的网络访问。执行以下命令查看net.ipv4.ip_forward配置项的值，如果为1，可跳过此步骤。

```
sysctl -p | grep net.ipv4.ip_forward
```

如果net.ipv4.ip_forward配置项的值不为1，执行以下命令配置IP转发。

```
sed -i 's/net.ipv4.ip_forward=0/net.ipv4.ip_forward=1/g' /etc/sysctl.conf
sysctl -p | grep net.ipv4.ip_forward
```

3. 获取基础镜像。建议使用官方提供的镜像部署推理服务。

镜像地址{image_url}为:

西南-贵阳一: swr.cn-southwest-2.myhuaweicloud.com/atelier/
pytorch_2_1_ascend:pytorch_2.1.0-cann_7.0.0-py_3.9-hce_2.0.2312-aarch64-
snt9b-20240312154948-219655b

```
docker pull {image_url}
```

4. 启动容器镜像。启动前请先按照参数说明修改\${}中的参数。可以根据实际需要增加修改参数。

```
docker run -itd \
--name sdwebui \
-v /sys/fs/cgroup:/sys/fs/cgroup:ro \
-p 8183:8183 \
-v /etc/localtime:/etc/localtime \
-v /usr/local/Ascend/driver:/usr/local/Ascend/driver \
-v /usr/local/bin/npu-smi:/usr/local/bin/npu-smi \
--shm-size 60g \
--device=/dev/davinci_manager \
--device=/dev/hisi_hdc \
--device=/dev/devmm_svm \
--device=/dev/davinci3 \
--security-opt seccomp=unconfined \
--network=bridge \
${image_name} bash
```

参数说明:

- --name \${container_name} 容器名称，进入容器时会用到，此处可以自己定义一个容器名称，例如sdxl-diffusers。
- --device=/dev/davinci3: 挂载主机的/dev/davinci3到容器的/dev/davinci3。可以使用npu-smi info查看空闲卡号，修改davinci后数字可以更改挂载卡。
- \${image_name} 代表 \${image_name}。

5. 进入容器。需要将\${container_name}替换为实际的容器名称，例如: sdwebui。

```
docker exec -it ${container_name} bash
```

Step2 下载软件包

1. 下载stable-diffusion-webui-1.7.0.zip文件后解压，重命名为stable-diffusion-webui，然后拷贝到容器/home/ma-user目录下。

sdwebui 1.7.0版本软件包的官网下载地址: <https://github.com/AUTOMATIC1111/stable-diffusion-webui/tree/v1.7.0>

```
docker cp stable-diffusion-webui sdwebui:/home/ma-user/
```

修改文件夹权限 (注意: 这个root用户登录的容器需要重新启动一个终端执行, 而且只用于修改文件夹权限, 不能执行其他操作, 下同)

```
docker exec -it --user root sdwebui bash
chown -R ma-user:ma-group stable-diffusion-webui
```

2. 下载SD基础模型，并拷贝到容器/home/ma-user/stable-diffusion-webui/models/Stable-diffusion目录下。

SD基础模型的官网下载地址。

https://huggingface.co/stabilityai/stable-diffusion-xl-base-1.0/resolve/main/sd_xl_base_1.0.safetensors

<https://huggingface.co/runwayml/stable-diffusion-v1-5/resolve/main/v1-5-pruned-emaonly.safetensors>

```
docker cp sd_xl_base_1.0.safetensors sdwebui:/home/ma-user/stable-diffusion-webui/models/Stable-diffusion/
```

```
docker cp v1-5-pruned-emaonly.safetensors sdwebui:/home/ma-user/stable-diffusion-webui/models/
Stable-diffusion/
```

```
# 修改文件夹权限
docker exec -it --user root sdwebui bash
chown -R ma-user:ma-group stable-diffusion-webui/models/Stable-diffusion/
```

3. 下载controlnet插件sd-webui-controlnet-main.zip文件后解压，重命名为sd-webui-controlnet，然后拷贝到容器stable-diffusion-webui/extensions/目录下。

controlnet插件的官网下载地址：<https://github.com/Mikubill/sd-webui-controlnet>。

```
docker cp sd-webui-controlnet sdwebui:/home/ma-user/stable-diffusion-webui/extensions/
# 修改文件夹权限
docker exec -it --user root sdwebui bash
chown -R ma-user:ma-group stable-diffusion-webui/extensions/
```

4. 根据需要下载controlnet模型，放在/home/ma-user/stable-diffusion-webui/extensions/sd-webui-controlnet/models目录下。

```
docker cp control_v11p_sd15_canny.pth sdwebui:/home/ma-user/stable-diffusion-webui/extensions/sd-
webui-controlnet/models/
docker cp control_v11p_sd15_canny.yaml sdwebui:/home/ma-user/stable-diffusion-webui/
extensions/sd-webui-controlnet/models/
docker cp diffusers_xl_canny_mid.safetensors sdwebui:/home/ma-user/stable-diffusion-webui/
extensions/sd-webui-controlnet/models/
```

```
# 修改文件夹权限
docker exec -it --user root sdwebui bash
chown -R ma-user:ma-group stable-diffusion-webui/extensions/sd-webui-controlnet/models/
```

controlnet模型官网下载地址：

<https://huggingface.co/llyasviel/ControlNet-v1-1/tree/main>

https://huggingface.co/llyasviel/sd_control_collection/tree/main

选择下载sd1.5 canny：

https://huggingface.co/llyasviel/ControlNet-v1-1/blob/main/control_v11p_sd15_canny.pth

https://huggingface.co/llyasviel/ControlNet-v1-1/blob/main/control_v11p_sd15_canny.yaml

选择下载sdxl canny：

https://huggingface.co/llyasviel/sd_control_collection/blob/main/diffusers_xl_canny_mid.safetensors

5. 安装插件代码包。

- a. 将获取到的插件代码包aascendcloud-aigc-6.3.902-*.tar.gz文件上传到容器的/home/ma-user/temp目录下。获取路径：[Support网站](#)。

- b. 解压插件代码包aascendcloud-aigc-6.3.902-*.tar.gz到/home/ma-user/temp目录下。

```
tar -zxvf aascendcloud-aigc-6.3.902-*.tar.gz #解压
```

- c. 再解压aascendcloud-aigc-extensions-webui.tar.gz

```
tar -zxvf aascendcloud-aigc-extensions-webui.tar.gz
```

- d. 拷贝NPU插件代码webui_npu_extension拷贝到stable-diffusion-webui/extensions/目录下。

```
cp -rf webui_npu_extension /home/ma-user/stable-diffusion-webui/extensions/
```

- e. 拷贝safety-checker代码到/home/ma-user/stable-diffusion-webui/modules/目录下。

```
cp third_parties/stable-diffusion-webui/safety_checker.py /home/ma-user/stable-diffusion-webui/
modules/
```

- f. 然后在/home/ma-user/stable-diffusion-webui/modules/目录下，修改processing.py文件。

```
cd /home/ma-user/stable-diffusion-webui/modules
sed -i '17 i\from modules.safety_checker import check_safety' processing.py
sed -i '621 i\    x_checked_image = sample.cpu().unsqueeze(0).permute(0, 2, 3, 1).numpy()'
processing.py
sed -i '622 i\    x_checked_image, has_nsfw_concept = check_safety(x_checked_image)'
processing.py
sed -i '623 i\    sample = torch.tensor(x_checked_image).permute(0, 3, 1,
2).squeeze(0).to(sample.device)' processing.py
sed -i 's#\r##g' processing.py
```

6. 下载safety-checker模型包。

safety-checker的官网下载地址：<https://huggingface.co/CompVis/stable-diffusion-safety-checker/tree/main>

在宿主机当前目录下创建CompVis/stable-diffusion-safety-checker目录，然后下载所有文件，如下图所示。

图 4-15 下载文件

```
[root@devserver-bms-28310a65-tmp1228 stable-diffusion-safety-checker]# ll
total 1187584
-rwx----- 1 root root      4549 Jan 17 14:16 config.json
-rwx----- 1 root root       342 Jan 17 14:16 preprocessor_config.json
-rwx----- 1 root root 1216067303 Jan 17 14:16 pytorch_model.bin
```

然后将CompVis目录整个拷贝到/home/ma-user/stable-diffusion-webui目录下。

```
docker cp CompVis sdwebui:/home/ma-user/stable-diffusion-webui/
```

```
# 修改文件夹权限
```

```
docker exec -it --user root sdwebui bash
```

```
chown -R ma-user:ma-group stable-diffusion-webui/CompVis
```

Step3 安装依赖

1. 在容器中执行如下命令，安装pip依赖。

```
cd /home/ma-user/stable-diffusion-webui
pip install --upgrade pip
pip install -r requirements.txt --no-deps
pip install lightning_utilities torchmetrics gradio_client matplotlib
pydantic aiofiles starlette ffmpeg pydub uvicorn orjson semantic_version
altair antlr4-python3-runtime==4.8.0 ftfy regex pytorch_lightning==1.6.5
gitdb trampoline clip aenum facexlib torch==2.1.0 python-multipart gdown

pip install -r requirements_versions.txt
pip install httpx==0.24.1
pip install diffuser
```

2. 安装Stable Diffusion依赖。

- 下载stablediffusion-main.zip文件解压后，重命名为stable-diffusion-stability-ai，然后拷贝到容器stable-diffusion-webui/repositories/目录下。stablediffusion-main.zip文件的官网下载地址：<https://github.com/Stability-AI/stablediffusion>。

```
docker cp stable-diffusion-stability-ai sdwebui:/home/ma-user/stable-diffusion-webui/
repositories/
```

📖 说明

如果stable-diffusion-webui/repositories/目录不存在，需要通过mkdir创建。

- 下载generative-models-main.zip文件解压后，重命名为generative-models，然后拷贝到容器stable-diffusion-webui/repositories/目录下。generative-models-main.zip文件的官网下载地址：<https://github.com/Stability-AI/generative-models.git>。

- ```
docker cp generative-models sdwebui:/home/ma-user/stable-diffusion-webui/repositories/
```
- c. 下载k-diffusion-master.zip文件解压后，重命名为k-diffusion，然后拷贝到容器stable-diffusion-webui/repositories/目录下。k-diffusion-master.zip文件的官网下载地址：<https://github.com/Stability-AI/k-diffusion>。
- ```
docker cp k-diffusion sdwebui:/home/ma-user/stable-diffusion-webui/repositories/
# 修改文件夹权限
docker exec -it --user root sdwebui bash
chown -R ma-user:ma-group stable-diffusion-webui/repositories/
```
3. 安装vaeapprox-sdxl.pt。
- 下载vaeapprox-sdxl.pt文件后，拷贝到容器/home/ma-user/stable-diffusion-webui/models/VAE-approx/目录下。vaeapprox-sdxl.pt的官网下载地址：<https://github.com/AUTOMATIC1111/stable-diffusion-webui/releases/tag/v1.0.0-pre>。
- ```
docker cp vaeapprox-sdxl.pt sdwebui:/home/ma-user/stable-diffusion-webui/models/VAE-approx/
修改文件夹权限
docker exec -it --user root sdwebui bash
chown -R ma-user:ma-group stable-diffusion-webui/models/VAE-approx/
```

## Step4 运行并验证 SDXL 模型

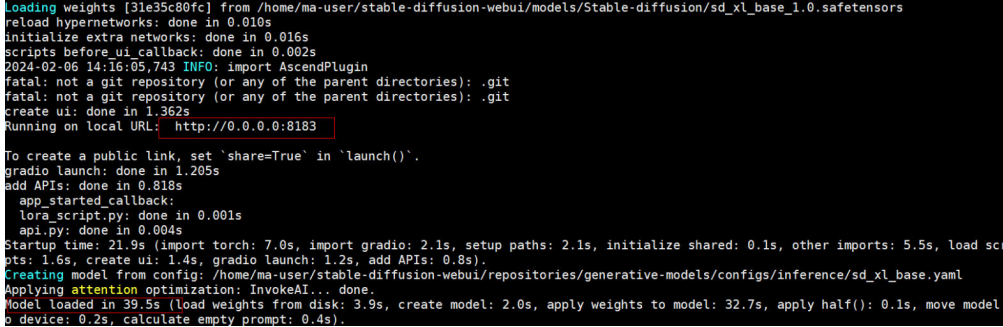
1. 首先在容器中运行命令。

```
cd /home/ma-user/stable-diffusion-webui
source /usr/local/Ascend/ascend-toolkit/set_env.sh
```
2. 在/home/ma-user目录下已经存在launch.py脚本文件，启动launch.py命令如下。

```
python3 launch.py --skip-torch-cuda-test --port 8183 --enable-insecure-extension-access --listen --log-startup --disable-safe-unpickle --skip-prepare-environment --api
```

启动成功后，打印如下信息。

图 4-16 启动成功

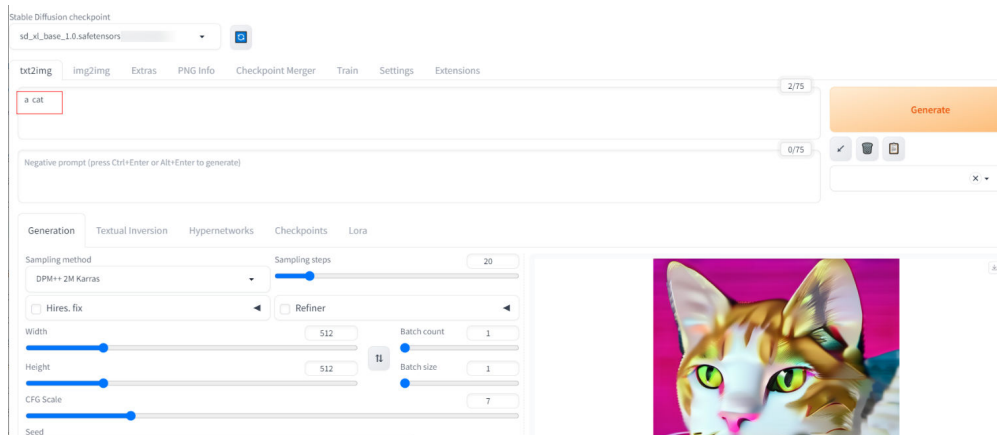


```
Loading weights [31e35c80fc] from /home/ma-user/stable-diffusion-webui/models/Stable-diffusion/sd_xl_base_1.0.safetensors
reread hypernetworks: done in 0.010s
initialize extra networks: done in 0.016s
scripts before ui callback: done in 0.002s
2024-02-06 14:16:05,743 INFO: import AscendPlugin
fatal: not a git repository (or any of the parent directories): .git
fatal: not a git repository (or any of the parent directories): .git
create ui: done in 1.362s
Running on local URL: http://0.0.0.0:8183

To create a public link, set `share=True` in `launch()`.
gradio launch: done in 1.205s
add APIs: done in 0.818s
 app_started_callback:
 lora_script.py: done in 0.001s
 api.py: done in 0.004s
Startup time: 21.9s (import torch: 7.0s, import gradio: 2.1s, setup paths: 2.1s, initialize shared: 0.1s, other imports: 5.5s, load sc
pts: 1.6s, create ui: 1.4s, gradio launch: 1.2s, add APIs: 0.8s).
Creating attention optimization: InvokeAI... done.
Model loaded in 39.5s (load weights from disk: 3.9s, create model: 2.0s, apply weights to model: 32.7s, apply half(): 0.1s, move model
o device: 0.2s, calculate empty prompt: 0.4s).
```

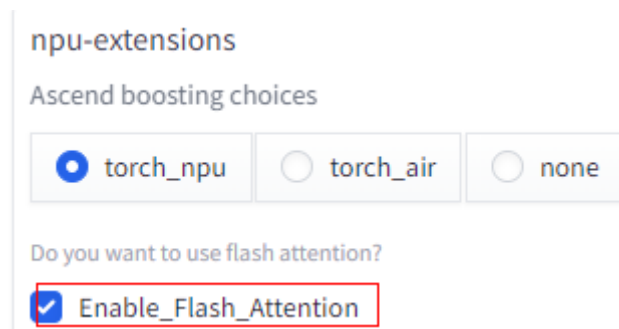
3. 使用http://{宿主机ip}:8183 可以访问前端页面，通过输入文字生成图片。

图 4-17 文生图



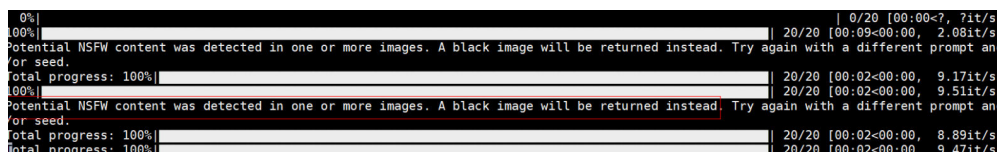
注意开启fa优化按钮。

图 4-18 开启 fa 优化按钮



如果使用涉黄文字，输出的图片会返回黑图，用于验证safety-checker功能。同时，服务端会打印如下信息。

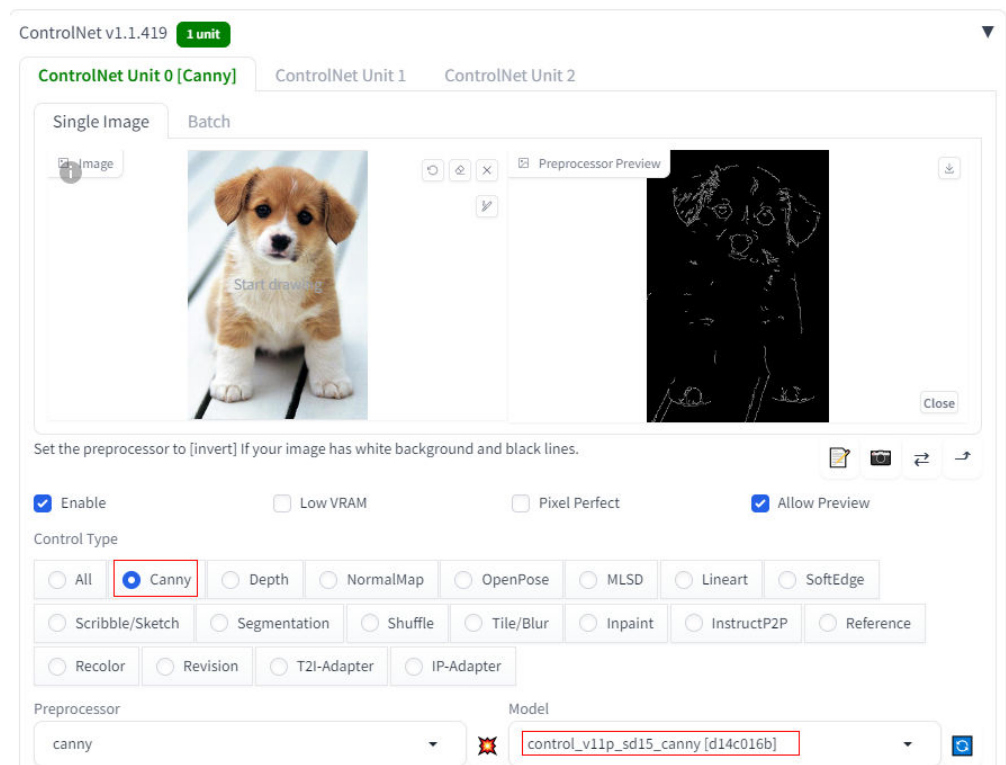
图 4-19 服务端返回信息



4. 带controlnet运行，默认使用canny。

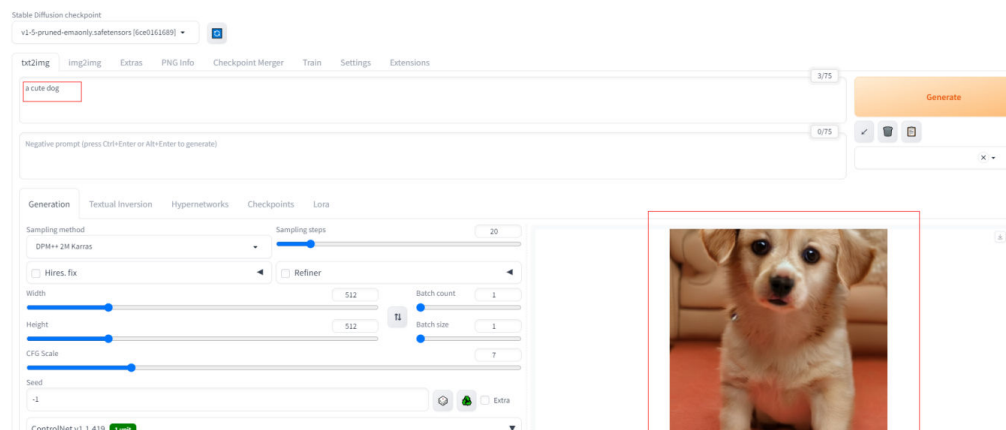


图 4-20 带 controlnet 运行



可以观察到输出的图片与canny输入图片很相近，坐姿和样子比较符合，如下图所示。

图 4-21 文生图



- 5. 使用后台API调用文生图接口。

```
curl -kv -X POST localhost:8183/sdapi/v1/txt2img -H "Content-Type: application/json" -d '{"prompt": "a dog"}'
```

客户端返回图像的base64编码，将base64编码再转换为图片，转换代码如下。

```
from PIL import Image
from io import BytesIO
import base64

def base64_to_image(base64_str):
 image = base64.b64decode(base64_str, altchars=None, validate=False)
 image = BytesIO(image)
```

```
image = Image.open(image)
image.save("./out_put_image.png")
```

## 4.4 AIGC 工具 tailor 使用指导

### tailor 简介

tailor是AIGC场景下用于模型转换（onnx到mindir）和性能分析的辅助工具，当前支持以下功能。

表 4-2 功能总览

| 功能大类      | 具体功能                                                                                                                            |
|-----------|---------------------------------------------------------------------------------------------------------------------------------|
| 模型转换      | <ul style="list-style-type: none"> <li>• 固定shape转模型</li> <li>• 动态shape传入指定档位转模型</li> <li>• 支持fp32</li> <li>• 支持AOE优化</li> </ul> |
| benchmark | <ul style="list-style-type: none"> <li>• 支持测试性能</li> <li>• 支持精度测试</li> </ul>                                                    |
| profiling | 支持分析算子的profiling                                                                                                                |

### 环境准备

本工具支持x86和ARM的系统环境，使用前需要安装以下软件。

表 4-3 安装软件及步骤

| 软件             | 安装步骤                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| mindspore-lite | 安装版本：2.2.10<br>下载地址： <a href="https://www.mindspore.cn/lite/docs/zh-CN/r2.2/use/downloads.html">https://www.mindspore.cn/lite/docs/zh-CN/r2.2/use/downloads.html</a><br>需要下载的安装包与机器规格有关，请根据需要选择合适的安装包。 <ul style="list-style-type: none"> <li>• 如果机器规格为Snt9B，则下载操作系统为Linux-aarch64的tag包：<a href="#">mindspore-lite-2.2.10-linux-aarch64.tar.gz</a>。</li> <li>• 如果机器规格为Snt3P，则下载操作系统为Linux-x86_64的tag包：<a href="#">mindspore-lite-2.2.10-linux-x64.tar.gz</a>。</li> </ul> |

| 软件     | 安装步骤                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|        | <p>安装方式如下：</p> <p>MindSpore Lite云侧推理包解压缩后，设置`LITE_HOME`环境变量为解压缩的路径，例如：</p> <pre>export LITE_HOME=\$some_path/mindspore-lite-2.2.10-linux-aarch64</pre> <p>设置环境变量LD_LIBRARY_PATH：</p> <pre>export LD_LIBRARY_PATH=\$LITE_HOME/runtime/lib:\$LITE_HOME/runtime/third_party/dnnl:\$LITE_HOME/tools/converter/lib:\$LD_LIBRARY_PATH</pre> <p>如果需要使用convert_lite或者benchmark工具，则需要设置环境变量PATH。</p> <pre>export PATH=\$LITE_HOME/tools/converter/converter:\$LITE_HOME/tools/benchmark:\$PATH</pre>                                                                                                                                                                                                                                               |
| cann   | <p>安装版本： CANN 7.0.0</p> <p>下载地址：<a href="https://support.huawei.com/enterprise/zh/ascend-computing/cann-pid-251168373/software/258923273?idAbsPath=fixnode01%7C23710424%7C251366513%7C22892968%7C251168373">https://support.huawei.com/enterprise/zh/ascend-computing/cann-pid-251168373/software/258923273?idAbsPath=fixnode01%7C23710424%7C251366513%7C22892968%7C251168373</a></p> <p>请下载toolkit和对应机器的kernels包，以Snt9B为例则下载“Ascend-cann-toolkit_7.0.0_linux-aarch64.run”和“Ascend-cann-kernels-型号_7.0.0_linux.run”。</p> <p>安装命令（以Snt9B的cann安装为例）：</p> <pre>./Ascend-cann-toolkit_7.0.0_linux-aarch64.run --full ./Ascend-cann-kernels-型号_7.0.0_linux.run --install</pre> <p>请安装在默认路径下： /usr/local/Ascend，暂不支持安装在自定义路径下。</p>              |
| tailor | <p>安装版本： 0.3.2</p> <p>下载地址：</p> <p><a href="https://cneast3-modelarts-sdk.obs.cn-east-3.myhuaweicloud.com/tailor-0.3.2-py3-none-any.whl/1705023096792/tailor-0.3.2-py3-none-any.whl">https://cneast3-modelarts-sdk.obs.cn-east-3.myhuaweicloud.com/tailor-0.3.2-py3-none-any.whl/1705023096792/tailor-0.3.2-py3-none-any.whl</a></p> <p>SHA-256：</p> <p><a href="https://cneast3-modelarts-sdk.obs.cn-east-3.myhuaweicloud.com/tailor-0.3.2-py3-none-any.whl/1705023096792/tailor-0.3.2-py3-none-any.whl.sha256">https://cneast3-modelarts-sdk.obs.cn-east-3.myhuaweicloud.com/tailor-0.3.2-py3-none-any.whl/1705023096792/tailor-0.3.2-py3-none-any.whl.sha256</a></p> <p>安装命令：</p> <pre>pip install tailor-0.3.2-py3-none-any.whl</pre> |

## 使用指导

tailor支持“命令行”和“Python API”两种方式使用。

- **命令行方式**

命令行运行样例：

```
tailor --model_path="./resnet50-v2-7.onnx"--config_path="./config.ini"--input_shape="data:1,3,224,224"--output_path="/home/"--accuracy="fp32"--aoe=True
```

config.ini参考内容如下：

```
[ascend_context]
input_shape=data:[-1,3,224,224]
dynamic_dims=[1],[2],[3]
```

表 4-4 参数说明

| 参数名称          | 功能描述           | 参数类型   | 是否必填 | 默认值       | 备注                                                                   |
|---------------|----------------|--------|------|-----------|----------------------------------------------------------------------|
| --model_path  | 指定onnx模型路径。    | string | 是    | -         | -                                                                    |
| --config_path | 指定模型配置文件路径。    | string | 否    | -         | tailor支持动态分档转换功能，需要指定配置文件路径，需要注意即便有配置文件，只要是动态模型就需要指定--input_shape参数。 |
| --input_shape | 指定模型转换的shape。  | string | 否    | -         | 固定shape模型转换可以不填，动态模型转换必填。                                            |
| --output_path | 指定结果输出路径。      | string | 否    | 默认为当前目录下。 | -                                                                    |
| --aoe         | 是否在转换时进行AOE优化。 | bool   | 否    | False     | AOE优化可以提升模型性能，但不是一定有提升，需要注意开启AOE，会导致模型转换耗时极大延长。                      |

| 参数名称       | 功能描述                 | 参数类型   | 是否必填 | 默认值  | 备注 |
|------------|----------------------|--------|------|------|----|
| --accuracy | 指定模型精度，只支持fp16和fp32。 | string | 否    | fp16 | -  |

● Python API

- 导入包并创建tailor对象。  

```
from tailor.tailor import Tailor
onnx_model_path = "./resnet50-v2-7.onnx" # 相对路径或者绝对路径均可以
t = Tailor(onnx_model_path)
```
- 查询onnx模型的输入信息。  

```
查询onnx模型的输入信息
t.get_model_input_info()
```

图 4-22 查询 onnx 模型的输入输出信息

```
In [3]: t.get_model_input_info()
Out[3]:
[{'name': 'data',
 'type': 'tensor(float)',
 'shape': ['N', 3, 224, 224],
 'np_type': numpy.float32}]
```

- 查询onnx模型的输出信息。  

```
查询模型的输出信息
t.get_model_output_info()
```

图 4-23 查询 onnx 模型的输出信息

```
In [4]: t.get_model_output_info()
Out[4]:
[{'name': 'resnetv24_dense0_fwd',
 'type': 'tensor(float)',
 'shape': ['N', 1000]}]
```

- 固定shape模型，可以直接运行。  

```
t.run()
```
- 指定档位信息运行。  

```
input_shape="data:1,3,224,224"
t.run(input_shape=input_shape)
```
- 动态档位执行config\_path运行。需要注意，只要是动态模型，就必须传入input\_shape，因为转换模型后的benchmark和profiling都依赖单个shape操作。  

```
input_shape="data:1,3,224,224"
config_path = "./resnet/config.ini"
t.run(input_shape=input_shape, config_path=config_path)
```
- 指定精度为fp32。  

```
input_shape="data:1,3,224,224"
t.run(input_shape=input_shape, accuracy='fp32')
```

- 开启AOE优化。  
input\_shape="data:1,3,224,224"  
t.run(input\_shape=input\_shape, aoe=True)
- 指定输出位置。  
input\_shape="data:1,3,224,224"  
# 不指定输出路径，则默认在当前执行目录存储结果  
t.run(input\_shape=input\_shape, output\_path="/home/xxx")

运行结果将存储在output文件夹中，如果用户指定了output\_path，会指定位置保存，如果不指定则在当前代码执行目录生成文件夹保存输出。整体运行的结果都存放在output文件夹中，每转一次模型就会根据模型名称以及相关参数生成结果文件，如下图所示。

图 4-24 output 文件

```
ll output/
}
-- 6 root 4096 Nov 6 15:21 resnet50-v2-7_fp16_20231106152024/
-- 6 root 4096 Nov 15 10:06 resnet50-v2-7_fp16_20231115100511/
-- 6 root 4096 Nov 6 23:57 resnet50-v2-7_fp16_aoe_20231106194012/
-- 6 root 4096 Nov 6 15:33 unet_fp16_20231106152314/
-- 6 root 4096 Nov 10 22:36 unet_fp16_aoe_20231107061337/
-- 6 root 4096 Nov 6 15:23 yolox_m_mmyolo_fp16_20231106152141/
-- 6 root 4096 Nov 7 06:13 yolox_m_mmyolo_fp16_aoe_20231106235726/
```

在每次运行的结果文件中，分为三部分：convert、benchmark、profiling，相关的文件及存储内容如下。

表 4-5 输出文件介绍（以模型名称为 resnet50-v2-7.onnx 为例）

| 类别                | 文件名称                              | 是否一定生成 | 文件存储内容                     |
|-------------------|-----------------------------------|--------|----------------------------|
| conv<br>ert       | resnet50-v2-7.mindir              | 是      | 转换后的mindir模型。              |
|                   | resnet50-v2-7.om                  | 否      | 转换过程中的om文件，不是必定生成。         |
|                   | onnx_to_minds<br>pore.sh          | 是      | 模型转换命令，可以本地直接运行。           |
|                   | resnet50-<br>v2-7_convert.lo<br>g | 是      | 模型转换过程的日志。                 |
|                   | config.ini                        | 否      | 配置文件，在指定fp32精度或者AOE打开时会生成。 |
|                   | onnx_to_minds<br>pore_aoe.sh      | 否      | 在打开AOE功能时会生成。              |
| benc<br>hma<br>rk | run_benchmark<br>.sh              | 是      | 运行benchmark的脚本，可本地直接运行。    |

| 类别            | 文件名称                      | 是否一定生成 | 文件存储内容                    |
|---------------|---------------------------|--------|---------------------------|
|               | run_benchmark_accuracy.sh | 是      | benchmark运行精度的脚本，可本地直接运行。 |
|               | performance.txt           | 是      | benchmark性能测试结果。          |
|               | accuracy.txt              | 是      | 精度测试结果。                   |
|               | *.bin                     | 是      | 自动构造的输入随机bin文件，可能存在多个。    |
|               | resnet50-v2-7_output.txt  | 是      | 上述bin文件作为输入时onnx模型运行的结果。  |
| profil<br>ing | run_profiling.sh          | 是      | 运行profiling的脚本，可本地直接运行。   |
|               | profiling.config          | 是      | 运行profiling的配置文件。         |
|               | profiling.json            | 是      | 运行profiling的配置文件。         |
|               | PROF_xxx开头的文件夹            | 是      | 运行profiling的结果文件夹。        |
|               | run_aggregate.sh          | 是      | 运行数据聚合的脚本，可直接本地运行。        |
|               | run_profiling.log         | 是      | 存储运行profiling的日志信息。       |

# 5 数字人

## 5.1 数字人 Wav2Lip 适配 PyTorch NPU 指导

本文档主要介绍如何在ModelArts Lite的DevServer环境中，使用NPU卡训练Wav2Lip模型。本文档中提供的Wav2Lip模型，是在原生Wav2Lip代码基础上适配后的模型，可以用于NPU芯片训练。

**Wav2Lip**是一种基于对抗生成网络的由语音驱动的人脸说话视频生成模型。主要应用于数字人场景。不仅可以基于静态图像来输出与目标语音匹配的唇形同步视频，还可以直接将动态的视频进行唇形转换，输出与输入语音匹配的视频，俗称“对口型”。该技术的主要作用就是在将音频与图片、音频与视频进行合成时，口型能够自然。

Wav2Lip模型的输入为任意的一段视频和一段语音，输出为一段唇音同步的视频。

Wav2Lip的网络模型总体上分成三块：生成器、判别器和一个预训练好的唇音同步判别模型Pre-trained Lip-sync Expert。

- 生成器是基于encoder-decoder的网络结构，分别利用2个encoder（speech encoder和identity encoder）去对输入的语音和视频人脸进行编码，并将二者的编码结果进行拼接，送入到face decoder中进行解码得到输出的视频帧。
- 判别器Visual Quality Discriminator对生成结果的质量进行规范，提高生成视频的清晰度。
- 引入预训练的唇音同步判别模型Pre-trained Lip-sync Expert，作为衡量生成结果的唇音同步性的额外损失，可以更好的保证生成结果的唇音同步性。

### 方案概览

本方案介绍了在ModelArts的DevServer上使用昇腾计算资源开展Wav2Lip训练推理的详细过程。完成本方案的部署，需要先联系您所在企业的华为方技术支持购买DevServer资源。

本方案目前仅适用于企业客户。

### 环境配置要求

准备一台ModelArts的DevServer物理机环境，推荐使用“西南-贵阳一”Region上的DevServer资源和Ascend Snt9B单机单卡。



表 5-1 环境要求

| 模型      | 版本    |
|---------|-------|
| CANN    | 7.0.1 |
| PyTorch | 3.1.0 |

## 获取软件

获取Wav2Lip Ascend适配代码`asscendcloud-aigc-6.3.902-*.tar.gz`文件。获取路径：[Support网站](#)。

### 📖 说明

如果没有软件下载权限，请联系您所在企业的华为方技术支持下载获取。  
`asscendcloud-aigc-6.3.902-*.tar.gz`文件名中的\*表示具体的时间戳，以包名的实际时间为准。

## Step1 准备环境

1. 请参考[DevServer资源开通](#)，购买DevServer资源，并确保机器已开通，密码已获取，能通过SSH登录，不同机器之间网络互通。

### 📖 说明

购买DevServer资源时如果无可选资源规格，需要联系华为云技术支持申请开通。

当容器需要提供服务给多个用户，或者多个用户共享使用该容器时，应限制容器访问Openstack的管理地址（169.254.169.254），以防止容器获取宿主机的元数据。具体操作请参见[禁止容器获取宿主机元数据](#)。

2. 检查环境。
  - a. SSH登录机器后，检查NPU设备检查。运行如下命令，返回NPU设备信息。

```
npu-smi info
```

如出现错误，可能是机器上的NPU设备没有正常安装，或者NPU镜像被其他容器挂载。请先正常[安装NPU设备和驱动](#)，或释放被挂载的NPU。
  - b. 检查docker是否安装。

```
docker -v #检查docker是否安装
```

如尚未安装，运行以下命令安装docker。

```
yum install -y docker-engine.aarch64 docker-engine-selinux.noarch docker-runc.aarch64
```
  - c. 配置IP转发，用于容器内的网络访问。执行以下命令查看`net.ipv4.ip_forward`配置项的值，如果为1，可跳过此步骤。

```
sysctl -p | grep net.ipv4.ip_forward
```

如果`net.ipv4.ip_forward`配置项的值不为1，执行以下命令配置IP转发。

```
sed -i 's/net.ipv4.ip_forward=0/net.ipv4.ip_forward=1/g' /etc/sysctl.conf
sysctl -p | grep net.ipv4.ip_forward
```
3. 获取基础镜像。建议使用官方提供的镜像部署推理服务。  
镜像地址`{image_url}`为：  
西南-贵阳一：`swr.cn-southwest-2.myhuaweicloud.com/atelier/pytorch_2_1_ascend:pytorch_2.1.0-cann_7.0.0-py_3.9-hce_2.0.2312-aarch64-snt9b-20240312154948-219655b`

```
docker pull ${image_url}
```

4. 启动容器镜像。启动前请先按照参数说明修改\${}中的参数。可以根据实际需要增加修改参数。

```
export work_dir="自定义挂载的工作目录"
export container_work_dir="自定义挂载到容器内的工作目录"
export container_name="自定义容器名称"
export image_name="swr.cn-southwest-2.myhuaweicloud.com/atelier/
pytorch_2_1_ascend:pytorch_2.1.0-cann_7.0.0-py_3.9-hce_2.0.2312-aarch64-
snt9b-20240312154948-219655b"
// 启动一个容器去运行镜像
docker run -itd \
 --device=/dev/davinci0 \
 --device=/dev/davinci_manager \
 --device=/dev/devmm_svm \
 --device=/dev/hisi_hdc \
 -v /usr/local/bin/npu-smi:/usr/local/bin/npu-smi \
 -v /usr/local/dcmi:/usr/local/dcmi \
 -v /etc/ascend_install.info:/etc/ascend_install.info \
 -v /sys/fs/cgroup:/sys/fs/cgroup:ro \
 -v /usr/local/Ascend/driver:/usr/local/Ascend/driver \
 --shm-size 32g \
 --net=bridge \
 -v ${work_dir}:${container_work_dir} \
 --name ${container_name} \
 ${image_name} bash
```

#### 参数说明：

- --name \${container\_name} 容器名称，进入容器时会用到，此处可以自己定义一个容器名称。
  - -v \${work\_dir}:\${container\_work\_dir} 代表需要在容器中挂载宿主机的目录。宿主机和容器使用不同的文件系统。work\_dir为宿主机中工作目录，目录下存放着训练所需代码、数据等文件。container\_work\_dir为要挂载到的容器中的目录。为方便两个地址可以相同。
  - \${image\_name} 代表 \${image\_name}。
5. 通过容器名称进入容器中。  
docker exec -it \${container\_name} bash

## Step2 安装依赖和软件包

1. Python版本要求3.10，如果不满足的话，建议更新容器的conda环境的Python版本。

```
输入如下命令，待conda界面准备完成后输入y，等待自动下载安装
conda create --name py310 python=3.10
```

#### 参数说明：

- --name: 该参数为新环境名字，可以自定义一个，此处以py310举例。
- python=新环境Python版本

```
完成后输入如下命令激活新环境
conda activate py310
```

激活新conda环境后控制台显示（py310）即为切换成功，如下图所示。

图 5-1 激活新 conda 环境

```
#
To activate this environment, use
#
$ conda activate py310
#
To deactivate an active environment, use
#
$ conda deactivate

(PyTorch-2.1.0) [ma-user@76f680033741 Wav2Lip]$ conda activate py310
(py310) [ma-user@76f680033741 Wav2Lip]$ pip install -r requirements.txt
```

2. 从github拉取Wav2Lip代码。

```
cd /home/ma-user
git clone https://github.com/Rudrabha/Wav2Lip.git
```

如果出现报错SSL certificate problem: self signed certificate in certificate chain

图 5-2 报错 SSL certificate problem

```
fatal: unable to access 'https://github.com/Rudrabha/Wav2Lip.git/': SSL certificate problem: self signed certificate in certificate chain
```

可采取忽略SSL证书验证：使用以下命令来克隆仓库，它将忽略SSL证书验证。

```
git clone -c http.sslVerify=false https://github.com/Rudrabha/Wav2Lip.git
```

3. 安装Wav2Lip Ascend软件包。
  - a. 将获取到的Wav2Lip Ascend软件包ascendcloud-aigc-\*.tar.gz文件上传到容器的/home/ma-user/Wav2Lip目录下。获取路径：[Support网站](#)。
  - b. 解压ascendcloud-aigc-\*.tar.gz文件，解压后将里面文件与对应Wave2Lip文件进行替换。

```
cd /home/ma-user/Wav2Lip
tar -zxvf ascendcloud-aigc-6.3.902-*.tar.gz
tar -zxvf ascendcloud-aigc-poc-Wav2Lip_Ascend.tar.gz
mv Wav2Lip_code/* ./
rm -rf ascendcloud-aigc-* Wav2Lip_code/
```

**说明**

ascendcloud-aigc-6.3.902-\*.tar.gz后面的\*表示时间戳，请按照实际替换。

要替换的文件目录结构如下所示：

```
|---Wav2Lip_code/
--- color_syncnet_train.py #训练expert discriminator唇形同步鉴别器
--- inference.py #推理代码，可以与任意音频或视频进行口型同步
--- preprocess.py #对初始视频数据进行推理
--- read.txt #关于包版本兼容问题的一些处理方案
--- requirements.txt #建议的依赖包版本
--- wav2lip_train.py #训练 Wav2Lip 模型
```

4. 安装Python依赖包，文件为requirements.txt文件。

```
pip install -r requirements.txt
```

由于librosa、numba、llvmlite包的版本兼容问题，会出现报错ModuleNotFoundError: No module named 'numba.decorators'。

此时进入Python包librosa安装位置，打开文件site-packages/librosa/util/decorators.py，修改文件如下：

```
import warnings
from decorator import decorator import six
#注释此行
#from numba.decorators import jit as optional_jit
```

```
#修改此行如下
#_all_ = ['moved', 'deprecated', 'optional_jit']
all = ['moved', 'deprecated']
```

## Step3 训练 Wav2Lip 模型

1. 准备预训练模型。下载需要使用的预训练模型。
  - 人脸检测预训练模型，[下载链接](#)。
  - 专家唇形同步鉴别器，[下载链接](#)，此链接是官方提供的预训练模型。训练 Wav2Lip模型时需要使用专家唇形同步鉴别器，用户可以用自己的数据训练，也可以直接使用官方提供的预训练模型。
2. 处理初始视频数据集。
  - a. 将下载好的人脸检测预训练模型上传到/home/ma-user/Wav2Lip/face\_detection/detection/sfd/s3fd.pth目录。
  - b. 下载LRS2数据集。数据集文件夹结构如下：

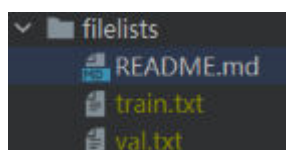
```
├── LRS2_partly
│ └── main
│ ├── five-digit numbered video IDs ending with (.mp4)
│ ├── 00001.mp4
│ └── 00002.mp4
```
  - c. 对数据集进行预处理。具体命令如下。

```
python preprocess.py --data_root ./LRS2_partly --preprocessed_root lrs2_preprocessed/
```

data\_root参数为原始视频根目录，preprocessed\_root参数为处理后生成的数据集目录。  
处理后数据目录如下所示。

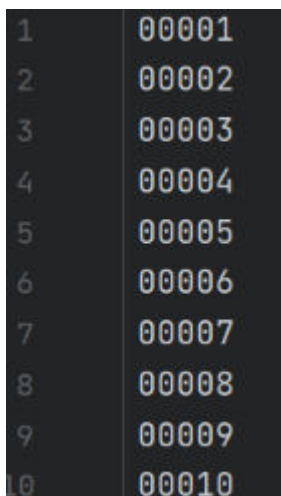
```
preprocessed_root (lrs2_preprocessed)
├── main
│ ├── Folders with five-digit numbered video IDs (00001)
│ ├── *.jpg
│ ├── audio.wav
│ └── 00001
│ ├── *.jpg
│ └── audio.wav
```
  - d. 将LRS2文件列表中的.txt文件（train、val）放入该filelists文件夹中。

图 5-3 filelists 文件夹



train.txt和val.txt内容参考如下，为处理后视频数据的目录名字。

图 5-4 train.txt 和 val.txt 内容



```
1 00001
2 00002
3 00003
4 00004
5 00005
6 00006
7 00007
8 00008
9 00009
10 00010
```

### 3. 训练专家唇形同步鉴别器。

如果使用LRS2数据集，可选择跳过此步骤。如果使用自己的数据集，训练命令参考如下。

```
python color_syncnet_train.py --data_root ./lrs2_preprocessed/main/ --checkpoint_dir ./savedmodel/syncnet_model/ --checkpoint_path ./checkpoints/lipsync_expert.pth
```

参数说明：

- --data\_root：处理后的视频数据目录，与train.txt内容拼接后得到单个数据目录，例如：lrs2\_preprocessed/main/00001。
- --checkpoint\_dir：此目录用于保存模型。
- --checkpoint\_path：（可选）可基于此目录的lipsync\_expert模型继续进行训练，如果重新训练则不需要此参数。

默认每10000 step保存一次模型。

### 4. 训练Wav2Lip模型。

训练Wav2Lip模型时需要使用专家唇形同步鉴别器。可以使用上一步3中的训练结果，也可以直接下载官方提供的[预训练权重](#)来使用。

具体训练命令如下。

```
python wav2lip_train.py --data_root ./lrs2_preprocessed/main/ --checkpoint_dir ./savedmodel --syncnet_checkpoint_path ./checkpoints/lipsync_expert.pth --checkpoint_path ./checkpoints/wav2lip.pth
```

参数说明：

- --data\_root：处理后的视频数据目录，与train.txt内容拼接后得到单个数据目录，例如：lrs2\_preprocessed/main/00001。
- --checkpoint\_dir：此目录用于保存模型。
- --syncnet\_checkpoint\_path：专家鉴别器的目录。
- --checkpoint\_path：（可选）可基于此目录的Wav2Lip模型继续进行训练，如果重新训练则不需要此参数。

默认每3000 step保存一次模型。

专家鉴别器的评估损失应降至约 0.25，Wav2Lip评估同步损失应降至约 0.2，以获得良好的结果。

## 常见问题

如果训练时遇到报错ImportError: /usr/lib64/libc.so.6: version `GLIBC\_2.34' not found，是由于编译Python的glibc环境版本过旧导致，建议重新安装python。

重新安装python命令如下。

```
输入如下命令，待conda界面准备完成后输入y，等待自动下载安装
conda create --name py310 python=3.10
```

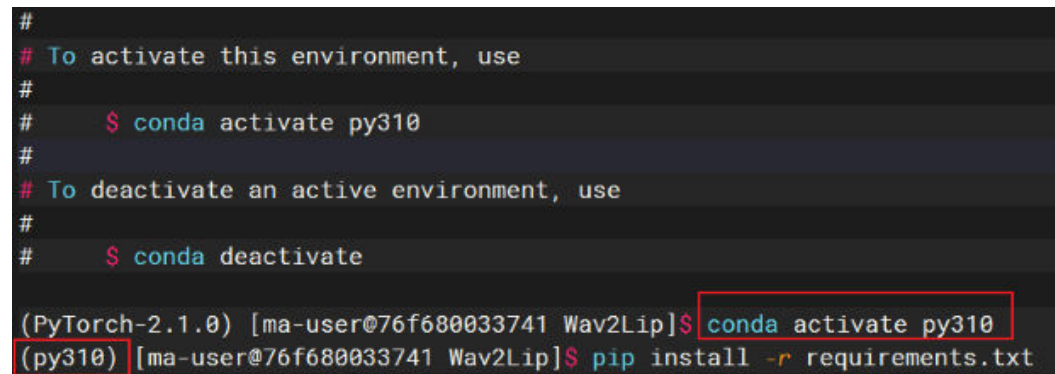
参数说明：

- --name: 该参数为新环境名字，可以自定义一个，此处以py310举例。
- python=新环境Python版本

```
完成后输入如下命令激活新环境
conda activate py310
```

激活新conda环境后控制台显示（py310）即为切换成功，如下图所示。

图 5-5 激活新 conda 环境



```

To activate this environment, use

$ conda activate py310

To deactivate an active environment, use

$ conda deactivate

(PyTorch-2.1.0) [ma-user@76f680033741 Wav2Lip]$ conda activate py310
(py310) [ma-user@76f680033741 Wav2Lip]$ pip install -r requirements.txt
```

# 6 业务迁移

## 6.1 LLM 训练业务昇腾迁移指导

### 6.1.1 场景介绍

本文以ChatGLM-6B为例，介绍如何将模型迁移至昇腾设备上训练、模型精度对齐以及性能调优。

主要包含以下步骤：

- [环境准备](#)
- [迁移适配](#)
- [精度对齐](#)
- [性能调优](#)

### 6.1.2 环境准备

**步骤1** 开通裸金属服务器资源（请见[DevServer资源开通](#)），并在裸金属服务器上搭建迁移环境请见[裸金属服务器环境配置指导](#)。

**步骤2** 启动华为云预置镜像环境，本案例使用的贵阳一的镜像环境。

```
#shell
docker run --privileged --name chatglm-test --cap-add=SYS_PTRACE -e ASCEND_VISIBLE_DEVICES=0-7 -u=0
swr.cn-southwest-2.myhuaweicloud.com/atelier/pytorch_1_11_ascend:pytorch_1.11.0-cann_7.0.1-py_3.9-
euler_2.10.7-aarch64-snt9b-20231107190844-50a1a83 bash
```

此处“-e ASCEND\_VISIBLE\_DEVICES”用于指定容器中启动的NPU device，0-7表示从0-7号卡，请按照实际NPU卡情况修改。

**步骤3** 安装相关依赖库。

ChatGLM-6B是完全基于Python开发的模型，训练之前需要事先安装与之依赖的Python库。其中部分依赖库可以使用pip工具安装，执行如下脚本：

```
#shell
pip install rouge_chinese nltk jieba sentencepiece datasets==2.12.0 fsspec==2022.11.0 transformers==4.29.2
deepspeed==0.9.2
```

与昇腾NPU适配的依赖库有torch\_npu，多卡训练也需要deepspeed\_npu，本文适配的版本如下：deepspeed\_npu(0.1)，torch\_npu(1.11)。其中torch\_npu在镜像环境中已经预置安装，deepspeed\_npu安装配置详见[deepspeed\\_npu](#)。

此外，transformers执行需要高版本的scikit-learn、accelerate，详见[常见问题5](#)、[常见问题6](#)。此处执行升级命令：

```
#shell
pip install scikit-learn accelerate --upgrade
```

transformers库的training\_args.py有部分操作是适配的cuda设备，详见[常见问题7](#)，本文使用昇腾ModelZoo的适配版本脚本替换（[下载链接](#)）。

**步骤4** 下载ChatGLM-6B源代码、模型权重与数据集到容器环境。

- 源代码：[chatglm-6B](#)
- 模型权重：[weights](#)
- 数据集：[Firefly\(流萤\)](#)、[ADGEN \(广告生成\)](#)

#### 📖 说明

- 源代码、模型权重使用的清华官方在Github和Hugging Face开源的版本，源代码适配的main分支，权重当前使用1d240ba固定分支。其他分支版本理论上也可以进行迁移工作，不过注意可能由于权重不同原因最后训练结果也不太一致，此处建议您使用固定分支进行迁移。
- 数据集Firefly为本文用于多卡训练使用的数据集，数据集ADGEN为ChatGLM-6B ptuning训练适配的数据集，如果您运行环境为单卡环境下载数据集ADGEN。

----结束

## 6.1.3 迁移适配

本文以PyTorch框架在NPU上完成自动迁移为例，对适配过程需要修改的部分进行说明。并且针对单卡环境以及单机多卡deepspeed环境提供训练脚本。无特别说明，以ChatGLM-6B源代码根目录作为当前目录。

### 自动迁移适配

修改“ptuning/main.py”，添加deepspeed\_npu、torch\_npu、transfer\_to\_npu依赖库，如下图所示。

```
导入deepspeed_npu和torch_npu
import deepspeed_npu
import torch_npu
导入一键迁移接口
from torch_npu.contrib import transfer_to_npu
```



图 6-1 自动迁移适配

```
16 """
17 Fine-tuning the library models for sequence to sequence.
18 """
19 # You can also adapt this script on your own sequence to sequence task. Pointers for this are left a
 s comments.
20
21 import logging
22 import os
23 import sys
24 import json
25
26 import numpy as np
27 from datasets import load_dataset
28 import jieba
29 from rouge_chinese import Rouge
30 from nltk.translate.bleu_score import sentence_bleu, SmoothingFunction
31 import torch
32
33 # 导入 torch_npu和deepspeed_npu包
34 import deepspeed_npu
35 import torch_npu
36 # 导入一键迁移接口
37 from torch_npu.contrib import transfer_to_npu
38 import transformers
39 from transformers import (
40 AutoConfig,
41 AutoModel,
42 AutoTokenizer,
43 DataCollatorForSeq2Seq,
44 HfArgumentParser,
45 Seq2SeqTrainingArguments,
46 set_seed,
47)
48 from trainer_seq2seq import Seq2SeqTrainer
```

## 单卡方式训练

单卡执行脚本如下：

```
ptuning/run_npu_1d.sh
export ASCEND_RT_VISIBLE_DEVICES=0 # 指定 0 号卡对当前进程可见
PRE_SEQ_LEN=128
LR=2e-2

python3 ptuning/main.py \
 --do_train \
 --train_file ${HOME}/AdvertiseGen/train.json \
 --validation_file ${HOME}/AdvertiseGen/dev.json \
 --prompt_column content \
 --response_column summary \
 --overwrite_cache \
 --model_name_or_path ${HOME}/chatglm \
 --output_dir output/adgen-chatglm-6b-pt-PRE_SEQ_LEN-LR \
 --overwrite_output_dir \
 --max_source_length 64 \
 --max_target_length 64 \
 --per_device_train_batch_size 4 \
 --per_device_eval_batch_size 1 \
 --gradient_accumulation_steps 1 \
 --predict_with_generate \
 --max_steps 3000 \
 --logging_steps 10 \
 --save_steps 1000 \
 --learning_rate $LR \
 --pre_seq_len $PRE_SEQ_LEN \
 --local_rank -1
```

通过设定ASCEND\_RT\_VISIBLE\_DEVICES环境变量为0，控制0号卡对当前进程可见，PRE\_SEQ\_LEN和LR分别是soft prompt长度和训练的学习率，可以进行调节以取得最佳的效果。此外，这里去掉了int 4量化默认为FP16精度。\${HOME} 目录需要根据读者实际数据集及模型路径匹配，适配的数据集是ADGEN数据集，如果需要读者也可以使用自定义的数据集训练，具体请参考[使用自己数据集](#)。另外通过指定local\_rank为-1为

单卡模式，多卡模式下无需指定，会默认启动DistributedDataParallel(DDP) 多卡并行模式，具体详情见[常见问题1](#)。GPU环境单卡执行同样需要指定local\_rank为 -1。

## 多卡分布式执行

PyTorch框架下常见的多卡分布式执行主要包括DataParallel ( DP ) 和Distributed Data Parallel ( DDP )。torch\_npu环境下针对DDP场景的多卡训练有提供支持，具体请参见[迁移单卡脚本为多卡脚本](#)。此外，针对deepspeed环境，昇腾有专门的适配环境deepspeed-npu。在此提供一种基于deepspeed的多卡训练脚本，内容如下：

```
ds_run_npu.sh
LR=1e-4
TRAIN_FILE=${HOME}/YeungNLPfirefly-train-1.1M/firefly-train-1.1M.jsonl
PER_DEVICE_TRAIN_BATCH_SIZE=4
GRADIENT_ACCUMULATION_STEPS=32
MODEL_DIR=${HOME}/chatglm
OUTPUT_DIR=${HOME}/ChatGLM-6B-main/ptuning/output
DS_CONFIG=${HOME}/ChatGLM-6B-main/ptuning/ds_config.json
APP_SCRIPT=${HOME}/ChatGLM-6B-main/ptuning/main.py
MASTER_PORT=$(shuf -n 1 -i 10000-65535)

deepspeed --num_gpus=8 --master_port $MASTER_PORT ${APP_SCRIPT} \
 --deepspeed ${DS_CONFIG} \
 --log_level debug \
 --model_name_or_path ${MODEL_DIR} \
 --train_file ${TRAIN_FILE} \
 --prompt_column input \
 --response_column target \
 --max_source_length 512 \
 --max_target_length 512 \
 --output_dir ${OUTPUT_DIR}/chatglm-6b-${LR} \
 --per_device_train_batch_size ${PER_DEVICE_TRAIN_BATCH_SIZE} \
 --per_device_eval_batch_size 1 \
 --gradient_accumulation_steps ${GRADIENT_ACCUMULATION_STEPS} \
 --gradient_checkpointing False \
 --num_train_epochs 1 \
 --predict_with_generate \
 --logging_steps 10 \
 --save_strategy "steps" \
 --save_total_limit 3 \
 --learning_rate $LR \
 --dataloader_num_workers 60 \
 --preprocessing_num_workers 60 \
 --do_train \
 --overwrite_output_dir \
 --max_steps 100 \
 --fp16
```

LR、PER\_DEVICE\_TRAIN\_BATCH\_SIZE、GRADIENT\_ACCUMULATION\_STEPS分别代表学习率、单个设备训练批次大小、梯度累计步数，作为超参数可以调优获得较好模型。同样，\${HOME} 需要根据数据集模型等路径做对应替换，这里脚本适配的数据集是Firefly，其中deepspeed使用了[zero 1](#)显存优化方式，配置方式如下：

```
{
 "fp16": {
 "enabled": "auto",
 "loss_scale": 0,
 "loss_scale_window": 1000,
 "initial_scale_power": 16,
 "hysteresis": 2,
 "min_loss_scale": 1
 },
 "bf16": {
 "enabled": "auto"
 },
 "optimizer": {
```

```
"type": "AdamW",
"params": {
 "lr": "auto",
 "betas": "auto",
 "eps": "auto",
 "weight_decay": "auto"
},
"scheduler": {
 "type": "WarmupLR",
 "params": {
 "warmup_min_lr": "auto",
 "warmup_max_lr": "auto",
 "warmup_num_steps": "auto"
 }
},
"zero_optimization": {
 "stage": 1,
 "offload_optimizer": {
 "device": "cpu",
 "pin_memory": true
 },
 "contiguous_gradients": true,
 "overlap_comm": true,
 "allgather_partitions": true,
 "reduce_scatter": true,
 "allgather_bucket_size": 2e8,
 "reduce_bucket_size": 4e8
},
"flops_profiler": {
 "enabled": true,
 "profile_step": 1,
 "module_path": -1,
 "top_modules": 1,
 "detailed": false,
 "output_file": null
},
"zero_allow_untested_optimizer": "true",
"gradient_clipping": "auto",
"gradient_accumulation_steps": "auto",
"train_batch_size": "auto",
"train_micro_batch_size_per_gpu": "auto",
"wall_clock_breakdown": false
}
```

## 6.1.4 精度对齐

精度问题是指模型从GPU设备迁移到昇腾NPU设备之后由于软硬件差异引入的精度问题。根据是否在单卡环境下，可分为单卡精度问题与多卡精度问题。多卡相对于单卡，会有卡与卡之间的通信，这可能也是精度偏差的一种来源。所以多卡的精度对齐问题相对于单卡会更复杂。不过针对多卡的精度问题，可以分步骤先保证单卡对齐精度，然后分析通信过程的偏差。本文针对单卡的情形给出基于ptdbg-ascend精度对比工具的精度排查过程。

### loss 曲线对比

训练结束后，在output\_dir参数指定目录下会输出trainer\_state.json文件，该文件保存了训练过程loss以及learning\_rate的log信息。

将GPU设备训练输出的trainer\_state.json文件重命名为trainer\_state\_gpu.json，并复制到NPU节点的容器内，将NPU设备训练输出的trainer\_state.json文件重命名为trainer\_state\_npu.json。

对其进行解析就可以获取loss信息，这里可以使用如下脚本进行loss曲线的绘制。

```
compare_metric.py
import json
import os
from typing import List, Dict

import matplotlib.pyplot as plt
import numpy as np

解析 json 文件
def load_trainer_status(file_path):
 with open(file_path, "r") as f:
 trainer_status = json.load(f)
 return trainer_status.get("log_history")

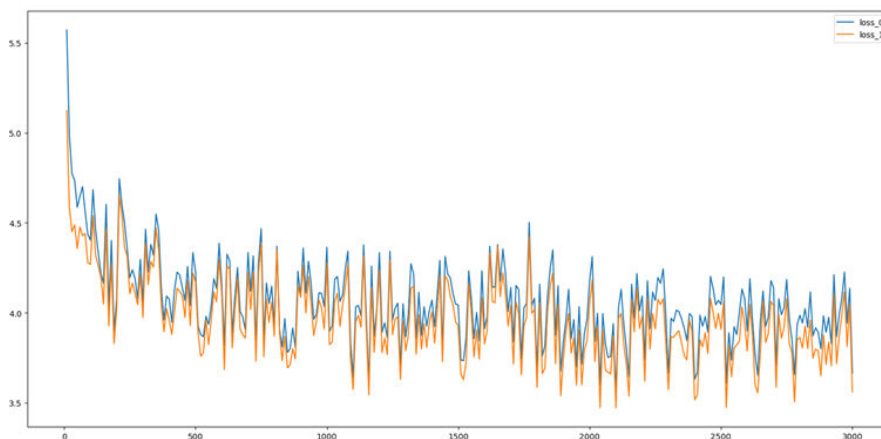
def plot_curve(data_source: List[Dict], tags: List[str]):
 fig, ax = plt.subplots()
 for tag in tags:
 # print(data_source[0], len(data_source[0]))
 # assert all([tag in status.keys() for status in data_source]), f"Tag {tag} is missing for data source."
 for index, source in enumerate(data_source):
 y = []
 x = []
 for log in source:
 x.append(log.get("step"))
 y.append(log.get(tag))
 ax.plot(x, y, label=f"{tag}_{index}")

 ax.legend()
 plt.savefig("loss.png")

if __name__ == "__main__":
 state_npu_path = os.path.join("trainer_state_npu.json")
 state_gpu_path = os.path.join("trainer_state_gpu.json")
 state_npu = load_trainer_status(state_npu_path)
 state_gpu = load_trainer_status(state_gpu_path)
 plot_curve([state_npu, state_gpu], ["loss"])
```

对比单卡模式下NPU和GPU训练曲线，发现loss曲线下下降趋势不一致。这说明迁移的模型存在精度偏差。

图 6-2 loss 曲线对比



图中蓝色loss\_0是NPU迭代曲线，黄色loss\_1是GPU的迭代曲线。

## 问题定位解决

使用ptdbg\_ascend工具dump全网数据，dump接口设置方法具体参考[PyTorch精度工具](#)。dump完成后compare GPU和NPU结果进行分析。

1. dropout算子引入了随机性偏差，如下图：

图 6-3 随机性偏差

| B  | C                                     | D                | E                  | F                | G                  | H        | I        | J        | K        | L        | M        | N        | O        | P         | Q                                             | R | S | T |
|----|---------------------------------------|------------------|--------------------|------------------|--------------------|----------|----------|----------|----------|----------|----------|----------|----------|-----------|-----------------------------------------------|---|---|---|
| 1  | Bench Name                            | NPU Tensor Dtype | Bench Tensor Dtype | NPU Tensor Dtype | Bench Tensor Dtype | MaxAbs   | NPU max  | NPU min  | NPU mean | Bench ma | Bench mi | Bench m  | Accuracy | Err_messa | Stack_Info                                    |   |   |   |
| 23 | Functional.embedding_1_forward_input0 | torch.float32    | torch.float32      | [1, 128]         | [1, 128]           | 1        | 0        | 127      | 0        | 63.5     | 127      | 0        | 63.5     | Yes       |                                               |   |   |   |
| 24 | Functional.embedding_1_forward_input1 | torch.float32    | torch.float32      | [128, 229]       | [128, 229]         | 1        | 0.001953 | 5.183584 | -5.26172 | 0.000107 | 5.183584 | -5.26172 | 0.000107 | Yes       |                                               |   |   |   |
| 25 | Functional.embedding_1_forward_input4 | <class 'float'>  | <class 'float'>    | 0                | 0                  | 1        | 0        | 2        | 2        | 2        | 2        | 2        | 2        | Yes       | This is type of scalar data, can not compare. |   |   |   |
| 26 | Functional.embedding_1_forward_input5 | <class 'bool'>   | <class 'bool'>     | 0                | 0                  | 1        | 0        | FALSE    | FALSE    | FALSE    | FALSE    | FALSE    | FALSE    | Yes       | This is type of scalar data, can not compare. |   |   |   |
| 27 | Functional.embedding_1_forward_input6 | <class 'bool'>   | <class 'bool'>     | 0                | 0                  | 1        | 0        | FALSE    | FALSE    | FALSE    | FALSE    | FALSE    | FALSE    | Yes       | This is type of scalar data, can not compare. |   |   |   |
| 28 | Functional.embedding_1_forward_output | torch.float32    | torch.float32      | [1, 128, 22]     | [1, 128, 22]       | 1        | 0.001953 | 5.183584 | -5.26172 | 0.000107 | 5.183584 | -5.26172 | 0.000107 | Yes       | 堆栈信息                                          |   |   |   |
| 29 | Functional.dropout_0_forward_input0   | torch.float16    | torch.float16      | [1, 128, 56]     | [1, 128, 56]       | 1        | 0.001953 | 5.183584 | -5.26172 | 0.000107 | 5.183584 | -5.26172 | 0.000107 | Yes       |                                               |   |   |   |
| 30 | Functional.dropout_0_forward_input1   | <class 'float'>  | <class 'float'>    | 0                | 0                  | 1        | 0        | 0.1      | 0.1      | 0.1      | 0.1      | 0.1      | 0.1      | Yes       | This is type of scalar data, can not compare. |   |   |   |
| 31 | Functional.dropout_0_forward_input2   | <class 'bool'>   | <class 'bool'>     | 0                | 0                  | 1        | 0        | TRUE     | TRUE     | TRUE     | TRUE     | TRUE     | TRUE     | Yes       | This is type of scalar data, can not compare. |   |   |   |
| 32 | Functional.dropout_0_forward_input3   | <class 'bool'>   | <class 'bool'>     | 0                | 0                  | 1        | 0        | FALSE    | FALSE    | FALSE    | FALSE    | FALSE    | FALSE    | Yes       | This is type of scalar data, can not compare. |   |   |   |
| 33 | Functional.dropout_0_forward_output   | torch.float16    | torch.float16      | [1, 128, 56]     | [1, 128, 56]       | 0.899809 | 5.828125 | 5.761719 | -5.84766 | 0.000179 | 5.757813 | -5.84766 | 5.69E-05 | No        |                                               |   |   |   |
| 34 | Tensor.permute_0_forward_input0       | torch.float16    | torch.float16      | [1, 128, 56]     | [1, 128, 56]       | 0.899809 | 5.828125 | 5.761719 | -5.84766 | 0.000179 | 5.757813 | -5.84766 | 5.69E-05 | No        |                                               |   |   |   |

根据堆栈信息定位得知dropout是使用的torch.nn.Dropout(), 为消除随机性需要将随机因子p改为0或者1, 此处是将model\_chatglm.py中随机因子改为了0, 如下修改:

图 6-4 随机因子改为 0

```

854 if self.pre_seq_len is not None:
855 for param in self.parameters():
856 param.requires_grad = False
857 self.prefix_tokens = torch.arange(self.pre_seq_len).long()
858 self.prefix_encoder = PrefixEncoder(config)
859 # self.dropout = torch.nn.Dropout(0.1)
860 self.dropout = torch.nn.Dropout(0.0)

```

2. 使用ptdbg修改register\_hook方式做精度溢出检查。结果显示Tensor\_\_add\_\_233\_forward执行时有溢出, 这里使用浮点数精度的是float16, 结果显示输入的最大、最小、平均值都为65504 (float16的精度范围是-65504至65504), 如下图所示:

图 6-5 精度溢出检查

```

2023-08-07 20:42:48(100)-[WARNING][overflow 3 times]: module name 'tensor__add__233_forward' is overflow and dump file is saved in '/home/ma-user/work/ChatGLM-6B-ptuning/ptdbg_dump_v3.1/rank0/overflow_info_20230807_124248_3.pkl'.
Traceback (most recent call last):
 File "main.py", line 459, in module-main()
 train_result = trainer.train(resume_from_checkpoint)
 File "/home/ma-user/work/ChatGLM-6B-ptuning/trainer.py", line 1639, in train
 ignore_keys = eval(ignore_keys_for_eval)
 File "/home/ma-user/work/ChatGLM-6B-ptuning/trainer.py", line 1904, in inner_training_loop
 tr_loss_step = self.training_step(model, inputs)
 File "/home/ma-user/work/ChatGLM-6B-ptuning/trainer.py", line 2665, in training_step
 loss.backward()
 File "/home/ma-user/anaconda3/envs/PyTorch-1.11.0/lib/python3.7/site-packages/torch/_tensor.py", line 363, in backward
 torch.autograd.backward(self, gradient, retain_graph, create_graph, input_tensors)
 File "/home/ma-user/anaconda3/envs/PyTorch-1.11.0/lib/python3.7/site-packages/torch/autograd/init_.py", line 175, in backward
 allow_unreachable=True, accumulate_grad=True) # Calls into the C++ engine to run the backward pass
 File "/home/ma-user/anaconda3/envs/PyTorch-1.11.0/lib/python3.7/site-packages/torch/autograd/function.py", line 253, in apply
 return user_cls(*args)
 File "/home/ma-user/anaconda3/envs/PyTorch-1.11.0/lib/python3.7/site-packages/torch/npu/utils/checkpoint.py", line 189, in backward
 OXP_CONST_VAR + OXP_OVERFLOW_FLAG + 18989
 File "/home/ma-user/anaconda3/envs/PyTorch-1.11.0/lib/python3.7/site-packages/ptdbg_ascend/hook_module/wrap_tensor.py", line 58, in tensor_op_template
 return TensorOpTemplate(op_name, hook)(*args, **kwargs)
 File "/home/ma-user/anaconda3/envs/PyTorch-1.11.0/lib/python3.7/site-packages/ptdbg_ascend/hook_module/hook_module.py", line 78, in __call__
 hook_result = hook(self, input, resall)
 File "/home/ma-user/anaconda3/envs/PyTorch-1.11.0/lib/python3.7/site-packages/ptdbg_ascend/overflow_check/overflow_check.py", line 107, in overflow_check_hook
 format(OverflowUtil.real_overflow_dump_times, os.path.realpath(dump_file_name)))
ValueError: [overflow 3 times]: dump file is saved in '/home/ma-user/work/ChatGLM-6B-ptuning/ptdbg_dump_v3.1/rank0/overflow_info_20230807_124248_3.pkl'
[0] [0] [0] [1:36?: ?it/s]
[PyTorch-1.11.0] [ma-user@2f6ba13a1a89 ptuning]$
[PyTorch-1.11.0] [ma-user@2f6ba13a1a89 ptuning]$ ls ptdbg_dump_v3.1/rank0/overflow_info_20230807_12
[PyTorch-1.11.0] [ma-user@2f6ba13a1a89 ptuning]$ ls ptdbg_dump_v3.1/rank0/overflow_info_20230807_124248_3.pkl
[PyTorch-1.11.0] [ma-user@2f6ba13a1a89 ptuning]$ cat ptdbg_dump_v3.1/rank0/overflow_info_20230807_124248_3.pkl
{"tensor__add__233_forward_input": 0, "1", [{"torch.float16": [1], [65504.0, 65504.0, 65504.0]}]}
{"tensor__add__233_forward_output": 101, [{"torch.float16": [1], [65504.0, 65504.0, 65504.0]}]}

```

因为在NPU下对INF和NAN的支持默认是饱和模式, 会将INF置为MAX, NAN置为0, 此处Tensor\_\_add\_\_233\_forward的输入输出都是fp16的, 会将Inf置为65504。但是在GPU下采用的是INF\_NAN模式 (保留INF及NAN的结果), 所以



在做精度对比时先修改NPU支持模式为INF\_NAN模式与GPU保持一致，请参考 [INF\\_NAN\\_MODE\\_ENABLE](#)。

开启INF\_NAN模式方式命令如下：

```
#shell
export INF_NAN_MODE_ENABLE=1
```

修改之后再次做溢出检查显示所有API正常，无溢出情况。

- 3. GPU dump数据缺失，从Tensor\_transpose\_2\_forward\_output之后没有与NPU对应的bench data数据。

图 6-6 GPU dump 数据

在pkl文件中找到对应缺失的位置，发现Tensor\_transpose\_2\_forward\_output之后，NPU下一个执行的算子是Tensor\_squeeze\_0\_forward\_input，而GPU下一个执行的算子是Tensor\_\_getitem\_\_6\_forward\_input。

图 6-7 api\_stack\_dump.pkl

根据stack信息查找到对应源码的代码行，发现对应函数上添加了@torch.jit.script装饰器，经过调试发现，GPU也执行了这个函数，但是没有dump算子执行信息，而且pdb无法在函数中正常中断，删除此装饰器后，GPU能够正常dump数据。

图 6-8 删除@torch.jit.script 装饰器

```

235 @torch.jit.script
236 def apply_rotary_pos_emb_index(q, k, cos, sin, position_id):
237 # position_id: [sq, b], q, k: [sq, b, np, hn], cos: [sq, 1, hn] -> [sq, b, 1, hn]
238 cos, sin = F.embedding(position_id, cos.squeeze(1)).unsqueeze(2), \
239 F.embedding(position_id, sin.squeeze(1)).unsqueeze(2)
240 q, k = (q * cos) + (rotate_half(q) * sin), (k * cos) + (rotate_half(k) * sin)
241 return q, k

```

加了@torch.jit.script装饰器，torch\_npu能采到数据，而GPU上则不行的原因：  
@torch.jit.script装饰器会将装饰函数作为ScriptFunction对象返回，不会产生  
dump数据。而目前该装饰器在torch\_npu下不生效，NPU会按照普通函数执行，  
因此能够采集到数据。从精度对比角度考虑，先删除@torch.jit.script可以保证这  
块GPU和NPU dump的数据对齐。

- compare表中Cosine列第一个出现偏差的位置，为einsum算子的输入。

图 6-9 Cosine 列的偏差

| A   | B                               | C                               | D                        | E    | F    | G    | H         | I        | J        | K        | L        | M         | N        | O        | P                    | Q                    | R |
|-----|---------------------------------|---------------------------------|--------------------------|------|------|------|-----------|----------|----------|----------|----------|-----------|----------|----------|----------------------|----------------------|---|
| 101 | Tensor_chunk_0_forward_output.1 | Tensor_chunk_0_forward_output.1 | torch.float(torch.float) | 1.32 | 1.32 | 1.32 | 1.0007812 | Nan      | 17.59375 | -25.1094 | -0.02756 | 17.59375  | -25.1094 | -0.02756 | Yes                  | Cannot compare by h/ |   |
| 114 | Torch_einsum_0_forward_input.2  | Torch_einsum_0_forward_input.2  | torch.float(torch.float) | 1.32 | 1.32 | 1.32 | 0.843986  | 0.674988 | 9.00515  | 1.0001   | 0.19873  | 1.0000133 | 0.124939 | No       | Cannot compare by h/ |                      |   |

查看堆栈信息发现是self.inv\_freq的值存在精度偏差，再追溯到self.inv\_freq的定义片段。

图 6-10 inv\_freq 的定义片段

```

177 class RotaryEmbedding(torch.nn.Module):
178 def __init__(self, dim, base=10000, precision=torch.half, learnable=False):
179 super().__init__()
180 inv_freq = 1. / (base ** (torch.arange(0, dim, 2).float() / dim))
181 inv_freq = inv_freq.half()
182 self.learnable = learnable
183 if learnable:
184 self.inv_freq = torch.nn.Parameter(inv_freq)
185 self.max_seq_len_cached = None
186 else:
187 self.register_buffer('inv_freq', inv_freq)
188 self.max_seq_len_cached = None
189 self.cos_cached = None
190 self.sin_cached = None
191 self.precision = precision

```

通过构造该计算公式，发现在x86上：torch+CPU和torch+GPU以及aarch64 torch  
+NPU场景的结果都是一致的，而aarch64 torch+CPU结果不同，如下：

图 6-11 torch+CPU

```
import torch

inv_freq = 1. / (10000 ** (torch.arange(0, 64, 2).float() / 64))
inv_freq.min()
```

torch + CPU x86

tensor(0.0001)

图 6-12 torch+GPU

```
import torch

inv_freq = 1. / (10000 ** (torch.arange(0, 64, 2).float().cuda() / 64))
inv_freq.min()
```

torch + CUDA x86

tensor(0.0001, device='cuda:0')

图 6-13 aarch64 torch+NPU

```
>>> import torch
>>> import torch_npu
Warning : ASCEND_HOME_PATH environment variable is not set.
>>> inv_freq = 1. / (10000 ** (torch.arange(0, 64, 2).float().npu() / 64))
>>> inv_freq.min()
tensor(0.0001, device='npu:0')
```

torch npu

图 6-14 aarch64 torch+CPU

```
>>> import torch
>>> inv_freq = 1. / (10000 ** (torch.arange(0, 64, 2).float() / 64))
>>> inv_freq.min()
tensor(0.0010)
```

torch + Ascend  
pytorch

而inv\_freq恰好都是在CPU上初始化的。修改NPU版代码，强制使用torch+NPU进行初始化后，可以消除einsum算子输入偏差的问题。修改如下：

```
inv_freq = 1. / (base ** (torch.arange(0, dim, 2).float().npu() / dim))
```

另外的一种修改方式是转换到double下进行计算。

图 6-15 转换到 double 下进行计算

```
>>> import torch
>>> inv_freq = 1. / (10000 ** (torch.arange(0, 64, 2).float() / 64))
>>> inv_freq.min()
tensor(0.0010)
>>> inv_freq = 1. / (10000 ** (torch.arange(0, 64, 2).double() / 64))
>>> inv_freq.min()
tensor(0.0001, dtype=torch.float64)
```

- 修复上述问题后，Cosine值第一次出现偏差的位置为permute算子，在backward阶段作为input引入。



图 6-16 permute 算子偏差

| #     | Bench Name                               | B             | C             | D                             | E                             | F        | G        | H        | I        | J        | K        | L        | M        | N        | O        | P        |          |
|-------|------------------------------------------|---------------|---------------|-------------------------------|-------------------------------|----------|----------|----------|----------|----------|----------|----------|----------|----------|----------|----------|----------|
| 21629 | Tensor_permute_0_backward_input.0        | torch.float16 | torch.float16 | torch.float[128, 1, 32, 128]  | torch.float[128, 1, 32, 128]  | 0.999998 | 0.000002 | 0.000002 | 0.000002 | 0.000002 | 0.000002 | 0.000002 | 0.000002 | 0.000002 | 0.000002 | 0.000002 | 0.000002 |
| 21630 | Tensor_permute_0_backward_output.0       | torch.float16 | torch.float16 | torch.float[128, 56, 32, 128] | torch.float[128, 56, 32, 128] | 1.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      |
| 21631 | Functional_dropout_0_backward_input.0    | torch.float16 | torch.float16 | torch.float[128, 56, 32, 128] | torch.float[128, 56, 32, 128] | 1.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      |
| 21632 | Functional_dropout_0_backward_output.0   | torch.float16 | torch.float16 | torch.float[128, 229376]      | torch.float[128, 229376]      | 1.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      |
| 21633 | Torch_embedding_1_backward_input.0       | torch.float32 | torch.float32 | torch.float[128, 229376]      | torch.float[128, 229376]      | 1.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      |
| 21634 | Torch_embedding_1_backward_output.0      | torch.float32 | torch.float32 | torch.float[128, 229376]      | torch.float[128, 229376]      | 1.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      |
| 21635 | Functional_embedding_1_backward_input.0  | torch.float32 | torch.float32 | torch.float[128, 229376]      | torch.float[128, 229376]      | 1.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      |
| 21636 | Functional_embedding_1_backward_output.0 | torch.float32 | torch.float32 | torch.float[128, 229376]      | torch.float[128, 229376]      | 1.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      |
| 21660 | Tensor_mul_0_forward_input.0             | torch.float32 | torch.float32 | torch.float[128, 229376]      | torch.float[128, 229376]      | 1.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      |
| 21662 | Tensor_mul_0_forward_output.0            | torch.float32 | torch.float32 | torch.float[128, 229376]      | torch.float[128, 229376]      | 1.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      |
| 21666 | Tensor_add_0_forward_input.0             | torch.float32 | torch.float32 | torch.float[128, 229376]      | torch.float[128, 229376]      | 1.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      |
| 21667 | Tensor_add_0_forward_input.1             | torch.float32 | torch.float32 | torch.float[128, 229376]      | torch.float[128, 229376]      | 1.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      |
| 21668 | Tensor_add_0_forward_output.0            | torch.float32 | torch.float32 | torch.float[128, 229376]      | torch.float[128, 229376]      | 1.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      |
| 21672 | Tensor_addcmul_0_forward_input.0         | torch.float32 | torch.float32 | torch.float[128, 229376]      | torch.float[128, 229376]      | 1.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      |
| 21673 | Tensor_addcmul_0_forward_input.1         | torch.float32 | torch.float32 | torch.float[128, 229376]      | torch.float[128, 229376]      | 1.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      |
| 21674 | Tensor_addcmul_0_forward_input.2         | torch.float32 | torch.float32 | torch.float[128, 229376]      | torch.float[128, 229376]      | 1.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      |
| 21675 | Tensor_addcmul_0_forward_output.0        | torch.float32 | torch.float32 | torch.float[128, 229376]      | torch.float[128, 229376]      | 1.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      |
| 21676 | Tensor_sqr_0_forward_input.0             | torch.float32 | torch.float32 | torch.float[128, 229376]      | torch.float[128, 229376]      | 1.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      |
| 21677 | Tensor_sqr_0_forward_output.0            | torch.float32 | torch.float32 | torch.float[128, 229376]      | torch.float[128, 229376]      | 1.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      |
| 21678 | Tensor_add_1_forward_input.0             | torch.float32 | torch.float32 | torch.float[128, 229376]      | torch.float[128, 229376]      | 1.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      |
| 21680 | Tensor_add_1_forward_output.0            | torch.float32 | torch.float32 | torch.float[128, 229376]      | torch.float[128, 229376]      | 1.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      |
| 21682 | Tensor_adddiv_0_forward_input.1          | torch.float32 | torch.float32 | torch.float[128, 229376]      | torch.float[128, 229376]      | 1.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      |
| 21683 | Tensor_adddiv_0_forward_input.2          | torch.float32 | torch.float32 | torch.float[128, 229376]      | torch.float[128, 229376]      | 1.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      |

由于在backward阶段ptdbg-ascend没有输出执行的堆栈信息，先查找了Tensor\_permute\_0在forward阶段相应的堆栈信息。

图 6-17 Tensor\_permute\_0 在 forward 阶段相应的堆栈信息

```
[~/home/ma-user/.cache/huggingface/modules/transformers_modules/chatglm_modeling_chatglm.py, '927', 'get_prompt', 'past_key_values = past_key_values.permute([2, 1, 0, 3]).split(2)']
```

可以得知此处进行了换轴操作，但是在forward时输入输出均无精度异常。因此转换排查思路，全局查找Cosine、MaxAbsErr值和Tensor\_permute\_0\_backward相同的行。发现在Tensor\_\_getitem\_\_490\_backward\_output.0处MaxAbsErr的值和Tensor\_permute\_0\_backward一样

图 6-18 Tensor\_\_getitem\_\_490\_backward\_output.0

| #     | NPU Name                               | Bench Name                             | B             | C             | D                               | E                               | F        | G        | H        | I        | J        | K        | L        | M        | N        |          |
|-------|----------------------------------------|----------------------------------------|---------------|---------------|---------------------------------|---------------------------------|----------|----------|----------|----------|----------|----------|----------|----------|----------|----------|
| 10269 | Tensor_transpose_184_backward_output.0 | Tensor_transpose_184_backward_output.0 | torch.float16 | torch.float16 | torch.float[256, 32, 128]       | torch.float[256, 32, 128]       | 0.999998 | 0.000002 | 0.000002 | 0.000002 | 0.000002 | 0.000002 | 0.000002 | 0.000002 | 0.000002 | 0.000002 |
| 10270 | Tensor_transpose_183_backward_input.0  | Tensor_transpose_183_backward_input.0  | torch.float16 | torch.float16 | torch.float[32, 128, 128]       | torch.float[32, 128, 128]       | 1.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      |
| 10271 | Tensor_transpose_183_backward_output.0 | Tensor_transpose_183_backward_output.0 | torch.float16 | torch.float16 | torch.float[128, 32, 128]       | torch.float[128, 32, 128]       | 1.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      |
| 10272 | Tensor_truediv_30_backward_input.0     | Tensor_truediv_30_backward_input.0     | torch.float16 | torch.float16 | torch.float[128, 1, 32, 128]    | torch.float[128, 1, 32, 128]    | 0.999998 | 0.000002 | 0.000002 | 0.000002 | 0.000002 | 0.000002 | 0.000002 | 0.000002 | 0.000002 | 0.000002 |
| 10273 | Tensor_truediv_30_backward_output.0    | Tensor_truediv_30_backward_output.0    | torch.float16 | torch.float16 | torch.float[128, 1, 32, 128]    | torch.float[128, 1, 32, 128]    | 0.999998 | 0.000002 | 0.000002 | 0.000002 | 0.000002 | 0.000002 | 0.000002 | 0.000002 | 0.000002 | 0.000002 |
| 10274 | Torch_cat_215_backward_input.0         | Torch_cat_215_backward_input.0         | torch.float16 | torch.float16 | torch.float[256, 1, 32, 128]    | torch.float[256, 1, 32, 128]    | 1.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      |
| 10275 | Torch_cat_215_backward_output.0        | Torch_cat_215_backward_output.0        | torch.float16 | torch.float16 | torch.float[128, 1, 32, 128]    | torch.float[128, 1, 32, 128]    | 1.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      |
| 10276 | Torch_cat_215_backward_input.1         | Torch_cat_215_backward_input.1         | torch.float16 | torch.float16 | torch.float[128, 1, 32, 128]    | torch.float[128, 1, 32, 128]    | 1.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      |
| 10277 | Torch_cat_214_backward_input.0         | Torch_cat_214_backward_input.0         | torch.float16 | torch.float16 | torch.float[256, 1, 32, 128]    | torch.float[256, 1, 32, 128]    | 0.999998 | 0.000002 | 0.000002 | 0.000002 | 0.000002 | 0.000002 | 0.000002 | 0.000002 | 0.000002 | 0.000002 |
| 10278 | Torch_cat_214_backward_output.0        | Torch_cat_214_backward_output.0        | torch.float16 | torch.float16 | torch.float[128, 1, 32, 128]    | torch.float[128, 1, 32, 128]    | 1.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      |
| 10279 | Torch_cat_214_backward_input.1         | Torch_cat_214_backward_input.1         | torch.float16 | torch.float16 | torch.float[128, 1, 32, 128]    | torch.float[128, 1, 32, 128]    | 0.999998 | 0.000002 | 0.000002 | 0.000002 | 0.000002 | 0.000002 | 0.000002 | 0.000002 | 0.000002 | 0.000002 |
| 10280 | Tensor_getitem_491_backward_input.0    | Tensor_getitem_491_backward_input.0    | torch.float16 | torch.float16 | torch.float[128, 1, 32, 128]    | torch.float[128, 1, 32, 128]    | 1.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      |
| 10281 | Tensor_getitem_491_backward_output.0   | Tensor_getitem_491_backward_output.0   | torch.float16 | torch.float16 | torch.float[2, 128, 1, 32, 128] | torch.float[2, 128, 1, 32, 128] | 1.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      |
| 10282 | Tensor_getitem_490_backward_input.0    | Tensor_getitem_490_backward_input.0    | torch.float16 | torch.float16 | torch.float[128, 1, 32, 128]    | torch.float[128, 1, 32, 128]    | 1.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      |
| 10283 | Tensor_getitem_490_backward_output.0   | Tensor_getitem_490_backward_output.0   | torch.float16 | torch.float16 | torch.float[2, 128, 1, 32, 128] | torch.float[2, 128, 1, 32, 128] | 1.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      | 0.0      |

并且Bench data列的max、min、mean对应值也一致，但是Tensor\_\_getitem\_\_490\_backward\_output.0在NPU下的max、min、mean值都是0，代表该处是全零的向量。猜想应该是梯度计算错误。使用PyTorch的index\_select函数作为getitem函数的替代，对modeling\_chatglm.py做如下修改：

图 6-19 modeling\_chatglm.py 修改

```
256 if layer_past is not None:
257 # past_key, past_value = layer_past[0], layer_past[1]
258 past_key = layer_past.index_select(0, torch.tensor([0]).to(layer_past.device)).squeeze(0)
259 past_value = layer_past.index_select(0, torch.tensor([1]).to(layer_past.device)).squeeze(0)
```

再次dump对比精度，发现该算子精度问题得到解决。

图 6-20 Tensor\_permute\_0 精度对比

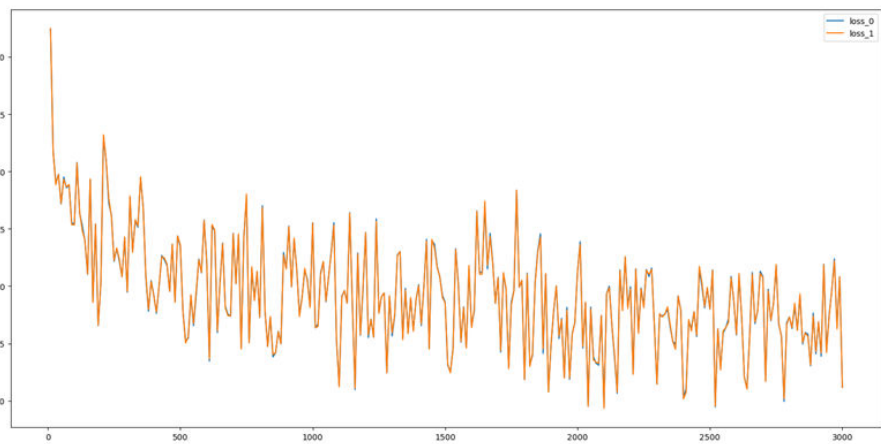
| ID   | NPU Name                             | Bench Name                             | NPU Tensor     | Bench Tensor   | NPU Te                   | Bench Te                 | Cosine      | MaxAbs   | MaxRel | NPU m    | Bench m  | NPU m    | Bench m  | Bench L  | Bench L  | Bench L  | Accurat |
|------|--------------------------------------|----------------------------------------|----------------|----------------|--------------------------|--------------------------|-------------|----------|--------|----------|----------|----------|----------|----------|----------|----------|---------|
| 2218 | Tensor_permute_0_backward_input.0    | Tensor_permute_0_backward_input.0      | torch.float16  | torch.float16  | [56, 128, 1, 56, 128, 1] | [56, 128, 1, 56, 128, 1] | 0.999985    | 0.000035 | Nan    | 0.004658 | -0.00243 | 0        | 0.004646 | -0.00243 | 0        | Yes      |         |
| 2218 | Tensor_permute_0_backward_output.0   | Tensor_permute_0_backward_output.0     | torch.float16  | torch.float16  | [1, 128, 56, 1, 128, 56] | [1, 128, 56, 1, 128, 56] | 0.999985    | 0.000035 | Nan    | 0.004658 | -0.00243 | 0        | 0.004646 | -0.00243 | 0        | Yes      |         |
| 2219 | Functional_dropout_0_backward_input  | Functional_dropout_0_backward_input.0  | torch.float16  | torch.float16  | [1, 128, 56, 1, 128, 56] | [1, 128, 56, 1, 128, 56] | 0.999985    | 0.000035 | Nan    | 0.004658 | -0.00243 | 0        | 0.004646 | -0.00243 | 0        | Yes      |         |
| 2219 | Functional_dropout_0_backward_output | Functional_dropout_0_backward_output.0 | torch.float16  | torch.float16  | [1, 128, 56, 1, 128, 56] | [1, 128, 56, 1, 128, 56] | 0.999985    | 0.000035 | Nan    | 0.004658 | -0.00243 | 0        | 0.004646 | -0.00243 | 0        | Yes      |         |
| 2219 | Tensor_embedding_1_backward_input.0  | Tensor_embedding_1_backward_input.0    | torch.float32  | torch.float32  | [1, 128, 22, 1, 128, 22] | [1, 128, 22, 1, 128, 22] | 0.999985    | 0.000035 | Nan    | 0.004658 | -0.00243 | 9.64e-09 | 0.004646 | -0.00243 | 9.65e-09 | Yes      |         |
| 2219 | Tensor_embedding_1_backward_output.0 | Tensor_embedding_1_backward_output.0   | torch.float32  | torch.float32  | [128, 2293, 128, 2293]   | [128, 2293, 128, 2293]   | 0.999985    | 0.000035 | Nan    | 0.004658 | -0.00243 | 9.64e-09 | 0.004646 | -0.00243 | 9.65e-09 | Yes      |         |
| 2219 | Functional_embedding_1_backward_in   | Functional_embedding_1_backward_inpu   | torch.float32  | torch.float32  | [1, 128, 22, 1, 128, 22] | [1, 128, 22, 1, 128, 22] | 0.999985    | 0.000035 | Nan    | 0.004658 | -0.00243 | 9.64e-09 | 0.004646 | -0.00243 | 9.65e-09 | Yes      |         |
| 2219 | Functional_embedding_1_backward_out  | Functional_embedding_1_backward_out    | torch.float32  | torch.float32  | [128, 2293, 128, 2293]   | [128, 2293, 128, 2293]   | 0.999985    | 0.000035 | Nan    | 0.004658 | -0.00243 | 9.64e-09 | 0.004646 | -0.00243 | 9.65e-09 | Yes      |         |
| 2219 | Tensor_snan_0_forward_input.0        | Tensor_snan_0_forward_input.0          | torch.float16  | torch.float16  | [0]                      | [0]                      | unsupported | 0        | Nan    | 0        | 5.882813 | 5.882813 | 5.882813 | 5.882813 | 5.882813 | 5.882813 | Nan     |
| 2219 | Tensor_snan_0_forward_output         | Tensor_snan_0_forward_output           | torch.bool     | torch.bool     | [0]                      | [0]                      | unsupported | 0        | Nan    | [0]      | [0]      | [0]      | [0]      | [0]      | [0]      | [0]      | Nan     |
| 2219 | Tensor_bool_84_forward_input.0       | Tensor_bool_84_forward_input.0         | torch.bool     | torch.bool     | [0]                      | [0]                      | unsupported | 0        | Nan    | [0]      | [0]      | [0]      | [0]      | [0]      | [0]      | [0]      | Nan     |
| 2219 | Tensor_bool_84_forward_output        | Tensor_bool_84_forward_output          | <class 'bool'> | <class 'bool'> | [0]                      | [0]                      | unsupported | 0        | Nan    | FALSE    | FALSE    | FALSE    | FALSE    | FALSE    | FALSE    | FALSE    | Nan     |
| 2220 | Tensor_sni_0_forward_input.0         | Tensor_sni_0_forward_input.0           | torch.float16  | torch.float16  | [0]                      | [0]                      | unsupported | 0        | Nan    | 0        | 5.882813 | 5.882813 | 5.882813 | 5.882813 | 5.882813 | 5.882813 | Nan     |
| 2220 | Tensor_sni_0_forward_output          | Tensor_sni_0_forward_output            | torch.bool     | torch.bool     | [0]                      | [0]                      | unsupported | 0        | Nan    | [0]      | [0]      | [0]      | [0]      | [0]      | [0]      | [0]      | Nan     |
| 2220 | Tensor_bool_85_forward_input.0       | Tensor_bool_85_forward_input.0         | torch.bool     | torch.bool     | [0]                      | [0]                      | unsupported | 0        | Nan    | [0]      | [0]      | [0]      | [0]      | [0]      | [0]      | [0]      | Nan     |
| 2220 | Tensor_bool_85_forward_output        | Tensor_bool_85_forward_output          | <class 'bool'> | <class 'bool'> | [0]                      | [0]                      | unsupported | 0        | Nan    | FALSE    | FALSE    | FALSE    | FALSE    | FALSE    | FALSE    | FALSE    | Nan     |
| 2220 | Tensor_sadd_0_forward_input.0        | Tensor_sadd_0_forward_input.0          | torch.float32  | torch.float32  | [0]                      | [0]                      | unsupported | 0        | Nan    | 0        | 5.882813 | 5.882813 | 5.882813 | 5.882813 | 5.882813 | 5.882813 | Nan     |
| 2220 | Tensor_sadd_0_forward_output.1       | Tensor_sadd_0_forward_output.1         | torch.float16  | torch.float16  | [0]                      | [0]                      | unsupported | 0        | Nan    | 0        | 5.882813 | 5.882813 | 5.882813 | 5.882813 | 5.882813 | 5.882813 | Nan     |
| 2220 | Tensor_sadd_0_forward_output         | Tensor_sadd_0_forward_output           | torch.float32  | torch.float32  | [0]                      | [0]                      | unsupported | 0        | Nan    | 0        | 5.882813 | 5.882813 | 5.882813 | 5.882813 | 5.882813 | 5.882813 | Nan     |

图 6-21 算子精度对比

| ID    | NPU Name                            | Bench Name                          | NPU Tensor    | Bench Tensor  | NPU Te                   | Bench Te                 | Cosine   | MaxAbs   | MaxRel | NPU m    | Bench m  | NPU m    | Bench m  | Bench L  | Bench L  | Bench L | Accurat |
|-------|-------------------------------------|-------------------------------------|---------------|---------------|--------------------------|--------------------------|----------|----------|--------|----------|----------|----------|----------|----------|----------|---------|---------|
| 10525 | Tensor_transpose_184_backward_outp  | Tensor_transpose_184_backward_outp  | torch.float16 | torch.float16 | [256, 32, 1, 256, 32, 1] | [256, 32, 1, 256, 32, 1] | 0.999984 | 0.000031 | Nan    | 0.003242 | -0.00496 | 0        | 0.003249 | -0.00499 | 0        | Yes     |         |
| 10526 | Tensor_transpose_183_backward_inpu  | Tensor_transpose_183_backward_inpu  | torch.float16 | torch.float16 | [32, 128, 1, 32, 128, 1] | [32, 128, 1, 32, 128, 1] | 0.999984 | 0.000031 | Nan    | 1.000078 | -1.41895 | 1.97e-05 | 1.079102 | -1.41899 | 1.94e-05 | Yes     |         |
| 10527 | Tensor_transpose_183_backward_outp  | Tensor_transpose_183_backward_outp  | torch.float16 | torch.float16 | [128, 32, 1, 128, 32, 1] | [128, 32, 1, 128, 32, 1] | 0.999984 | 0.000031 | Nan    | 1.000078 | -1.41895 | 1.97e-05 | 1.079102 | -1.41899 | 1.94e-05 | Yes     |         |
| 10528 | Tensor_truediv_30_backward_inpu     | Tensor_truediv_30_backward_inpu     | torch.float16 | torch.float16 | [128, 1, 32, 128, 1, 32] | [128, 1, 32, 128, 1, 32] | 0.999984 | 0.000031 | Nan    | 1.000078 | -1.41895 | 1.97e-05 | 1.079102 | -1.41899 | 1.94e-05 | Yes     |         |
| 10529 | Tensor_truediv_30_backward_outp     | Tensor_truediv_30_backward_outp     | torch.float16 | torch.float16 | [128, 1, 32, 128, 1, 32] | [128, 1, 32, 128, 1, 32] | 0.999984 | 0.000031 | Nan    | 0.00367  | -0.00482 | 5.96e-08 | 0.003668 | -0.00482 | 5.96e-08 | Yes     |         |
| 10530 | Tensor_cat_215_backward_input.0     | Tensor_cat_215_backward_input.0     | torch.float16 | torch.float16 | [256, 1, 32, 256, 1, 32] | [256, 1, 32, 256, 1, 32] | 1        | 0.00001  | Nan    | 0.00367  | -0.003   | 0        | 0.00367  | -0.003   | 0        | Yes     |         |
| 10531 | Tensor_cat_215_backward_output.0    | Tensor_cat_215_backward_output.0    | torch.float16 | torch.float16 | [128, 1, 32, 128, 1, 32] | [128, 1, 32, 128, 1, 32] | 1        | 0.00002  | Nan    | 0.00633  | -0.00556 | #####    | 0.00632  | -0.00556 | #####    | Yes     |         |
| 10532 | Tensor_cat_215_backward_output.1    | Tensor_cat_215_backward_output.1    | torch.float16 | torch.float16 | [128, 1, 32, 128, 1, 32] | [128, 1, 32, 128, 1, 32] | 1        | 0.00001  | Nan    | 0.00367  | -0.003   | 1.19e-07 | 0.00367  | -0.003   | 1.19e-07 | Yes     |         |
| 10533 | Tensor_cat_214_backward_input.0     | Tensor_cat_214_backward_input.0     | torch.float16 | torch.float16 | [256, 1, 32, 256, 1, 32] | [256, 1, 32, 256, 1, 32] | 0.999984 | 0.000031 | Nan    | 0.003242 | -0.00496 | 0        | 0.003249 | -0.00499 | 0        | Yes     |         |
| 10534 | Tensor_cat_214_backward_output.0    | Tensor_cat_214_backward_output.0    | torch.float16 | torch.float16 | [128, 1, 32, 128, 1, 32] | [128, 1, 32, 128, 1, 32] | 1        | 0.00006  | Nan    | 0.002789 | -0.00216 | 5.96e-08 | 0.002785 | -0.00216 | 5.96e-08 | Yes     |         |
| 10535 | Tensor_cat_214_backward_output.1    | Tensor_cat_214_backward_output.1    | torch.float16 | torch.float16 | [128, 1, 32, 128, 1, 32] | [128, 1, 32, 128, 1, 32] | 0.999983 | 0.000031 | Nan    | 0.003242 | -0.00496 | #####    | 0.003248 | -0.00499 | #####    | Yes     |         |
| 10536 | Tensor_squeeze_185_backward_inpu    | Tensor_squeeze_185_backward_inpu    | torch.float16 | torch.float16 | [128, 1, 32, 128, 1, 32] | [128, 1, 32, 128, 1, 32] | 1        | 0.00002  | Nan    | 0.00633  | -0.00556 | #####    | 0.00632  | -0.00556 | #####    | Yes     |         |
| 10537 | Tensor_squeeze_185_backward_outp    | Tensor_squeeze_185_backward_outp    | torch.float16 | torch.float16 | [1, 128, 1, 1, 128, 1]   | [1, 128, 1, 1, 128, 1]   | 1        | 0.00002  | Nan    | 0.00633  | -0.00556 | #####    | 0.00632  | -0.00556 | #####    | Yes     |         |
| 10538 | Tensor_index_select_61_backward_inp | Tensor_index_select_61_backward_inp | torch.float16 | torch.float16 | [1, 128, 1, 1, 128, 1]   | [1, 128, 1, 1, 128, 1]   | 1        | 0.00002  | Nan    | 0.00633  | -0.00556 | #####    | 0.00632  | -0.00556 | #####    | Yes     |         |
| 10539 | Tensor_index_select_61_backward_out | Tensor_index_select_61_backward_out | torch.float16 | torch.float16 | [2, 128, 1, 2, 128, 1]   | [2, 128, 1, 2, 128, 1]   | 1        | 0.00002  | Nan    | 0.00633  | -0.00556 | #####    | 0.00632  | -0.00556 | #####    | Yes     |         |
| 10540 | Tensor_squeeze_184_backward_inpu    | Tensor_squeeze_184_backward_inpu    | torch.float16 | torch.float16 | [128, 1, 32, 128, 1, 32] | [128, 1, 32, 128, 1, 32] | 1        | 0.00006  | Nan    | 0.002789 | -0.00216 | 5.96e-08 | 0.002785 | -0.00216 | 5.96e-08 | Yes     |         |
| 10541 | Tensor_squeeze_184_backward_outp    | Tensor_squeeze_184_backward_outp    | torch.float16 | torch.float16 | [1, 128, 1, 1, 128, 1]   | [1, 128, 1, 1, 128, 1]   | 1        | 0.00006  | Nan    | 0.002789 | -0.00216 | 5.96e-08 | 0.002785 | -0.00216 | 5.96e-08 | Yes     |         |
| 10542 | Tensor_index_select_60_backward_inp | Tensor_index_select_60_backward_inp | torch.float16 | torch.float16 | [1, 128, 1, 1, 128, 1]   | [1, 128, 1, 1, 128, 1]   | 1        | 0.00006  | Nan    | 0.002789 | -0.00216 | 5.96e-08 | 0.002785 | -0.00216 | 5.96e-08 | Yes     |         |
| 10543 | Tensor_index_select_60_backward_out | Tensor_index_select_60_backward_out | torch.float16 | torch.float16 | [2, 128, 1, 2, 128, 1]   | [2, 128, 1, 2, 128, 1]   | 1        | 0.00006  | Nan    | 0.002789 | -0.00216 | 5.96e-08 | 0.002785 | -0.00216 | 5.96e-08 | Yes     |         |

修改上述问题之后，重新对比精度数据后发现，重新进行训练任务，通过对比NPU和GPU的loss曲线，可以发现，两者的下降趋势几乎是一致的。

图 6-22 loss 曲线



图中蓝色loss\_0是NPU的loss曲线，黄色loss\_1是GPU的loss曲线。

## 6.1.5 性能调优

### 算子优化

为了更好地发挥昇腾设备的性能，将ChatGLM-6B原模型中的部分算子替换成了NPU亲和的算子，修改的是modeling\_chatglm.py文件，下图通过对比列举了对应的修改方式，图示中左边为原始方式，右边为修改后的方式。

1. 使用torch.bmm替换torch.baddbmm。

图 6-23 torch.bmm 替换

```

287 manual_result = torch.zeros(
288 1, 1, 1,
289 dtype=query_layer.dtype,
290 device=query_layer.device,
291)
292 manual_result = torch.baddbmm(
293 manual_result,
294 query_layer.transpose(0, 1), # [b * np, sq, hn]
295 key_layer.transpose(0, 1).transpose(1, 2), # [b * np, hm, sk]
296 beta=0.0,
297 alpha=1.0,
298)
299
300 manual_result = torch.bmm(query_layer.transpose(0, 1), key_layer.permute(1, 2, 0))

```

因为toch.baddbmm函数中beta=0.0、alpha=1.0，所以是等价替换。

2. npu\_scaled\_masked\_softmax亲和api替换。

图 6-24 亲和 api 替换

```

301 self_scale_mask_softmax_scale = query_key_layer_scaling_coeff
302 attention_probs = self_scale_mask_softmax(attention_scores, attention_mask.contiguous())
303
304 attention_probs = npu_scaled_masked_softmax(attention_scores, attention_mask,
305 query_key_layer_scaling_coeff, False)

```

3. 连续性转换。

图 6-25 连续性转换

```

455 cos, sin = self.rotary_emb(q1, seq_len=position_ids.max()+1)
456 position_ids, block_position_ids = position_ids[:, 0, :].transpose(0, 1).contiguous(), \
457 position_ids[:, 1, :].transpose(0, 1).contiguous()
458
459 q1, q2, k1, k2 = q1.contiguous(), q2.contiguous(), k1.contiguous(), k2.contiguous()
460 cos, sin = self.rotary_emb(q1, seq_len=q1.shape[0])
461 # position_ids, block_position_ids = position_ids[:, 0, :].transpose(0, 1).contiguous(), \
462 # position_ids[:, 1, :].transpose(0, 1).contiguous()
463 # modify by lig
464 position_ids_1 = position_ids.permute(1, 2, 0).contiguous()
465 position_ids = position_ids_1[0, :, :]
466 block_position_ids = position_ids_1[1, :, :]

```

4. 数组切片操作改用torch接口方式。

图 6-26 数组切片操作修改 1

```

218 cos_cached = emb.cos()[None, :]
219 sin_cached = emb.sin()[None, :]
220
221 cos_cached = emb.cos().unsqueeze(1)
222 sin_cached = emb.sin().unsqueeze(1)

```

图 6-27 数组切片操作修改 2

```

223 x1, x2 = x[:, :, x.shape[-1] // 2, x[:, :, x.shape[-1] // 2]
224
225 x1, x2 = torch.chunk(x, 2, dim=-1)

```

5. gelu小算子使用torch的fast\_gelu()、gelu()融合算子替换。

图 6-28 融合算子替换

```

@torch.jit.script
def fast_gelu_impl(x):
 """OpenAI's gelu implementation"""
 return 0.5 * x * (1.0 + torch.tanh(0.7978845608928654 * x *
 (1.0 + 0.044715 * x * x)))

@torch.jit.script
def gelu_impl(x):
 """OpenAI's gelu implementation"""
 # logger.warning_once("*****use origin gelu")
 return 0.5 * x * (1.0 + torch.tanh(0.7978845608928654 * x *
 (1.0 + 0.044715 * x * x)))
 # logger.warning_once("*****use npu fast_gelu")
 # return torch.fast_gelu(x)
 # logger.warning_once("*****use torch functional gelu")
 return F.gelu(x)

```

## profiling 数据采集

在本例chatglm-6B中，添加profiling接口入口在ptuning/trainer.py的\_inner\_training\_loop()下。具体采集方式参考[Ascend PyTorch Profiler数据采集与分析方式](#)。

## 调优结果

这里对deepspeed单机8卡环境下，调优之前和调优之后的train metrics做了统计，结果如下。

性能基线：

```

***** train metrics *****
epoch = 0.06
train_loss = 3.0146
train_runtime = 2:15:20.44
train_samples = 1649399

```

```
train_samples_per_second = 12.61
train_steps_per_second = 0.012
```

算子调优后结果:

```
**** train metrics ****
epoch = 0.06
train_loss = 3.0128
train_runtime = 1:39:41.32
train_samples = 1649399
train_samples_per_second = 17.12
train_steps_per_second = 0.017
```

## 6.1.6 常见问题

### 6.1.6.1 报错提示 “RuntimeError: Default process group has not been initialized, please make sure to call init\_process\_group.”

#### 问题现象

报错提示 “RuntimeError: Default process group has not been initialized, please make sure to call init\_process\_group.”。

#### 原因分析

原因由于单卡脚本中未添加参数 “--local\_rank -1”，单卡执行脚本如下，需要指定 local\_rank 为 -1 为单卡模式。

```
ptuning/run_npu_1d.sh
export ASCEND_RT_VISIBLE_DEVICES=0 # 指定 0 号卡对当前进程可见
PRE_SEQ_LEN=128
LR=2e-2

python3 ptuning/main.py \
 --do_train \
 --train_file ${HOME}/AdvertiseGen/train.json \
 --validation_file ${HOME}/AdvertiseGen/dev.json \
 --prompt_column content \
 --response_column summary \
 --overwrite_cache \
 --model_name_or_path ${HOME}/chatglm \
 --output_dir output/adgen-chatglm-6b-pt-PRE_SEQ_LEN-LR \
 --overwrite_output_dir \
 --max_source_length 64 \
 --max_target_length 64 \
 --per_device_train_batch_size 4 \
 --per_device_eval_batch_size 1 \
 --gradient_accumulation_steps 1 \
 --predict_with_generate \
 --max_steps 3000 \
 --logging_steps 10 \
 --save_steps 1000 \
 --learning_rate $LR \
 --pre_seq_len $PRE_SEQ_LEN \
 --local_rank -1
```

#### 处理方法

单卡执行脚本中添加参数 “--local\_rank -1”。

多卡模式下无需指定，会默认启动 DistributedDataParallel (DDP) 多卡并行模式。GPU 环境单卡执行同样需要指定 local\_rank 为 -1。



## 6.1.6.2 训练运行报错 AttributeError: 'torch\_npu.C.\_NPUDeviceProperties' object has no attribute 'multi\_processor\_count'

### 问题现象

训练运行报错 “AttributeError: 'torch\_npu.C.\_NPUDeviceProperties' object has no attribute 'multi\_processor\_count'”。

图 6-29 报错信息

```
Traceback (most recent call last):
 File "main.py", line 439, in <module>
 main()
 File "main.py", line 378, in main
 train_result = trainer.train(resume_from_checkpoint=checkpoint)
 File "/home/renlei/ChatGLM-6B-main/ptuning/trainer.py", line 1639, in train
 ignore_keys_for_eval=ignore_keys_for_eval,
 File "/home/renlei/ChatGLM-6B-main/ptuning/trainer.py", line 1722, in _inner_training_loop
 model = self._wrap_model(self.model_wrapped)
 File "/home/renlei/ChatGLM-6B-main/ptuning/trainer.py", line 1392, in _wrap_model
 model = nn.DataParallel(model)
 File "/home/ma-user/anaconda3/envs/PyTorch-1.11.0/lib/python3.7/site-packages/torch/nn/parallel/data_parallel.py", line
e 142, in _init
 check_balance(self.device_ids)
 File "/home/ma-user/anaconda3/envs/PyTorch-1.11.0/lib/python3.7/site-packages/torch/nn/parallel/data_parallel.py", lin
e 36, in check_balance
 if warn_imbalance(lambda props: props.multi_processor_count):
 File "/home/ma-user/anaconda3/envs/PyTorch-1.11.0/lib/python3.7/site-packages/torch/nn/parallel/data_parallel.py", lin
e 26, in warn_imbalance
 values = [get_prop(props) for props in dev_props]
 File "/home/ma-user/anaconda3/envs/PyTorch-1.11.0/lib/python3.7/site-packages/torch/nn/parallel/data_parallel.py", lin
e 26, in <listcomp>
 values = [get_prop(props) for props in dev_props]
 File "/home/ma-user/anaconda3/envs/PyTorch-1.11.0/lib/python3.7/site-packages/torch/nn/parallel/data_parallel.py", lin
e 36, in <lambda>
 if warn_imbalance(lambda props: props.multi_processor_count):
AttributeError: 'torch_npu.C._NPUDeviceProperties' object has no attribute 'multi_processor_count'
(PyTorch-1.11.0) [root@ed0481b03994 ptuning]# pip show torch_npu
Name: torch-npu
Version: 1.11.0.post1.dev20230719
Summary: NPU bridge for PyTorch
Home-page: https://github.com/ascend/pytorch
Author: UNKNOWN
Author-email: UNKNOWN
License: UNKNOWN
Location: /home/ma-user/anaconda3/envs/PyTorch-1.11.0/lib/python3.7/site-packages
Requires:
Required-by:
```

### 原因分析

这是因为torch\_npu当前不支持DataParallel(DP) 并行模式。

### 处理方法

如果是运行单卡模式，在训练脚本中加入export ASCEND\_RT\_VISIBLE\_DEVICES=0（指定 0 号卡对当前进程可见）。多卡环境模式需要运行DDP并行模式。

## 6.1.6.3 deepspeed 多卡训练报错 TypeError: deepspeed\_init() got an unexpected keyword argument 'resume\_from\_checkpoint'

### 问题现象

deepspeed多卡训练报错TypeError: deepspeed\_init() got an unexpected keyword argument 'resume\_from\_checkpoint'

### 原因分析

由于transformers版本问题，使用transformers==4.29.2。

### 处理方法

请参见[运行bash ds\\_train\\_finetune.sh报错](#)。

### 6.1.6.4 Huggingface 缓存目录空间不足，出现 OSError: [Errno 122] Disk quota exceeded:

#### 问题现象

报错提示OSError: [Errno 122] Disk quota exceeded。

#### 原因分析

默认情况下，下载数据集缓存目录为“~/cache/huggingface/dataset”，Huggingface缓存目录空间不足导致出现该报错。

#### 处理方法

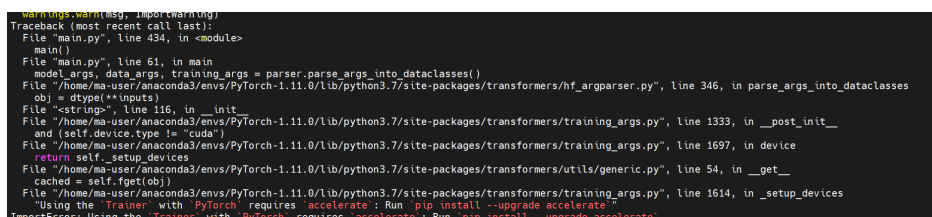
通过环境变量“HF\_HOME”设置Huggingface的缓存目录为比较大的路径，或者对“~/cache”目录扩容。

### 6.1.6.5 调用 transformers 出现 ImportError: Using the `Trainer` with `PyTorch` requires `accelerate`: Run `pip install --upgrade accelerate`

#### 问题现象

调用transformers出现ImportError: Using the `Trainer` with `PyTorch` requires `accelerate`: Run `pip install --upgrade accelerate`。

图 6-30 报错信息



```
WARNING: pip is using legacy fallback resolver; pip 23.0+ uses the modern dependency resolver by default. Run 'pip install --upgrade pip' to get the latest pip version.
Traceback (most recent call last):
 File "main.py", line 434, in <module>
 main()
 File "main.py", line 61, in main
 model_args, data_args, training_args = parser.parse_args_into_dataclasses()
 File ~/home/ma-user/anaconda3/envs/PyTorch-1.11.0/lib/python3.7/site-packages/transformers/hf_argparser.py, line 346, in parse_args_into_dataclasses
 obj = dtype(**inputs)
 File ~-strings, line 116, in __init__
 File ~/home/ma-user/anaconda3/envs/PyTorch-1.11.0/lib/python3.7/site-packages/transformers/training_args.py, line 1333, in __post_init__
 and (self.device.type != "cuda")
 File ~/home/ma-user/anaconda3/envs/PyTorch-1.11.0/lib/python3.7/site-packages/transformers/training_args.py, line 1697, in device
 return self._setup_devices
 File ~/home/ma-user/anaconda3/envs/PyTorch-1.11.0/lib/python3.7/site-packages/transformers/accelerator.py, line 54, in __get__
 cached = self.fget(obj)
 File ~/home/ma-user/anaconda3/envs/PyTorch-1.11.0/lib/python3.7/site-packages/transformers/training_args.py, line 1614, in _setup_devices
 "Using the `Trainer` with `PyTorch` requires `accelerate`: Run `pip install --upgrade accelerate`"
ImportError: Using the `Trainer` with `PyTorch` requires `accelerate`: Run `pip install --upgrade accelerate`
```

#### 原因分析

accelerate库版本需要升级。

#### 处理方法

升级accelerate库，执行“pip install accelerate --upgrade”。

### 6.1.6.6 调用 transformers 出现 ImportError: libblas.so.3: cannot open shared object file: No such file or directory

#### 问题现象

调用transformers出现ImportError: libblas.so.3: cannot open shared object file: No such file or directory

## 原因分析

scikit-learn库版本需要升级。

## 处理方法

升级scikit-learn库，执行“pip install scikit-learn --upgrade”。

### 6.1.6.7 transformers 调用 cuda 上的操作，或者执行卡死

## 问题现象

图 6-31 报错信息

```
No modifications detected for re-loaded extension module utils, skipping build step...
Loading extension module utils...
Time to load utils op: 0.00607285908378906 seconds
Using /root/.cache/torch_extensions/py37_cpu as PyTorch extensions root...
No modifications detected for re-loaded extension module utils, skipping build step...
Loading extension module utils...
Time to load utils op: 0.0069748925699462891 seconds
Using /root/.cache/torch_extensions/py37_cpu as PyTorch extensions root...
No modifications detected for re-loaded extension module utils, skipping build step...
Loading extension module utils...
Time to load utils op: 0.0011649131774902344 seconds
Using /root/.cache/torch_extensions/py37_cpu as PyTorch extensions root...
No modifications detected for re-loaded extension module utils, skipping build step...
Loading extension module utils...
Time to load utils op: 0.0013995170593261719 seconds
Using /root/.cache/torch_extensions/py37_cpu as PyTorch extensions root...
No modifications detected for re-loaded extension module utils, skipping build step...
Loading extension module utils...
Time to load utils op: 0.002980470657348633 seconds
09/28/2023 11:07:45 - WARNING - transformers_modules.chatglm.modeling_chatglm - 'use_cache=True' is incompatible with gradient checkpointing. Setting 'use_cache=False'
09/28/2023 11:07:45 - WARNING - transformers_modules.chatglm.modeling_chatglm - 'use_cache=True' is incompatible with gradient checkpointing. Setting 'use_cache=False'
09/28/2023 11:07:45 - WARNING - transformers_modules.chatglm.modeling_chatglm - 'use_cache=True' is incompatible with gradient checkpointing. Setting 'use_cache=False'
09/28/2023 11:07:46 - WARNING - transformers_modules.chatglm.modeling_chatglm - 'use_cache=True' is incompatible with gradient checkpointing. Setting 'use_cache=False'
09/28/2023 11:07:46 - WARNING - transformers_modules.chatglm.modeling_chatglm - 'use_cache=True' is incompatible with gradient checkpointing. Setting 'use_cache=False'
09/28/2023 11:07:46 - WARNING - transformers_modules.chatglm.modeling_chatglm - 'use_cache=True' is incompatible with gradient checkpointing. Setting 'use_cache=False'
09/28/2023 11:07:46 - WARNING - transformers_modules.chatglm.modeling_chatglm - 'use_cache=True' is incompatible with gradient checkpointing. Setting 'use_cache=False'
Warning: Device do not support double dtype now, dtype cast repalce with float.Warning: Device do not support double dtype now, dtype cast repalce with float.Warning: Device do not support double dtype now, dtype cast repalce with float.
Warning: Device do not support double dtype now, dtype cast repalce with float.
Warning: Device do not support double dtype now, dtype cast repalce with float.
```

## 原因分析

transformers库的training\_args.py目前适配的是CUDA的部分操作，需要替换为适配NPU的脚本。

## 处理方法

training\_args.py替换为适配NPU的脚本，替换的脚本请见[training\\_args.py](#)。

## 6.2 训练业务昇腾迁移通用指导

### 6.2.1 简介

#### 场景介绍

本文旨在针对客户已有的PyTorch训练业务迁移到昇腾设备上运行，并获得较好的模型训练效果。华为云ModelArts针对该使用场景，在给出系统化训练业务昇腾迁移方案的基础上，提供了即开即用的云上集成开发环境，包含迁移所需要的算力资源和工具链，及具体的代码运行示例和最佳实践，并对于实际的操作原理和迁移流程进行说明，包含迁移后的精度和性能验证、调试方法说明。

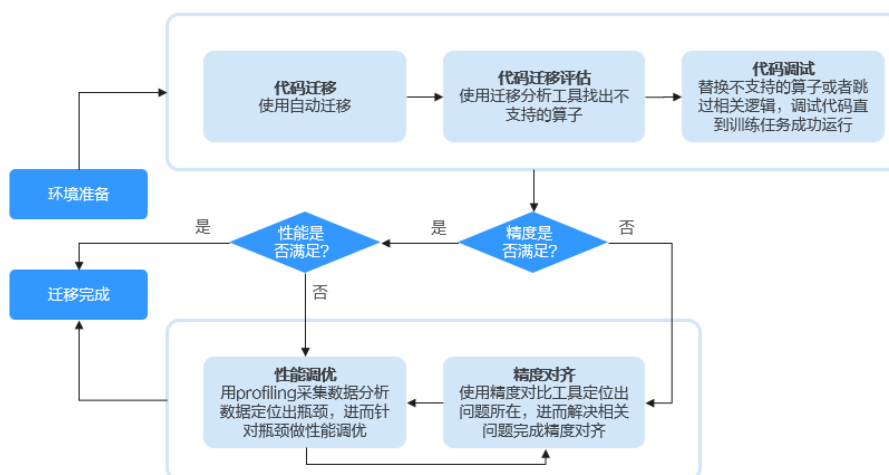
## 范围

本文涉及PyTorch训练的单卡、分布式业务迁移到昇腾的业务范围。

## 迁移流程

模型迁移主要指将开源社区中实现过的模型迁移到昇腾AI处理器上，需要保证模型已经在CPU/GPU上运行成功，迁移到昇腾AI处理器的主要流程如下所示。

图 6-32 迁移流程



### 6.2.2 昇腾迁移快速入门案例

请参考《LLM训练业务迁移指导》，该案例以ChatGLM-6B为例，介绍如何将模型迁移至昇腾设备上训练、模型精度对齐以及性能调优。

### 6.2.3 环境准备

本文以弹性裸金属作为开发环境，弹性裸金属支持深度自定义环境安装，可以方便的替换驱动、固件和上层开发包，具有root权限，结合配置指导、初始化工具及容器镜像可以快速搭建昇腾开发环境。

开通裸金属服务器资源请见[DevServer资源开通](#)，在裸金属服务器上搭建迁移环境请见[裸金属服务器环境配置指导](#)。

### 6.2.4 训练业务代码适配昇腾 PyTorch 代码适配

#### 前提条件

- 要迁移的训练任务代码在GPU上多次训练稳定可收敛。训练业务代码和数据，应该确保在GPU环境中能够运行，并且训练任务有稳定的收敛效果。
- 本文只针对基于PyTorch的训练脚本迁移。这里假设用户使用的是基于PyTorch的训练代码进行迁移。其他的AI引擎如TensorFlow、Caffe等不在本指导的讨论范围中。
- 已经完成环境准备（参考[环境准备](#)），并且代码、预训练模型、数据等训练必需内容已经上传到环境中。



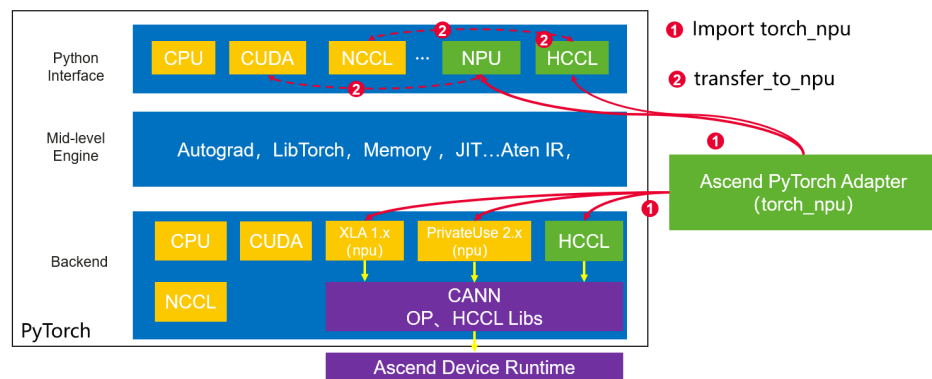
## 约束和限制

- 安装插件后，大部分能力能够对标在GPU上的使用，但是不是100%的行为和GPU上是一一对应的，比如在torch\_npu下，一个进程只能操作一张昇腾卡，而没有一个进程可以操作多卡的能力等。
- 基于PyTorch上的第三方开发库非常多，例如transformers、accelerate、deepspeed以及Megatron等，这些三方库昇腾也做了类似PyTorch Adapter的适配插件库，可以在Gitee的昇腾[官方仓库](#)中找到，请按需进行使用。

## 代码迁移基础知识

- PyTorch官方并不直接支持昇腾的后端，所以官方的版本无法直接利用昇腾设备完成训练加速。当前PyTorch直接支持的后端包括CUDA和AMD ROCm。
- PyTorch Adapter作为一个PyTorch“插件”，在已安装PyTorch的基础上安装后，支持在不改变PyTorch表达层的基础上，动态添加昇腾后端适配，包含增加了NPU设备、hccl等一系列能力的支持。安装后可以直接使用PyTorch的表达层来运行在NPU设备上。
- 当前提供了“一键迁移”脚本进行GPU到昇腾适配，原理是通过[monkey-patch](#)的方式将torch下的CUDA、nccl等操作映射为NPU和hccl对应的操作。如果没有用到GPU的高阶能力，例如自定义算子、直接操作GPU显存等操作，简单场景下可以直接使用“一键迁移”。

图 6-33 torch\_npu 工作原理示意图



- NPU ( Neural Network Processing Unit ) 和GPU在构造结构上存在差异，因此迁移过程并不是完全平替的关系。昇腾训练芯片属于NPU的范畴，虽然在表达层可以通过torch.cuda和torch.npu的形式来替代，但是真实的算子下发、显存管理、集合通信等，在进阶问题分析时需要了解NPU的运行机制，能够更好的使用NPU设备。

## 迁移操作步骤

**步骤1** 在训练任务启动Python脚本入口，初始化PyTorch Adapter ( torch\_npu )。

在torch\_npu安装后，该部分并没有直接植入到PyTorch中生效，其实是在显式的调用后，前端通过monkey-patch的方式注入到torch对象中，后端的注册了NPU设备，以及HCCL的参数面通信能力可以直接使用。

```
#torch npu初始化
import torch_npu
```

在执行对应的导入torch\_npu代码后，可以直接使用torch.npu相关接口和能力。

图 6-34 torch\_npu 导入

```
Python 3.7.10 | packaged by conda-forge | (default, Oct 13 2021, 22:05:51)
[GCC 9.4.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>> import torch
>>> torch.npu
Traceback (most recent call last):
 File "<stdin>", line 1, in <module>
AttributeError: module 'torch' has no attribute 'npu'
>>> import torch_npu
>>> torch.npu
<module 'torch_npu.npu' from '/home/ma-user/anaconda3/envs/PyTorch-1.11.0/lib/python3.7/site-packages/torch_npu/npu/_init_.py'>
>>>
```

步骤2 “一键迁移”完成GPU代码到昇腾的快速适配。

torch\_npu初始化后，原则上需要用户将原来代码中CUDA相关的内容适配到NPU相关的接口上，包含算子API、显存操作、数据集操作，以及分布式训练的参数面通信nccl适配到hccl上，手动操作修改点相对较为分散，可以通过transfer\_npu的模式来进行快速适配。

一键迁移的原理是，通过注入的方式将当前Python运行环境中，运行时的torch.cuda等需要适配的接口和操作都映射成为torch.npu对应的接口。所以理论上常见的场景下当前的代码不需要额外的适配就可以运行到昇腾设备上了。

```
#自动映射cuda API到npu的代码
from torch_npu.contrib import transfer_to_npu
```

图 6-35 一键迁移后 cuda 映射为 npu 相关的 API

```
Python 3.7.10 | packaged by conda-forge | (default, Oct 13 2021, 22:05:51)
[GCC 9.4.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>> import torch
>>> import torch_npu
>>> torch.cuda.is_available()
False
>>> from torch_npu.contrib import transfer_to_npu
/home/ma-user/anaconda3/envs/PyTorch-1.11.0/lib/python3.7/site-packages/torch_npu/contrib/transfer_to_npu.py:167: ImportWarning:

The torch.Tensor.cuda and torch.nn.Module.cuda are replaced with torch.Tensor.npu and torch.nn.Module.npu now..
The torch.cuda.DoubleTensor is replaced with torch.npu.FloatTensor cause the double type is not supported now..
The backend in torch.distributed.init_process_group set to hccl now..
The torch.cuda.* and torch.cuda.amp.* are replaced with torch.npu.* and torch.npu.amp.* now..
The device parameters have been replaced with npu in the function below:
torch.logspace, torch.randint, torch.hann_window, torch.rand, torch.full_like, torch.ones_like, torch.randperm, torch.arange, torch.
frombuffer, torch.normal, torch.empty_per_channel_affine_quantized, torch.empty_strided, torch.empty_like, torch.scalar_tensor, torch.tril_indices, torc
h.barlett_window, torch.ones, torch.sparse_coo_tensor, torch.randn, torch.kaiser_window, torch.tensor, torch.triu_indices, torch.as_tensor, torch.zeros,
torch.randint_like, torch.full, torch.eye, torch.sparse_csr_tensor_unsafe, torch.empty, torch.sparse_coo_tensor_unsafe, torch.blackman_window, torch.z
eros_like, torch.range, torch.sparse_csr_tensor, torch.randn_like, torch.from_file, torch.cudnn_init_dropout_state, torch.empty_affine_quantized, torch.
.linspace, torch.hamming_window, torch.empty_quantized, torch.pin_memory, torch.autocast, torch.Tensor.new_empty, torch.Tensor.new_empty_strided, torch.
Tensor.new_full, torch.Tensor.new_ones, torch.Tensor.new_tensor, torch.Tensor.new_zeros, torch.Tensor.to, torch.nn.Module.to, torch.nn.Module.to_empty

warnings.warn(msg, ImportWarning)
>>> torch.cuda.is_available()
True
>>> torch.npu.is_available()
True
```

以chatGLM-6b为示例，在使用一键迁移时，在开发环境中克隆对应的代码，假设数据和预训练权重已经配置好，可以直接在ptuning目录下，训练入口代码main.py中添加两行代码来完成昇腾运行适配，注意添加位置为导入torch之后。启动训练脚本可以观察运行效果。

图 6-36 chatGLM-6b pTuning 训练入口迁移

```
import logging
import os
import sys
import json

import numpy as np
from datasets import load_dataset
import jieba
from rouge_chinese import Rouge
from nltk.translate.bleu_score import sentence_bleu, SmoothingFunction
import torch

import transformers
from transformers import (
 AutoConfig,
 AutoModel,
 AutoTokenizer,
 DataCollatorForSeq2Seq,
 HFArgumentParser,
 Seq2SeqTrainingArguments,
 set_seed,
)

import logging
import os
import sys
import json

import numpy as np
from datasets import load_dataset
import jieba
from rouge_chinese import Rouge
from nltk.translate.bleu_score import sentence_bleu, SmoothingFunction
import torch
import torch_npu // 初始化torch_npu
from torch_npu.contrib import transfer_to_npu // 自动映射cuda等接口到npu

import transformers
from transformers import (
 AutoConfig,
 AutoModel,
 AutoTokenizer,
 DataCollatorForSeq2Seq,
 HFArgumentParser,
 Seq2SeqTrainingArguments,
 set_seed,
)
```

### 📖 说明

“一键迁移”脚本适合没有使用CUDA高阶能力的简单场景，如果涉及自定义算子、主动申请GPU显存等操作则需要额外自行适配。

### 步骤3 手动迁移。

手动迁移意味着需要将GPU相关的代码调用修改为NPU对应的接口，适配的内容包含但不局限于以下内容，可能会涉及到逐步的排错和适配。

- 迁移GPU相关从cuda API调用到npu的API。

迁移前：

```
model.cuda(args.gpu)
torch.cuda.set_device(args.gpu)
torch.cuda.is_available()
```

迁移后：

```
model.npu(args.gpu)
torch_npu.npu.set_device(args.gpu)
torch_npu.npu.is_available()
```

- 多卡多机场景下，迁移nccl相关调用到hccl。

迁移前：

```
dist.init_process_group(backend='nccl',init_method = "tcp://:127.0.0.1:**", ,rank = args.rank)
```

迁移后：

```
dist.init_process_group(backend='hccl',init_method = "tcp://:127.0.0.1:**", ,rank = args.rank)
```

### 📖 说明

手动迁移可以在一键迁移有问题后，以此为线索来进行逐个适配，或者对于代码实现比较了解的前提下，主动完成代码改造。

----结束

## 常见问题

1. 如何检测当前的torch\_npu是否正确安装？  
可以用如下的python命令在对应的运行环境中初步校验torch\_npu是否正常安装。  

```
python3 -c "import torch;import torch_npu;print(torch_npu.npu.is_available())"
```
2. torch\_npu使用报错看不懂怎么办？应该怎么求助？  
如果报错可以首先在昇腾社区的[常见问题](#)，以及Gitee的[PyTorch](#)社区中查看是否有类似的问题找到一些线索。如果还无法解决可以通过提交工单的形式从华为云ModelArts入口来进行咨询以及求助对应的专业服务。
3. “一键迁移”似乎还是要改很多脚本才能运行起来？  
因为一键迁移其实是对于torch运行环境中常用的GPU上的接口进行和昇腾设备相应的映射，原有的训练任务代码逻辑中例如数据集导入，预训练权重的内容，以及对应的环境的超参数等内容都需要在实际的昇腾环境中进行调整。

## 6.2.5 PyTorch 迁移精度调优

基于PyTorch Adapter完成代码迁移适配后，用户需要进一步验证精度是否达标。迁移过程精度偏差的来源，一方面是昇腾设备部分算子的实现和CUDA算子有差异，另一方面则是硬件方面的差异，如Ascend Snt9芯片上的Matmul和Conv等cube算子只支持FP16，可能会导致数值溢出，从而引起精度误差。此外，网络随机参数初始化差异以及典型场景（比如dropout和数据集shuffle等操作）都可能引入误差，所以迁移模型精度校验以及精度调优工作是至关重要的。

## 精度校验

迁移之后的精度校验工作是以CPU/GPU环境训练过程作为标杆的，这里的前提是在迁移前，模型已经在CPU/GPU环境达到预期训练结果。在此基础上，迁移过程的精度问题一般包括：

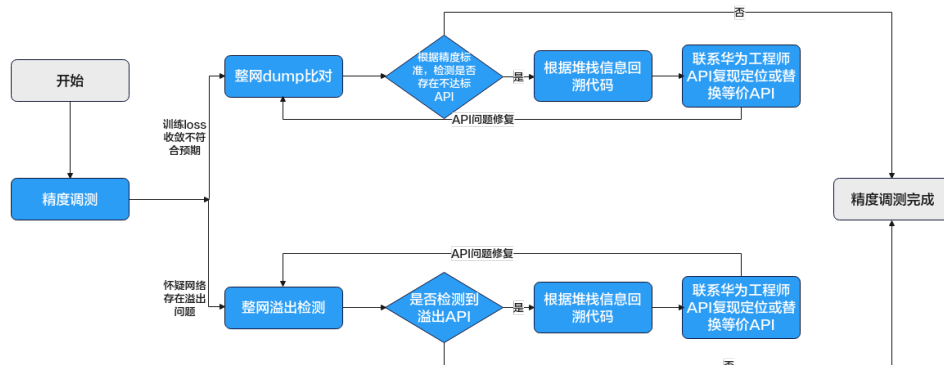
- loss曲线与CPU/GPU差异不符合预期。
- 验证准确度与CPU/GPU差异不符合预期。

在迁移到NPU环境下训练时发现以上问题时，说明精度存在偏差，需要进一步做精度调优。下文将分别阐述精度诊断的整体思路和借助工具如何进行精度问题的定位。

## 精度调优总体思路

一般场景的训练模型都是包括随机种子、数据集shffule、网络结构dropout等操作的，目的是在网络训练阶段引入一定的随机性使得训练结果更加具有鲁棒性。然而在精度诊断或者对齐阶段需要暂时关闭这些随机特性，使得需要对齐的标杆结果是确定唯一的。针对精度问题比较有效的诊断方法有整网dump和整网的溢出检测两种方式。下图是昇腾社区针对PyTorch训练迁移场景的精度调优流程示意图，请见[详情](#)。

图 6-37 精度调优流程



整网dump和溢出检测是通过在PyTorch模型中注入hook、dump模型训练过程的输入输出数据，比对NPU环境和标杆环境的所有输入输出发现异常信息。具体可以参见精度比对工具[ptdbg-ascend](#)。

精度调优的另一个角度可以从网络的单个API角度分析，通过提取模型中所有的API前反向信息，构造相应的API单元测试，将NPU输出与标杆比对，从而检测出精度有问题的API。具体参见精度预检工具[api\\_accuracy\\_checker](#)。

## 精度比对工具使用说明

ptdbg-ascend是昇腾开源的用于PyTorch框架迁移训练的精度对比工具。使用时需要两组模型运行环境，一组是基于昇腾AI芯片的NPU环境，另一组是CPU/GPU环境（标杆环境）。ptdbg-ascend通过在PyTorch训练脚本中插入dump接口，跟踪计算图中算子的前向传播与反向传播时的输入与输出，然后再compare将对结果写出到.csv表格中。

当前支持计算Cosine（余弦相似度）、MaxAbsErr（最大绝对误差）和MaxRelativeErr（最大相对误差）这三种评价指标，通过设定相似度阈值和最大绝对偏差限来判断API运行时是否存在精度问题。

### 步骤1 安装ptdbg\_ascend工具。

下载最新的whl包至服务器，并通过pip安装ptdbg\_ascend工具（[工具链接](#)）。

```
#shell
pip install ./ptdbg_ascend-3.1-py3-none-any.whl
```

### 步骤2 获取NPU和GPU的dump数据。

在单卡场景下，PyTorch训练脚本插入dump接口方式如下：

```
导入ptdbg_ascend依赖包
from ptdbg_ascend import register_hook, overflow_check, seed_all, set_dump_path, set_dump_switch,
acc_cmp_dump
在 main 函数中固定随机数
seed_all(seed=1234, mode=False)
设置 dump 文件保存路径
set_dump_path("./npu_dump", dump_tag='all')
添加hook函数和数据比对dump开关
register_hook(model, acc_cmp_dump)
dump 开启和关闭。在一个 iter 的开始和结束位置设置
set_dump_switch("ON", mode="api_stack", filter_switch="OFF")

iteration

set_dump_switch("OFF", mode="api_stack", filter_switch="OFF")、
```

以上给出的是dump整网精度数据的方式，在迁移过程中也会碰到数值溢出问题。在ptdbg中设置检查精度溢出方式如下：

```
dump 开启和关闭。在一个 iter 的开始和结束位置设置
register_hook(model, overflow_check, overflow_nums=3)
set_overflow_check_switch("ON")

iteration

set_overflow_check_switch("OFF")
```

这里的overflow\_sum用来控制溢出次数，表示多少次溢出时停止训练。

### 步骤3 生成精度对比表。

dump得到NPU和GPU数据之后，会得到保存api完整输入输出Tensor的“.npy”文件以及保存API简单统计信息的“.pkl”文件。在compare对比时，需要分别指定NPU和GPU的pkl文件路径和dump数据路径（具体参数请按实际路径填写），compare.py实现如下：

```
compare.py
from ptdbg_ascend import compare
dump_result_param= {
 "npu_pkl_path": "${dump_data_npu}/api_stack_dump.pkl",
 "bench_pkl_path": "${dump_data_gpu}/api_stack_dump.pkl",
 "npu_dump_data_dir": "${dump_data_npu}/api_stack_dump/",
 "bench_dump_data_dir": "${dump_data_npu}/api_stack_dump/",
 "is_print_compare_log": True
}
compare(dump_result_param, "./output", stack_mode=True)
```

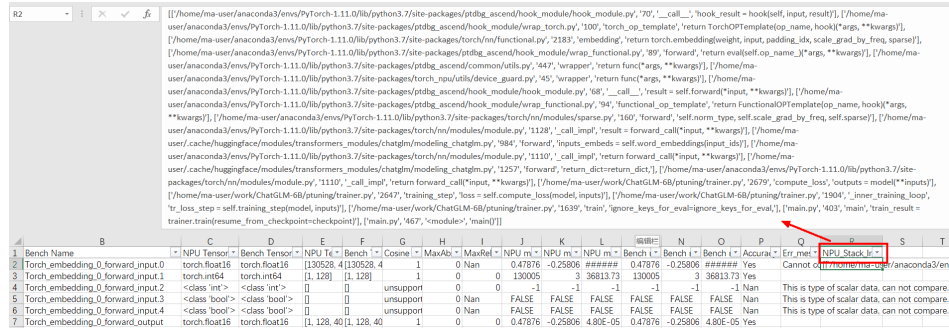
执行comapre.py对比之后会在output目录下输出compare\_result\_{timestamp}.csv文件。根据此文件，可以查看网络训练过程中各个API执行的输入输出以及评价指标的信息。

### 步骤4 根据堆栈信息定位代码差异点。

在compare对比表文件NPU\_Stack\_Info列，有各个算子在执行时的堆栈信息。如下图所示，列出的是NPU下Torch\_embedding\_0\_forward（代表torch的embedding算子在第0次执行forward阶段）的堆栈信息。



图 6-38 堆栈信息



部分情况下也需要查看GPU训练时的堆栈信息来排除GPU和NPU是否执行的不同逻辑代码。这种情况可以根据NPU Name在dump阶段生成的.pkl文件中查找。在ptdbg-ascend中，有支持使用API接口parse堆栈信息的方式，代码如下：

```
compare.py
from ptdbg_ascend import parse
parse("./dump_data /npu/rank0/api_stack_dump.pkl", "Torch_embedding_0_forward")
```

### 步骤5 精度对齐。

ptdbg-ascend当前支持的评判指标有Cosine、MaxAbsError（可参见[接口函数说明](#)）：

精度存在异常的情况包含以下三种情况：

- Cosine < 0.99且MaxAbsError > 0.001
- Cosine < 0.9
- MaxAbsError > 1

其余情况都视为达标。精度对齐时，需要根据compare表格查找精度不达标的算子进行调整优化。由于算子间可能存在前后数据传输的相关性，一般先定位第一个不达标的算子，然后结合堆栈信息进行分析和调整，调整之后重新训练dump数据再做对比，直至模型训练的loss曲线和在验证集上做测试的结果和GPU标杆结果一致为止。

----结束

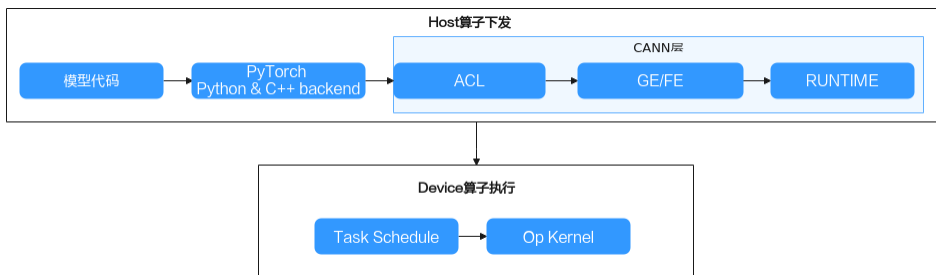
## 6.2.6 PyTorch 迁移性能调优

### 6.2.6.1 性能调优总体原则和思路

PyTorch在昇腾AI处理器的加速实现方式是以算子为粒度进行调用（OP-based），即通过Python与C++调用CANN层接口Ascend Computing Language（AscendCL）调用一个或几个亲和算子组合的形式，代替原有GPU的实现方式，具体逻辑模型参考[此处](#)。

在PyTorch模型迁移后进行训练的过程中，CPU只负责算子的下发，而NPU负责算子的执行，算子下发和执行异步发生，性能瓶颈在此过程中体现。在PyTorch的动态图机制下，算子被CPU逐个下发到NPU上执行。一方面，理想情况下CPU侧算子下发会明显比NPU侧算子执行更快，此时性能瓶颈主要集中在NPU侧；另一方面，理想情况下NPU侧算子计算流水线一直执行，不会出现NPU等待CPU算子下发即NPU空转的场景，如果存在，则CPU侧算子下发存在瓶颈。

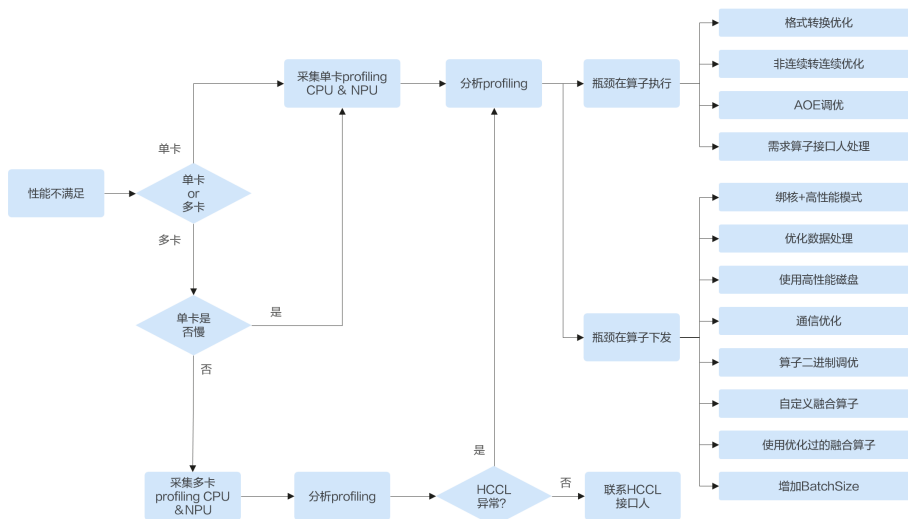
图 6-39 Host 算子下发和 Device 算子执行



综上所述，性能优化的总体原则为：减少Host算子下发时间、减少Device算子执行时间。

训练代码迁移完成后，如存在性能不达标的问题，可参考下图所示流程进行优化。建议按照单卡、单机多卡、多机多卡的流程逐步做性能调优。

图 6-40 性能调优总体思路



### 6.2.6.2 性能调优五板斧

性能调优相对来说门槛较高，对PyTorch以及昇腾AI处理器的理解越深刻，越能发挥昇腾AI处理器的计算能力，从而提高训练性能。一般情况下，通过对PyTorch代码做 profiling，从而基于数据分析，调整代码，尽可能发挥硬件能力，但在做 profiling 数据分析前，通常可简单地基于性能优化五板斧先尝试做性能调优：

- **NPU亲和API以及亲和优化器替换**
- **算子二进制调优**
- **AOE自动性能调优**
- **多进程绑核**
- **优化数据处理**

#### NPU 亲和 API 以及亲和优化器替换

可对训练代码中的部分API替换成NPU亲和API、亲和优化器或者NPU自定义算子，能够提升训练性能，但需要注意的是，在一些场景下，替换后的算子可能会对模型精度

有影响，所以适配后，需要验证精度，如果确认有影响，需要在精度和性能之间做取舍。

- **NPU亲和API替换**

可使用pytorch\_analyse.sh工具扫描训练代码中的NPU亲和API，NPU亲和API适配昇腾AI处理器，性能更优。具体用法详见[此处](#)。示例如下：

```
./pytorch_analyse.sh -i $HOME/chatglm-6b/ -o $HOME/result/ -v 1.11.0 -m affinity_apis
```

#### 📖 说明

- 当前适配的NPU亲和API请见[此处](#)。
  - “/usr/local/Ascend/ascend-toolkit/latest/tools/ms\_fmkt\_transplt/pytorch\_analyse.sh”为默认路径。
  - pytorch\_analyse.sh只能扫描指定目录下的.py文件，所以如果代码中引入了其他目录或者第三方库的代码，需要对其他目录或者第三方库的代码也做同样的扫描，并基于扫描结果对相应代码做API替换。
- **NPU亲和优化器替换**
- PyTorch原生优化器在训练过程中，一般需要下发多个NPU算子完成梯度和参数的更新计算，过多的算子下发，可能造成NPU空等。可将PyTorch优化器替换成NPU亲和优化器提高训练性能，详情请见[此处](#)。
  - **NPU亲和API替换**

NPU亲和API替换优化相对较难，需要对正在训练的模型架构有比较深入的理解，在此基础上，可尝试对代码中的部分操作通过NPU自定义算子做等价替换，NPU自定义算子列表详见[这里](#)。NPU自定义算子对一些常见的算子组合基于NPU进行了算子融合，训练迁移过程中可有意识地对训练代码中的实现用这些自定义算子替换。

例如激活函数gelu的常见实现如下：

```
def gelu_impl(x):
 return 0.5 * x * (1.0 + torch.tanh(0.7978845608028654 * x * (1.0 + 0.044715 * x * x)))
```

可通过NPU自定义算子torch\_npu.fast\_gelu替换提高训练性能。

## 算子二进制调优

PyTorch Adaptor框架提供与算子编译相关的二进制配置参数，可设置模型编译时是否优先在线编译，以此优化模型训练性能。在main函数训练逻辑开始前通过以下函数设置（True为启动优先在线编译、False为取消优先在线编译）。

```
torch_npu.npu.set_compile_mode(jit_compile=False)
```

对于固定shape场景和动态shape场景，是否优先在线编译对训练性能带来不同的效果：

- **固定shape场景**：固定shape是指在模型计算过程中，模型的输入和输出的shape是固定的。如果优先在线编译，可根据当前获得的算子信息，进行融合和优化，在线编译出运行性能更优的算子。反之，则编译优化少，性能降低。
- **动态shape场景**：动态shape是指在模型计算过程中，模型的输入和输出存在多种shape。如果对动态shape的算子优先编译，会导致编译时间长训练性能差。如果取消优先编译，会优先查找当前编译好的算子二进制配置文件，如果存在则不在线编译算子；如果不存在，再进行在线编译。此时虽然编译优化少，但是没有编译时间，模型训练性能大概率比配置为优先编译高。

总结：



- 如果模型中无动态shape，启动优先在线编译，可提高训练性能。
- 如果模型中只有动态shape（该情况较少），关闭优先在线编译，模型训练性能大概率会更高。
- 既有动态shape也有固定shape，启动优先在线编译对训练性能是否提升无法确定，因此可以在调整训练代码后，分别尝试开关优先在线编译后根据训练性能的优劣再设置。

#### 📖 说明

- Snt9B芯片默认关闭了优先在线编译，可通过以下命令获取当前模式。如果返回为False，代表已启动优先在线编译。

```
print(torch_npu.npu.is_jit_compile_false())
```
- 算子会根据该开关走不同的代码逻辑，如出现jit\_compile切换后，代码运行失败的情况，需要联系昇腾技术支持获取帮助。

## AOE 自动性能调优

AOE（Ascend Optimization Engine）是一款自动调优工具，当训练模型全部为固定shape时，可选择AOE调优，具体操作参见[此处](#)。该优化会进行算子融合，将融合得到的图进行算子粒度切分，针对每一个融合算子子图生成不同的算子调优策略，从而实现最优的算子性能，并将得到的最优策略保存在算子知识库。性能调优期间只要做了代码修改后，可尝试运行AOE自动性能调优。

## 多进程绑核

相比于x86服务器，ARM服务器通常CPU核数更多，但单核性能更弱，因此更容易触发内核的负载均衡策略，该策略是通过启用进程迁移来降低繁忙的处理器压力。进程迁移会导致进程上下文切换、降低Cache命中率和跨numa内存访问等，从而影响训练性能。

如果使用docker容器作为训练环境，启动容器的时候，通过cpuset-cpus参数指定当前容器绑定的cpu核（如绑定16个cpu核60~75，命令示例为“docker run -d --cpuset-cpus=60-75 myimage bash”），这样容器中的进程只能在指定的CPU核上运行，达到绑核的效果。

## 优化数据处理

训练性能依赖训练数据是否及时准备好让NPU进行计算，因此需要尽量减少NPU等待数据准备的概率，主要优化方法包括：[使用高性能图像预处理工具如opencv](#)、[加速数据下沉到NPU设备](#)、[数据预取与数据计算并行](#)、[减少NPU与CPU数据交互](#)等。

### 6.2.6.3 训练 profiling 工具使用

五板斧操作之后，如果性能仍然不满足要求，便需要通过profiling工具采集性能数据，基于数据分析是哪个环节、哪个算子导致的性能消耗，进而做性能优化。

目前有两种方式采集训练profiling数据：[Ascend PyTorch Profiler数据采集与分析](#)和[E2E Profiling数据采集与分析](#)。

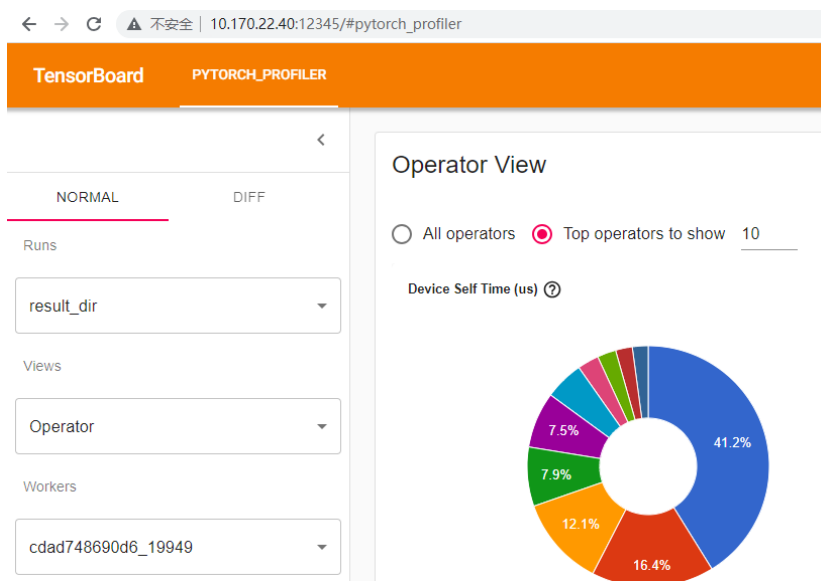
其中推荐使用Ascend PyTorch Profiler数据采集与分析方法，基于这种用法性能调优更高效，可以全面采集PyTorch训练场景下的性能数据，主要包括PyTorch层算子信息、CANN层算子信息、底层NPU算子信息、以及算子内存占用信息等，可以全方位分析PyTorch训练时的性能状态，有四种视图来展示PyTorch性能数据，其中Trace视图与第二种profiling方法展示同样的信息。第二种采集方式的优势主要在于不需要额外启动tensorboard服务来展示数据，在本地浏览器就能展示性能数据。

训练profiling工具使用说明：

- 通过键盘上的快捷键（w：放大/s：缩小/a：左移/d：右移）可以很方便地进行查看算子运行信息（tensorboard的Trace View页面和chrome的tracing页面都支持快捷键）。
- 如果是在docker中运行tensorboard，启动docker容器的时候，需要将tensorboard的端口映射到宿主机的端口，这样才能在浏览器基于宿主机的ip+宿主机的端口访问tensorboard服务；同时启动tensorboard的时候，需要“—bind\_all”参数。

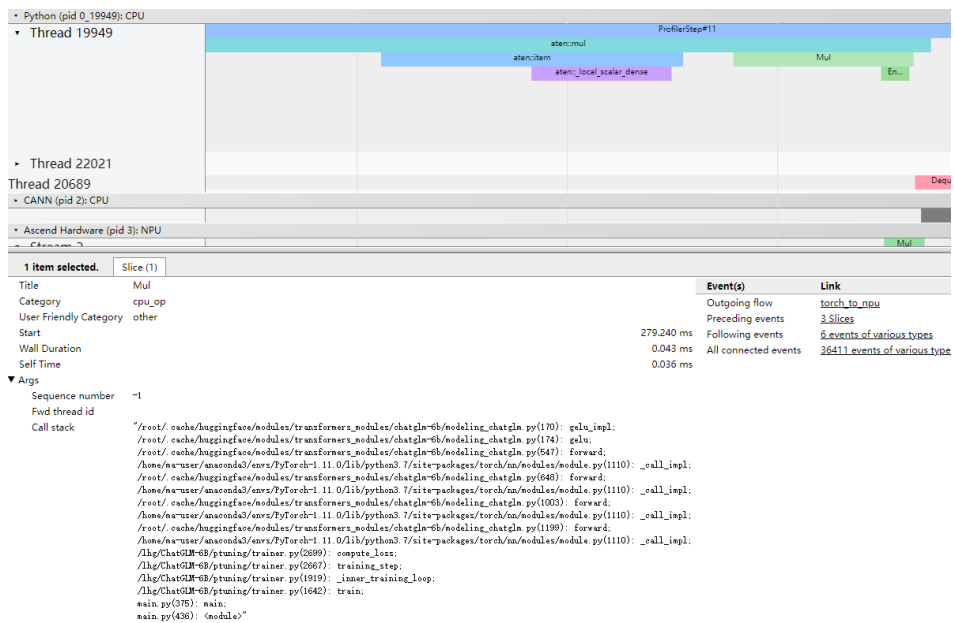
```
docker run -itd -p 12345:6006 my-image bash
....
tensorboard --bind_all --logdir result_dir/
```

图 6-41 TensorBoard



- 性能调优是一个不断迭代的过程，每个版本的代码与profiling的对应关系需要提前做好规划，否则随着迭代次数的增多，无法梳理清楚某一版本的代码修改究竟是否带来性能提升或带来多少性能提升。推荐对应关系可以使用git commit来管理。
- PyTorch API会调用其他API以及算子，调用关系在Trace View的Python cpu区域可以展示出来，如下图所示，tensor对象的\*或者mul操作（对应图中的aten::mul）会调用aten::item和Mul算子，以此类推。其中如果某一个算子调用了Enqueue算子，代表该算子将会被下发到NPU中执行。鼠标点中某个算子/API，可查看对应详情，包括调用堆栈。

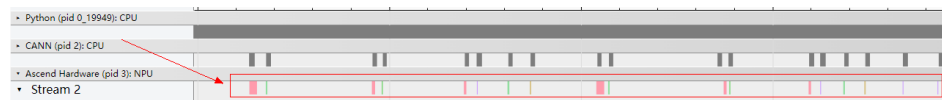
图 6-42 调用关系



### 6.2.6.4 优化算子下发

当发现NPU上有大量相邻算子之间有`时间间隙`出现时，代表算子下发的速度太慢导致NPU空等，NPU算力没有充分发挥，如下图所示。

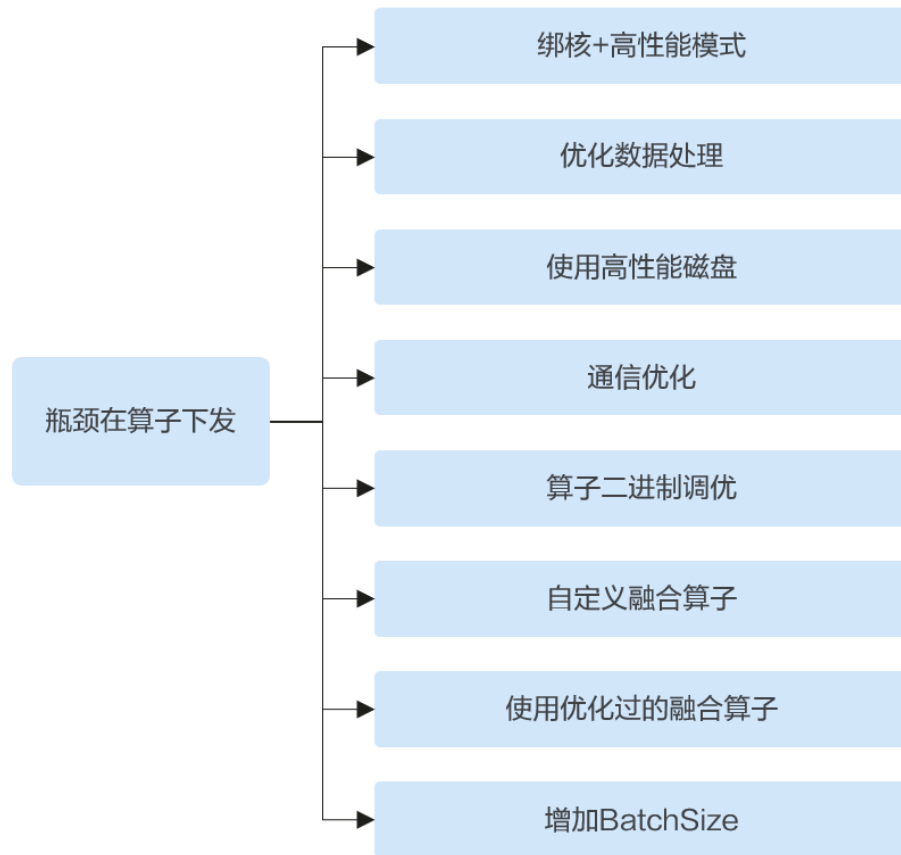
图 6-43 算子之间的时间间隙



优化该场景有三个思路：

- 加速算子下发。常用的优化方法有进程绑核（详见[性能调优五板斧](#)）、启用机器的cpu高性能模式、[启用机器的cpu高性能模式](#)、使用高性能磁盘、多级多卡训练场景下通信优化等。
- 融合多个算子的逻辑为单算子，从而减少算子下发的数量。常用的优化方法为使用Ascend自带的优化后的融合算子、算子二进制优化（详见[性能调优五板斧](#)）或者开发者自己开发自定义融合算子[自定义融合算子](#)。此外，PyTorch同语义代码的执行时间有差异，可基于对同语义代码进行Profiling分析，使用性能好的实现，比如“`tensorA[:, None, :, :]`”与“`tensorA.unsqueeze(1)`”为同语义，但是前者会调用3次“`aten::slice`”接口加一次“`aten::unsqueeze`”接口，后者只调用一次“`aten::unsqueeze`”接口，所以应该选择“`tensorA.unsqueeze(1)`”。
- 让NPU上运行的算子处理更多的数据，算子执行时间变长，单算子下发时间几乎不变，掩盖了算子下发慢的问题。常用的方法是尽可能地增大batch size，让每一个step的NPU计算量增加。

图 6-44 优化思路

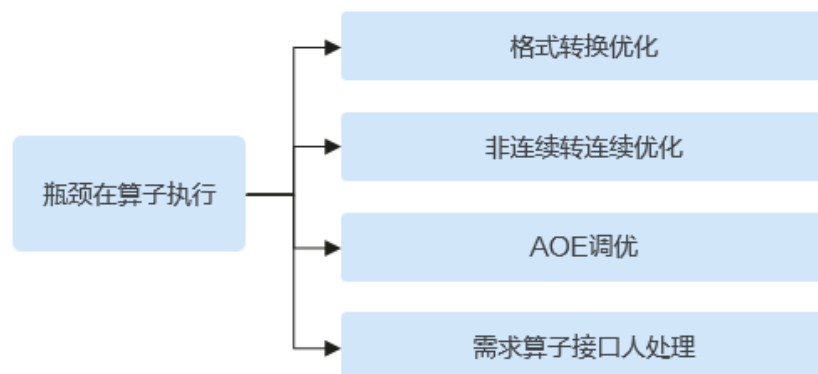


### 6.2.6.5 优化算子执行

优化算子执行有两个思路：

- 减少不必要的算子执行。比如减少不必要的格式转换算子和存储转连续算子。
- 加速慢算子的执行速度。遇到此类问题，尝试基于AOE调优（详见[性能调优五板斧](#)）或者联系华为工程师分析处理。

图 6-45 优化思路

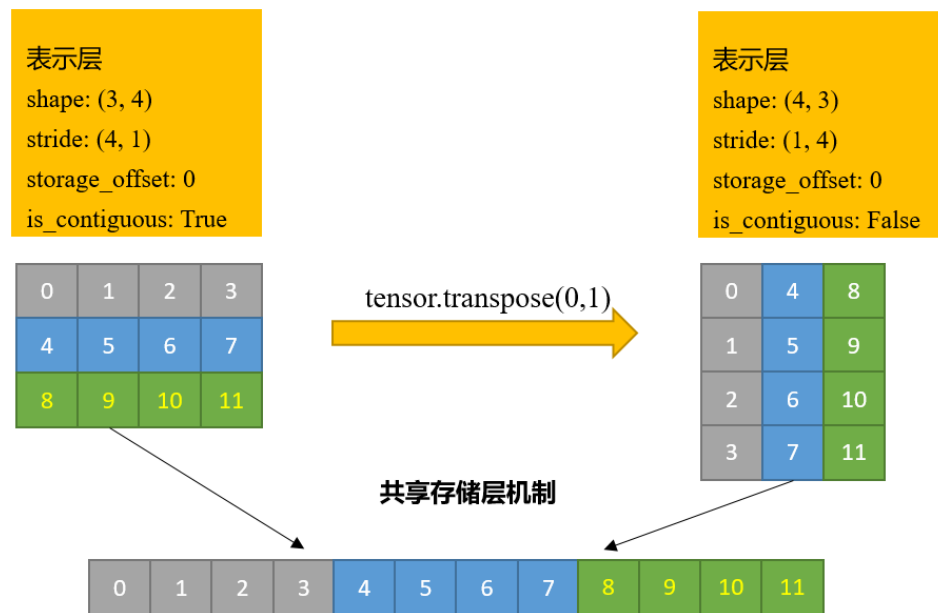


## 减少不必要的算子执行

- 减少不必要的存储转连续算子

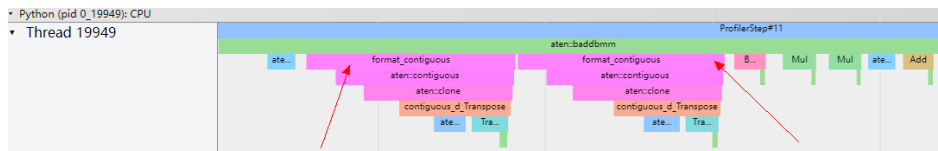
PyTorch的tensor对象由表示层和存储层（Storage）构成，表示层主要包含tensor的形状、步长、类型和是否连续等信息，存储层为连续内存的一维数组。对tensor的维度进行转换的操作（如transpose、permute等）后，转换前和转换后的两个tensor的表示层不同，但存储层相同，如下图所示。

图 6-46 表示层和存储层



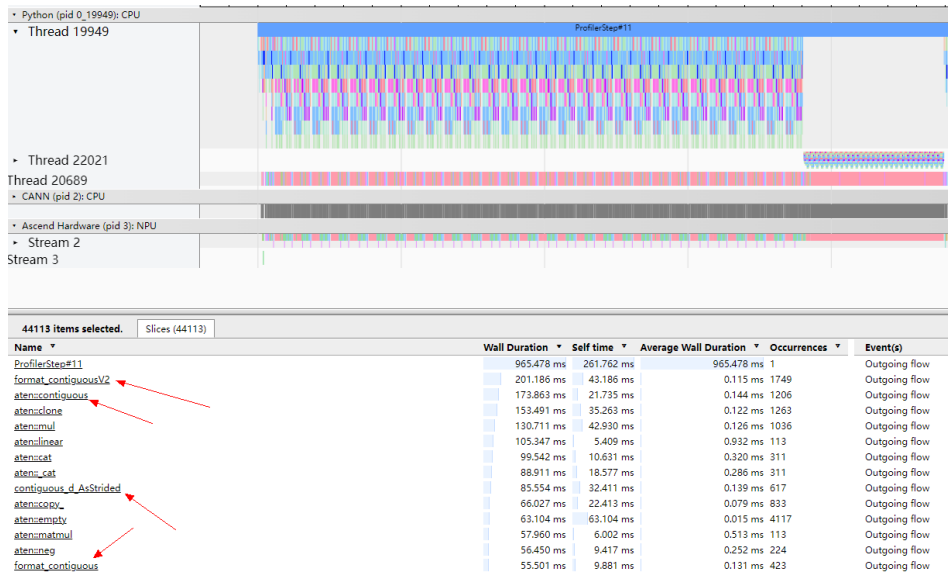
所以，会存在数学上相邻的元素在内存上不再连续排布的tensor。NPU的硬件工作机制要求所有的NPU算子只处理内存连续的tensor，为满足这一硬件限制，下发NPU算子前，PyTorch Adaptor的API会调用format\_contiguousV2 API，format\_contiguousV2会检测输入的tensor是否内存连续，如果不连续，会下发相关NPU算子完成新内存申请与数据copy保证输入tensor内存连续。开发者也可主动调用tensor的contiguous()方法提前完成这一操作，这样返回的就是内存连续的tensor。转存储连续操作涉及到内存申请以及写入，会导致NPU等待内存数据完成，而相对NPU执行速度来说，内存操作是比较慢的，因此应该尽量减少转存储连续操作。

图 6-47 format\_contiguous



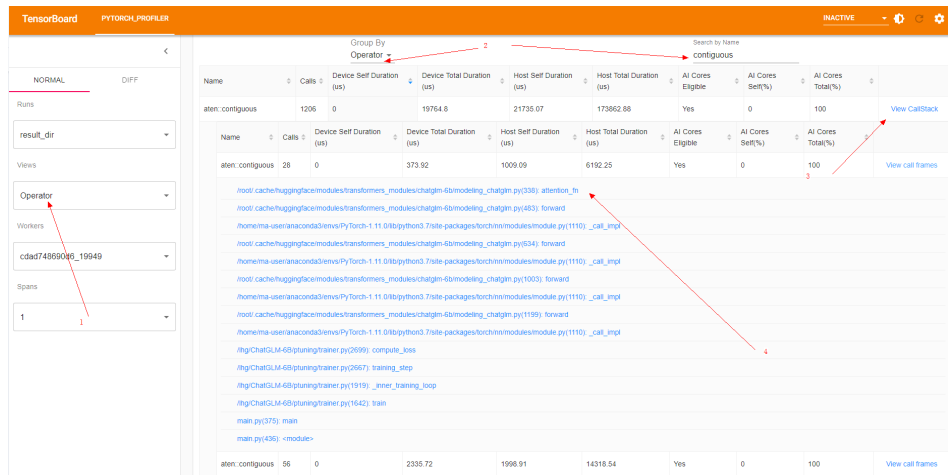
首先，统计一个step内的CPU profiling信息，查看是否有大量contiguous字样的API调用（如format\_contiguous、aten::contiguous等。特别需要强调：不需要关注format\_contiguousV2，format\_contiguousV2只有调用了aten::contiguous才代表对应tensor做了内存转连续操作）。

图 6-48 CPU profiling 信息



然后，切换到Operator视图，基于Operator分组，搜索contiguous关键字，进而从每一个调用栈信息定位到代码，逐个排查是否可以减少存储转连续算子的下发。

图 6-49 Operator 视图



可以通过如下几种优化策略尝试减少存储转连续算子的下发：

- 如果存在对同一tensor的多次非连续操作，则可通过优先将其转连续以避免多次转换。如下图，因为box1和box2进行转置后存储不连续，后续每一行代码都会触发4次转存储操作（4行代码总共触发16次），修改后，总共触发两次转存储操作。

修改前：

```

box1 = box1.transpose(0, 1)
box2 = box2.transpose(0, 1)
b1_x1, b1_x2 = box1[0] - box1[2] / 2, box1[0] + box1[2] / 2
b1_y1, b1_y2 = box1[1] - box1[3] / 2, box1[1] + box1[3] / 2
b2_x1, b2_x2 = box2[0] - box2[2] / 2, box2[0] + box2[2] / 2
b2_y1, b2_y2 = box2[1] - box2[3] / 2, box2[1] + box2[3] / 2

```

修改后：

```
box1 = box1.transpose(0, 1).contiguous()
box2 = box2.transpose(0, 1).contiguous()
b1_x1, b1_x2 = box1[0] - box1[2] / 2, box1[0] + box1[2] / 2
b1_y1, b1_y2 = box1[1] - box1[3] / 2, box1[1] + box1[3] / 2
b2_x1, b2_x2 = box2[0] - box2[2] / 2, box2[0] + box2[2] / 2
b2_y1, b2_y2 = box2[1] - box2[3] / 2, box2[1] + box2[3] / 2
```

- 使用计算类算子代替维度变换的View类算子。如下所示使用“index\_select”代替“torch.transpose(x, 1, 2).contiguous”。

原始channel\_shuffle操作:

```
def channel_shuffle(x, groups):
 # type: (torch.Tensor, int) -> torch.Tensor
 batchsize, num_channels, height, width = x.data.size()
 channels_per_group = num_channels // groups # reshape
 x = x.view(batchsize, groups,
 channels_per_group, height, width)
 x = torch.transpose(x, 1, 2).contiguous()
 # flatten
 x = x.view(batchsize, -1, height, width)
 return x
```

同等语义修改:

```
def channel_shuffle_index_select(x, groups=2):
 N, C, H, W = x.shape
 inp = C
 # channel_shuffle操作是对C维按一定规则的重排的工作，可以被表达为一次简单的重排
 group_len = inp // groups
 index = torch.from_numpy(np.array(list(range(inp))).reshape(groups, group_len).transpose(1,
0).flatten()).long()
 x = x.index_select(1, index)
 return x
```

- 涉及到非0轴的slice操作，尝试先做permute操作将对应轴改变到0轴后调用。contiguous()方法后，再做slice操作。背后的原理是：tensor的存储机制使得存储连续的tensor对象的0维slice的结果也是存储连续的。

举例如下，修改前需要做两次存储转连续操作，修改后只需一次存储转连续操作。

修改前:

```
position_ids, block_position_ids = position_ids[:, 0, :].transpose(0, 1).contiguous(), \
position_ids[:, 1, :].transpose(0, 1).contiguous()
```

修改后:

```
position_ids_t = position_ids.permute(1, 2, 0).contiguous()
position_ids, block_position_ids = position_ids_t[0, :, :], position_ids_t[1, :, :]
```

- Transpose+reshape操作使用自定义融合算子 torch\_npu.npu\_confusion\_transpose 替换，使用例子如下。

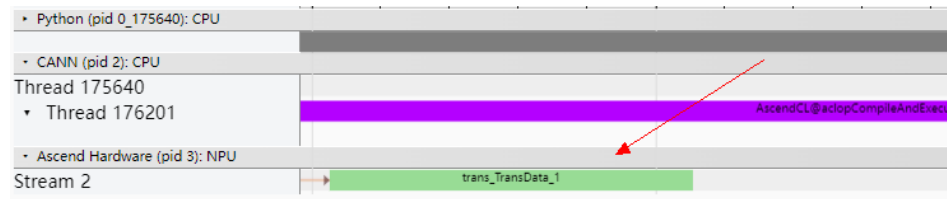
```
>>> x = torch.arange(24).reshape(2,3,4).npu()
>>> x
tensor([[[0, 1, 2, 3],
 [4, 5, 6, 7],
 [8, 9, 10, 11]],
 [[12, 13, 14, 15],
 [16, 17, 18, 19],
 [20, 21, 22, 23]]], device='npu:0')
>>> y = torch_npu.npu_confusion_transpose(x, (0,2,1), (2,2,6), True)
>>> y
tensor([[[0, 4, 8, 1, 5, 9],
 [2, 6, 10, 3, 7, 11]],
 [[12, 16, 20, 13, 17, 21],
 [14, 18, 22, 15, 19, 23]]], device='npu:0')
>>> x.shape
torch.Size([2, 3, 4])
>>> y.shape
torch.Size([2, 2, 6])
```



● 减少不必要的格式转换算子

关于数据排布格式，NPU在NCHW基础格式上，定义了众多与硬件强相关的私有格式，用于加速硬件计算，NPU对于不同的计算单元（cube、vector）所使用的默认私有格式不一致，导致在数据在不同的计算单元下流通时需要进行格式转化。此外，基础格式到NPU私有格式也需要进行格式转换，ACL编译期间根据算子的参数格式定义和当前输入的数据格式来决定是否向NPU侧下发格式转换的算子TransData。

图 6-50 算子 TransData

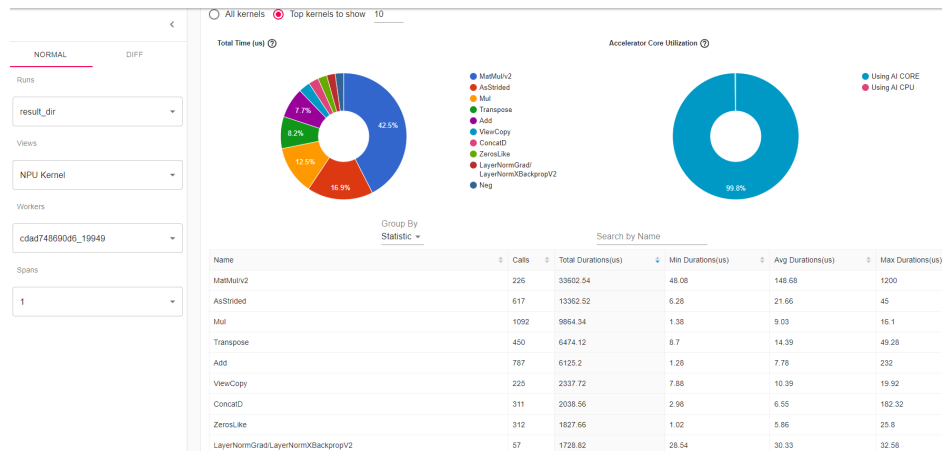


更多信息详见[此处](#)，算子的定义见[此处](#)，可以查看CANN算子参数的数据格式定义。可以通过tensor的“`npu_format_cast(format_type)`”方法进行tensor的格式转换以适配算子。

### 加速慢算子的执行速度

首先需要寻找执行速度比较慢的NPU算子列表，Kernel视图包含在NPU上执行的所有算子的信息，主要用于确认高耗时算子。

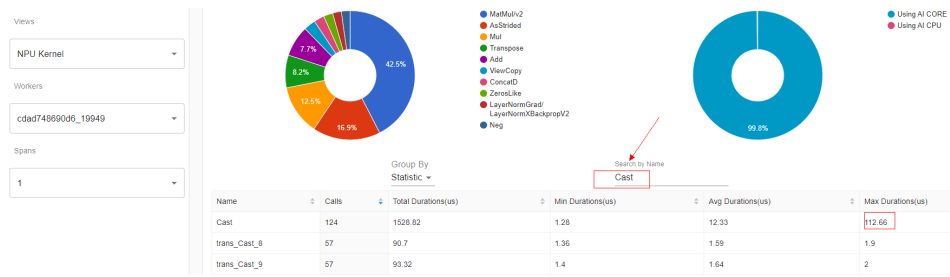
图 6-51 Kernel 视图



推荐基于以下思路尝试优化：

1. 搜索Cast类算子，查看是否Cast类算子最大耗时超过30us或者总耗时占比超过1%，如果超过，需尝试启动混合精度训练，详见[此处](#)。

图 6-52 Cast 类算子



2. 基于Accelerator Core排序，统计AI\_CPU算子，如果有AI\_CPU类算子执行时长超过1000us或者AI\_CPU类算子总执行时长占比超过10%，可尝试修改代码替换API\_CPU算子。

需要注意：PyTorch Adaptor针对部分算子，会基于输入类型下发不同运行硬件的算子，所以除了使用同语义算子替换API\_CPU算子外，还可以通过修改输入类型使算子下发到API\_CORE上（比如torch.topk在参数为一维list使用API\_CPU计算，多维参数则基于AI\_CORE Vector计算）。

图 6-53 Accelerator Core 排序

| Name      | Type      | Accelerator Core | Start Time(us)    | Duration(us) | Wait Time(us) | Block Dim | Mix Block Dim | Input Shapes | Input Data Types | Input Formats       | Output Shapes | Output Data Types | Output Formats      |
|-----------|-----------|------------------|-------------------|--------------|---------------|-----------|---------------|--------------|------------------|---------------------|---------------|-------------------|---------------------|
| TopKV2    | TopKV2    | MIX_AIV          | 22719379.940651   | 35.32        | 494.34        | 48        | 0             | "50,40,30;1" | FLOAT,INT32      | FORMAT_ND,FORMAT_ND | "50,40,20"    | FLOAT,INT32       | FORMAT_ND,FORMAT_ND |
| TopKV2    | TopKV2    | MIX_AIV          | 22719383.377831   | 37.02        | 87.24         | 48        | 0             | "50,40,30;1" | FLOAT,INT32      | FORMAT_ND,FORMAT_ND | "50,40,20"    | FLOAT,INT32       | FORMAT_ND,FORMAT_ND |
| TopKV2    | TopK      | AI_CPU           | 22719381.027431   | 404.06       | 515.92        | 0         | 0             | "10000;1"    | INT64,INT32      | FORMAT_ND,FORMAT_ND | "20;20"       | INT64,INT32       | FORMAT_ND,FORMAT_ND |
| TopKV2    | TopK      | AI_CPU           | 22719383.779531   | 383.94       | 299.82        | 0         | 0             | "10000;1"    | INT64,INT32      | FORMAT_ND,FORMAT_ND | "20;20"       | INT64,INT32       | FORMAT_ND,FORMAT_ND |
| Transpose | Transpose | AI_CORE          | 22719379.422291   | 24.02        | 0             | 48        | 0             | "50,30,40;3" | FLOAT,INT64      | FORMAT_ND,FORMAT_ND | "50,40,30"    | FLOAT             | FORMAT_ND           |
| Transpose | Transpose | AI_CORE          | 22719379.99753099 | 28.64        | 21.56         | 48        | 0             | "50,40,20;3" | FLOAT,INT64      | FORMAT_ND,FORMAT_ND | "50,20,40"    | FLOAT             | FORMAT_ND           |

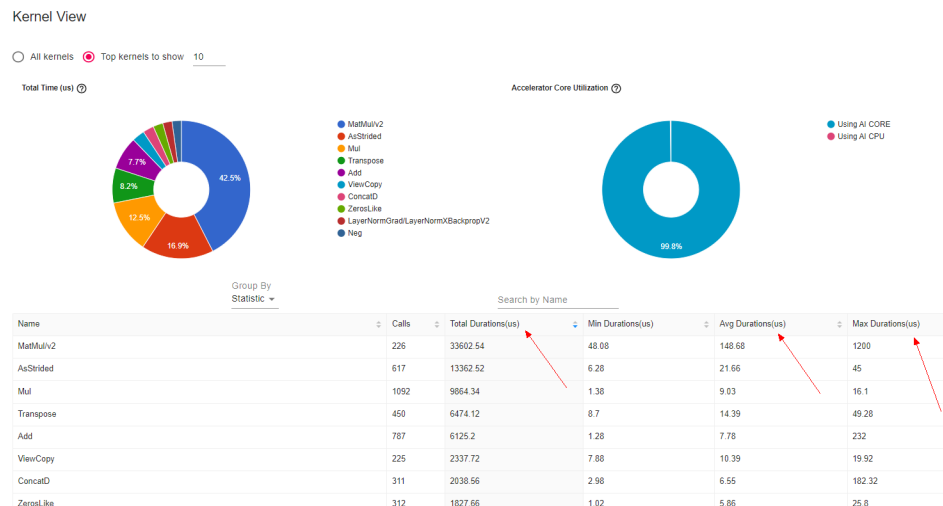
3. 如果遇到算子运行期间NPU的计算单元和存储单元使用率都未达到80%（查看aiv\_\*\_ratio和aic\_\*\_ratio是否达到0.8），或者算子的“Block Dim”小于AI Core/Vector Core，可尝试使用AOE算子调优，提高NPU硬件资源利用率。

图 6-54 aiv\_\*\_ratio

| aiv_vec_ratio | aiv_scalar_time(us) | aiv_scalar_ratio | aiv_mte2_time(us) | aiv_mte2_ratio | aiv_mte3_time(us) | aiv_mte3_ratio |
|---------------|---------------------|------------------|-------------------|----------------|-------------------|----------------|
| 0.2399        | 24.7964             | 0.7606           | 4.4083            | 0.1352         | 1.403             | 0.043          |
| 0.2352        | 25.1579             | 0.7564           | 4.7729            | 0.1435         | 1.367             | 0.0411         |
| N/A           | N/A                 | N/A              | N/A               | N/A            | N/A               | N/A            |
| N/A           | N/A                 | N/A              | N/A               | N/A            | N/A               | N/A            |
| 0.0531        | 5.2091              | 0.2886           | 4.1902            | 0.2321         | 2.0879            | 0.1157         |

- 针对总耗时最长、平均执行耗时最长以及最大耗时的三种排序的TOP算子，可联系华为工程师获得帮助。

图 6-55 耗时排序



## 6.2.7 训练网络迁移总结

- 确保算法在GPU训练时，持续稳定可收敛。避免在迁移过程中排查可能的算法问题，并且要有好的对比标杆。如果是NPU上全新开发的网络参考**PyTorch迁移精度调优**，排查溢出和精度问题。
- 理解GPU和NPU的构造以及运行的差别，有助于在迁移过程中问题分析与发挥NPU的能力。由于构造和运行机制的差别，整个迁移过程并非是完全平替，GPU在灵活性上是有其独特的优势的，而NPU上的执行目前还是依赖于算子的下发，对于NPU构造的理解是昇腾训练迁移中必备的知识，只有对于昇腾有基础理解，配合一些诊断工具，面对复杂问题时，才能进行进一步诊断与定位，进而发挥NPU的能力。
- 性能调优可以先将重点放在NPU不亲和的问题处理上，确保一些已知的性能问题和优化方法得到较好的应用。通用的训练任务调优、参数调优可以通过可观测数据来进行分析与优化，一般来说分段对比GPU的运行性能会有比较好的参考。算子级的调优某些情况下如果是明显的瓶颈或者性能攻坚阶段，考虑到门槛较高，可以联系华为工程师获得帮助。
- 精度诊断过程当前确实门槛较高，一般还是需要GPU上充分稳定的网络（包含混合精度）再到NPU上排查精度问题。常见的精度调测手段，包含使用全精度FP32，或者关闭算子融合开关等，先进行排查。对于精度问题，系统工程人员需要对算法原理有一定的理解，仅从工程角度分析有时候会非常受限，同时也可联系华为工程师进行诊断与优化。

## 6.2.8 常见问题

如果在PyTorch昇腾迁移过程中遇到问题，可以参考昇腾文档的**FAQ**。

## 6.3 AIGC 推理业务昇腾迁移指导

### 6.3.1 场景介绍

阅读本文前建议您先了解以下内容：

- Stable Diffusion的基础知识，可参考[Stable Diffusion github](#)、[Stable Diffusion wikipedia](#)、[diffusers github](#)、[Stable Diffusion with diffusers](#)
- 推理业务迁移到昇腾的通用流程，可参考[推理业务迁移通用指导](#)。

#### 📖 说明

由于Huggingface网站的限制，访问Stable Diffusion链接时需使用代理服务器，否则可能无法访问网站。

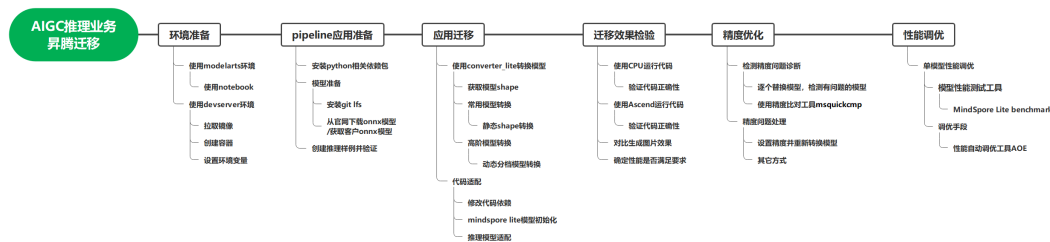
在Stable Diffusion迁移适配时，更多的时候是在适配Diffusers和Stable Diffusion WebUI，使其能够在昇腾的设备上运行。其中，Diffusers遵循了Huggingface的“**single-file policy**”的设计原则，它的三个主要模块Pipeline、Schedulers和预训练模型中，Pipeline和Schedulers都完全遵循了“single-file policy”原则。该设计原则更推荐复制粘贴代码而不是做抽象，因此所有和这个模型前向运算相关的源代码都被复制粘贴进同一个文件中，而不是调用某些抽象提取出的模块化的库，Diffusers的这种设计原则的好处是代码简单易用、对代码贡献者友好，但也有明显的缺点，因为这种反软件结构化的设计，导致对于昇腾适配来说比较复杂，因为没有统一的模块化的库可以适配，只能针对每个不同业务的Pipeline进行单独适配。本文以[Stable Diffusion v1.5](#)的图生图为例，通过可以直接执行的样例代码介绍Diffusers的昇腾迁移过程，其他的pipeline迁移可以在基于对pipeline的代码充分理解的基础上，参考本文的思路进行举一反三。Stable Diffusion WebUI的迁移不包含在本文中，具体原因详见[Stable Diffusion WebUI如何适配?](#)。

AI推理应用运行在昇腾设备上一般有两种方式：

- 方式1：通过Ascend PyTorch，后端执行推理，又称在线推理。
- 方式2：通过模型静态转换后，执行推理，又称离线推理。

通常为了获取更好的推理性能，推荐使用方式2的离线推理。下文将以Diffusers img2img onnx pipeline为示例来讲解如何进行离线推理模式下的昇腾迁移。迁移的整体流程如下图所示：

图 6-56 迁移流程图



### 6.3.2 迁移环境准备

迁移环境准备有以下两种方式：

- 方式一 ModelArts Notebook：该环境为在线调试环境，主要面向演示、体验和快速原型调试场景。
  - 优点：可快速、低成本地搭建环境，使用标准化容器镜像，官方notebook示例可直接运行。

- 缺点：由于是容器化环境因此不如裸机方式灵活，例如不支持root权限操作、驱动更新等。
- 环境开通指导参考：[Notebook环境创建](#)。
- 样例演示可参考[Notebook样例：Stable Diffusion模型迁移到Ascend上进行推理](#)。
- 方式二 ModelArts Lite DevServer：该环境为裸机开发环境，主要面向深度定制化开发场景。
  - 优点：支持深度自定义环境安装，可以方便的替换驱动、固件和上层开发包，具有root权限，结合配置指导、初始化工具及容器镜像可以快速搭建昇腾开发环境。
  - 缺点：资源申请周期长，购买成本高，管理视角下资源使用效率较低。
  - 环境开通指导参考：[DevServer资源开通](#)
  - 环境配置指导参考：[Snt9B裸金属服务器环境配置指南](#)

本文基于方式二的环境进行操作，请参考方式二中的环境开通和配置指导完成裸机和容器开发初始化配置。注意业务基础镜像选择Ascend+PyTorch镜像。

配置好的容器环境如下图所示：

图 6-57 环境配置完成

```
[root@devserver-modelarts-demanager-0eaabe8f ~]# docker run -itd --cap-add=SYS_PTRACE -e ASCEND_VISIBLE_DEVICES=3 -v /home:/home_host -u=0 --name pytorch_test swr.cn-southwest-2.myhuaweicloud.com/atelier/pytorch_1.11_ascend:pytorch_1.11.0-cann_6.3.2-py_3.7-euler_2.10.7-aarch64-d910b-20230815141604-3685231 /bin/bash
0292be41ac1ef03a37b7c78adcf4fc999a967e1163e5f6e565edbe6a638c69b
[root@devserver-modelarts-demanager-0eaabe8f ~]# docker exec -ti 0292be41a bash
The environment has been set
[root@0292be41ac1e ma-user]# source .bashrc
The environment has been set
The environment has been set
(PyTorch-1.11.0) [root@0292be41ac1e ma-user]# python3 -c "import torch;import torch_npu; a = torch.randn(3, 4).npu(); print(a + a);"
tensor([[-1.0911, -0.4146, 1.6027, 1.8585],
 [3.2549, 0.7026, 2.9356, 0.9544],
 [5.1409, -0.8820, -0.3400, 0.0257]]) , device='npu:0')
(PyTorch-1.11.0) [root@0292be41ac1e ma-user]#
```

### 6.3.3 pipeline 应用准备

当前迁移路径是从onnx模型转换到mindir模型，再用mindspore lite做推理，所以迁移前需要用户先准备好自己的onnx pipeline。下文以官方开源的图生图的Stable Diffusion v1.5的onnx pipeline代码为例进行说明。

**步骤1** 进入容器环境，创建自己的工作目录，由于在[Snt9B裸金属服务器环境配置指南](#)的配置环境步骤中，在启动容器时将物理机的home目录挂载到容器的“/home\_host”目录下，该目录下可以直接使用上传到物理机“home”目录下的文件。本文中，将基于容器的“/home\_host”目录创建工作目录：

```
mkdir -p /home_host/work
cd /home_host/work
```

**步骤2** 在迁移onnx pipeline前，首先需要确保原始的onnx pipeline能在昇腾机器的ARM CPU上正常执行。进入容器环境后，安装依赖包。

```
pip install torch==1.11.0 onnx transformers==4.27.4 accelerate onnxruntime diffusers==0.11.1
```

**步骤3** 下载git lfs，用于下载git仓中的大文件。由于欧拉源上没有git-lfs包，所以需要从压缩包中解压使用，在浏览器中输入如下地址下载git-lfs压缩包并上传到服务器的/home目录。

```
https://github.com/git-lfs/git-lfs/releases/download/v3.2.0/git-lfs-linux-arm64-v3.2.0.tar.gz
```

**步骤4** 安装git lfs：

```
tar -zxvf git-lfs-linux-arm64-v3.2.0.tar.gz
cd git-lfs-3.2.0
```

```
sh install.sh
rm -rf git-lfs-linux-arm64-v3.2.0.tar.gz git-lfs-3.2.0
```

### 步骤5 通过git下载sd pytorch模型。

该模型用于获取模型shape，也可以转换生成onnx模型。后文中的modelarts-ascend仓库已经给出了模型shape，可以直接使用，onnx模型也可以单独下载。

```
git clone sd模型
git lfs install
mkdir -p /home_host/work/runwayml
cd /home_host/work/runwayml
git clone https://huggingface.co/runwayml/stable-diffusion-v1-5/ -b main
将下载的文件重命名，以便后续脚本中引用
mv stable-diffusion-v1-5 pytorch_models
```

#### 📖 说明

这里由于Huggingface网站的限制以及模型文件的大小原因，很可能会下载失败。可以进到[Huggingface网站](#)，从浏览器下载模型后，再手工上传到物理机/home/pytorch\_models目录下。

### 步骤6 通过git下载sd onnx模型。

```
git clone sd模型
git lfs install
cd /home_host/work/runwayml
git clone https://huggingface.co/runwayml/stable-diffusion-v1-5 -b onnx
将下载的文件重命名，以便后续脚本中引用
mv stable-diffusion-v1-5 onnx_models
```

#### 📖 说明

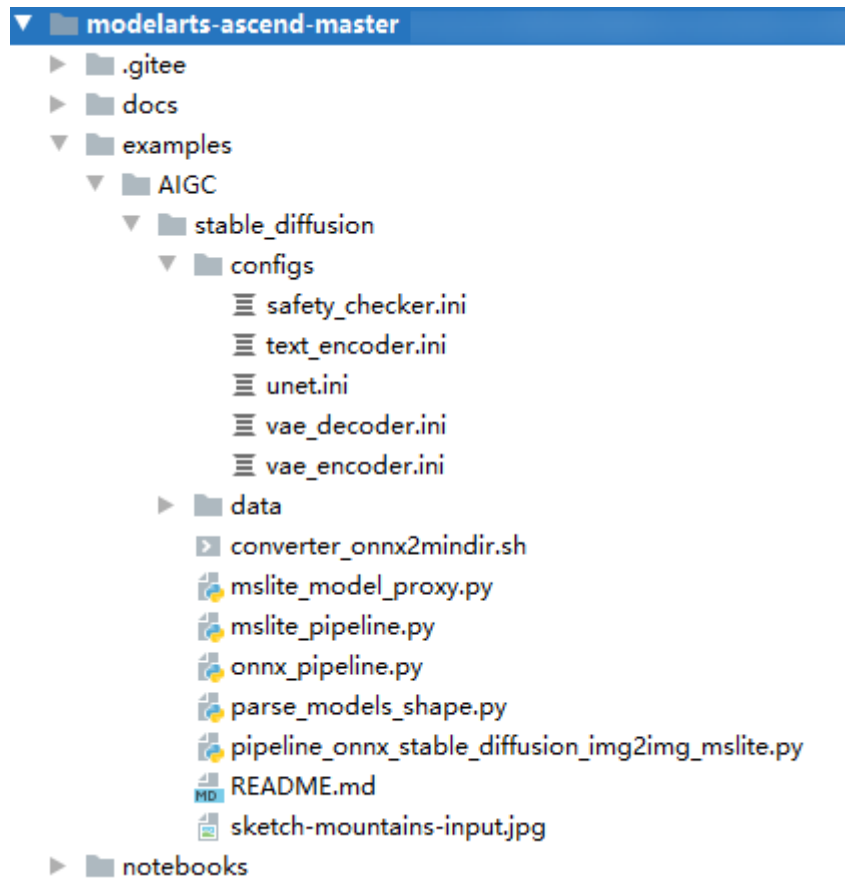
这里由于Huggingface网站的限制以及模型文件的大小原因，很可能会下载失败。可以进到[Huggingface网站](#)，从浏览器下载模型后，再手工上传到物理机/home/onnx\_models目录下。

### 步骤7 下载好模型后，需要编写推理脚本。为了便于讲解，本指导中所需的代码已发布在ModelArts代码仓，可以使用如下命令下载推理脚本样例代码：

```
cd /home_host/work
git clone https://gitee.com/ModelArts/modelarts-ascend.git
ll modelarts-ascend/examples/AIGC/stable_diffusion
```

代码目录如下图所示，onnx\_pipeline.py是图生图推理脚本。mslite\_pipeline.py、mslite\_model\_proxy.py、pipeline\_onnx\_stable\_diffusion\_img2img\_mslite.py是迁移后的文件，其中mslite\_model\_proxy.py是代理模型类，pipeline\_onnx\_stable\_diffusion\_img2img\_mslite.py是从Stable Diffusion源码中的pipeline复制并修改的，这些文件在后续的章节中会使用并做进一步讲解。

图 6-58 代码目录



**步骤8** 将“modelarts-ascend/examples/AIGC/stable\_diffusion/onnx\_pipeline.py”文件中的“onnx\_model\_path”改为步骤6中下载的onnx\_models地址“/home\_host/work/runwayml/onnx\_models”。执行推理脚本进行测试，这里使用的推理硬件是CPU，验证待迁移的代码能在CPU跑通，由于是CPU执行会比较慢，大约需要15分钟左右：

```
cd modelarts-ascend/examples/AIGC/stable_diffusion # 必须执行该命令，否则会报错找不到sketch-mountains-input.jpg
python onnx_pipeline.py
```

生成的图片fantasy\_landscape.png会保存在当前路径下，该图片也可以作为后期精度校验的一个对比。



图 6-59 生成图片



---结束

## 6.3.4 应用迁移

### 6.3.4.1 模型适配

MindSpore Lite是华为自研的推理引擎，能够最大化地利用昇腾芯片的性能。在使用MindSpore Lite进行离线推理时，需要先将模型转换为mindir模型，再利用MindSpore Lite作为推理引擎，将转换后的模型直接运行在昇腾设备上。模型转换需要使用converter\_lite工具。

huggingface提供的onnx模型文件的输入是动态shape，而mindir不支持动态shape，只能使用静态shape或者几个固定档位的分档shape代替。使用converter\_lite转换模型时，也分为静态shape和分档shape两种方式，需要根据具体的业务需求使用对应的转换方式。本次迁移使用的是静态shape方式进行模型转换。

### 获取模型 shape

由于在后续模型转换时需要知道待转换模型的shape信息，这里指导如何通过训练好的stable diffusion pytorch模型获取模型shape，主要有如下两种方式获取：

- 方式1：通过stable diffusion的pytorch模型获取模型shape。

- 方式2: 通过查看[代码仓库](#), 根据每个模型的configs文件获取已知的shape大小。

下文主要介绍方式1如何通过stable diffusion的pytorch模型获取模型shape。

**步骤1** 在pipeline应用准备章节, 已经下载到sd的pytorch模型 ( /home\_host/work/runwayml/pytorch\_models )。进入工作目录:

```
cd /home_host/work
```

**步骤2** 新建python脚本文件 “parse\_models\_shape.py” 用于获取shape, 其中model\_path是指上面下载的pytorch\_models的路径。

```
parse_models_shape.py
import torch
import numpy as np
from diffusers import StableDiffusionPipeline

model_path = '/home_host/work/runwayml/pytorch_models'
pipeline = StableDiffusionPipeline.from_pretrained(model_path, torch_dtype=torch.float32)

TEXT ENCODER
num_tokens = pipeline.text_encoder.config.max_position_embeddings
text_hidden_size = pipeline.text_encoder.config.hidden_size
text_input = pipeline.tokenizer(
 "A sample prompt",
 padding="max_length",
 max_length=pipeline.tokenizer.model_max_length,
 truncation=True,
 return_tensors="pt",
)
print("# TEXT ENCODER")
print(f"input_ids: {np.array(text_input.input_ids.shape).tolist()}")

UNET
UNET_in_channels = pipeline.unet.config.in_channels
UNET_sample_size = pipeline.unet.config.sample_size
print("# UNET")
print(f"sample: [{2}, {UNET_in_channels} {UNET_sample_size} {UNET_sample_size}]")
print(f" timestep: [{1}]") # 此处应该是1, 否则和后续的推理脚本不一致
print(f"encoder_hidden_states: [{2}, {num_tokens} {text_hidden_size}]")

VAE ENCODER
vae_encoder = pipeline.vae
vae_in_channels = vae_encoder.config.in_channels
vae_sample_size = vae_encoder.config.sample_size
print("# VAE ENCODER")
print(f"sample: [{1}, {vae_in_channels}, {vae_sample_size}, {vae_sample_size}]")

VAE DECODER
vae_decoder = pipeline.vae
vae_latent_channels = vae_decoder.config.latent_channels
vae_out_channels = vae_decoder.config.out_channels
print("# VAE DECODER")
print(f"latent_sample: [{1}, {vae_latent_channels}, {UNET_sample_size}, {UNET_sample_size}]")

SAFETY CHECKER
safety_checker = pipeline.safety_checker
clip_num_channels = safety_checker.config.vision_config.num_channels
clip_image_size = safety_checker.config.vision_config.image_size
print("# SAFETY CHECKER")
print(f"clip_input: [{1}, {clip_num_channels}, {clip_image_size}, {clip_image_size}]")
print(f"images: [{1}, {vae_sample_size}, {vae_sample_size}, {vae_out_channels}]")
```

**步骤3** 执行以下命令获取shape信息。

```
python parse_models_shape.py
```

可以看到获取的shape信息如下图所示。

图 6-60 shape 信息

```
(PyTorch-1.8) [ma-user@TEST]python parse_models_shape.py
/home/ma-user/anaconda3/envs/PyTorch-1.8/lib/python3.7/site-packages/requests/_init_.py:104: RequestsDependencyWarning: urllib3 (1.26.12) or chardet (5.0.0)/charset_normalizer (2.0.12) doesn't match a supported version
RequestsDependencyWarning)
text_config_dict is provided which will be used to initialize 'CLIPTextConfig'. The value 'text_config["id2label"]' will be overridden.
/home/ma-user/anaconda3/envs/PyTorch-1.8/lib/python3.7/site-packages/transformers/models/clip/feature_extraction_clip.py:31: FutureWarning: The class CLIPFeatureExtractor is deprecated and will be removed in version 4.0. Please use CLIPImageProcessor instead.
FutureWarning:
TEXT ENCODER
input_ids: [1, 77]
INET
sample: [2, 4, 64, 64]
timeStep: [1]
encoder_hidden_states: [2, 77, 768]
VAE ENCODER
latent_sample: [1, 3, 512, 512]
VAE DECODER
sample: [2, 4, 64, 64]
SAFETY CHECKER
clip_input: [1, 3, 224, 224]
images: [1, 222, 512, 3]
(PyTorch-1.8) [ma-user@TEST]#
```

----结束

## PyTorch 模型转换为 Onnx 模型（可选）

获取onnx模型有两种方式，方式一是使用官方提供的模型转换脚本将pytorch模型转换为onnx模型，方式二是对于提供了onnx模型的仓库，可以直接下载onnx模型。下面介绍方式一如何操作，如果采用方式二，可以跳过此步骤。

**步骤1** 通过git下载diffusers对应版本的源码。

```
git clone https://github.com/huggingface/diffusers.git -b v0.11.1
```

**步骤2** 在diffusers的script/convert\_stable\_diffusion\_checkpoint\_to\_onnx.py脚本中，可以通过执行以下命令生成onnx模型，其中model\_path指定pytorch的模型根目录，output\_path指定生成的onnx模型目录。

```
cd /home_host/work
python diffusers/scripts/convert_stable_diffusion_checkpoint_to_onnx.py --model_path "./runwayml/pytorch_models" --output_path "./pytorch_to_onnx_models"
```

----结束

## 静态 shape 模型转换

转换静态shape模型需要在模型转换阶段固定模型的输入shape，也就是说每个输入shape是唯一的。静态shape转换主要包括两种场景：

- 第一种是待转换onnx模型的输入本身已经是静态shape，此时不需要在转换时指定输入shape也能够正常转换为和onnx模型输入shape一致的mindir模型。
- 第二种是待转换onnx模型的输入是动态shape（导出onnx模型时指定了dynamic\_axes参数），此时需要在转换时明确指定输入的shape。

转换时指定输入shape可以在命令行中指定，也可以通过配置文件的形式进行指定。

- 在命令行中指定输入shape。

命令行可以直接通过--inputShape参数指定输入的shape，格式为“input\_name:input\_shape”，如果有多个输入，需要使用“;”隔开，比如“input1\_name:input1\_shape;input2\_name:input2\_shape”。

```
converter_lite --modelFile=./text_encoder/model.onnx --fmk=ONNX --saveType=MINDIR --optimize=ascend_oriented --outputFile=./text_encoder --inputShape="input_ids:1,77"
```

- 在配置文件中指定输入shape。

配置文件中通过“[ascend\_context]”配置项指定input\_shape，格式与命令行一致，多个输入，需要使用“;”隔开；然后在命令行中通过--configFile指定对应的配置文件路径即可。

```
text_encoder.ini
```

```
[ascend_context]
input_shape=input_ids:[1,77]
```

转换命令如下：

```
converter_lite --modelFile=./text_encoder/model.onnx --fmk=ONNX --saveType=MINDIR --
optimize=ascend_oriented --outputFile=./text_encoder --configFile=./text_encoder.ini
```

在使用converter\_lite工具转换时，默认是将所有算子转换为fp16，如果想要将固定shape的模型精度修改为fp32进行转换，需要在配置文件中指定算子的精度模式为precision\_mode，配置文件的写法如下（更多精度模式请参考[precision\\_mode](#)）：

```
text_encoder.ini
[ascend_context]
input_shape=input_ids:[1,77]
precision_mode=enforce_fp32
```

对于本次AIGC迁移，为了方便对多个模型进行转换，可以通过批量模型转换脚本自动完成所有模型的转换。

**步骤1** 执行以下命令创建并进入static\_shape\_convert目录。

```
mkdir -p /home_host/work/static_shape_convert
cd /home_host/work/static_shape_convert
```

**步骤2** 在static\_shape\_convert目录下新建converter\_onnx2mindir.sh文件并复制下面内容。其中，onnx\_dir表示onnx模型的目录，mindir\_dir指定要生成的mindir模型的保存目录。

```
converter_onnx2mindir.sh
设置onnx模型和mindir模型目录
onnx_dir=/home_host/work/runwayml/onnx_models
mindir_dir=./mindir_models

指定配置文件路径
config_dir=/home_host/work/modelarts-ascend/examples/AIGC/stable_diffusion/configs

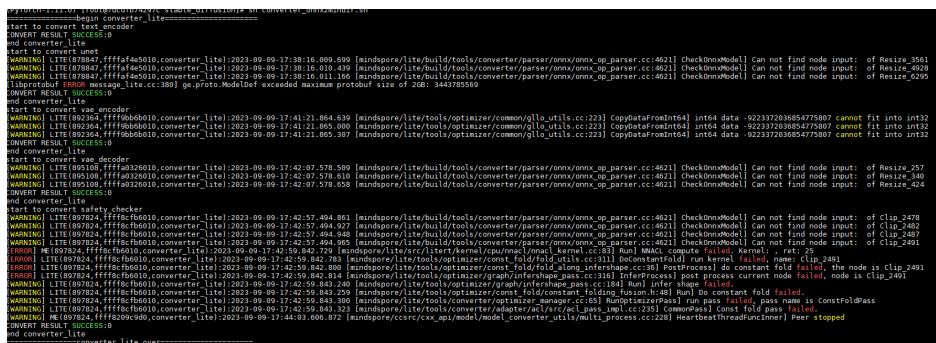
echo "=====begin converter_lite===== "

sub_cmd='--fmk=ONNX --optimize=ascend_oriented --saveType=MINDIR'
mkdir -p $mindir_dir
rm缓存,慎改
atc_data_dir=/root/atc_data/
通用转换方法
common_converter_model() {
 model_name=$1
 echo "start to convert $model_name"
 rm -rf $atc_data_dir
 converter_lite --modelFile="$onnx_dir/$model_name/model.onnx" \
 --outputFile="$mindir_dir/$model_name" \
 --configFile="$config_dir/$model_name.ini" \
 $sub_cmd
 printf "end converter_lite\n"
}
common_converter_model "text_encoder"
common_converter_model "unet"
common_converter_model "vae_encoder"
common_converter_model "vae_decoder"
common_converter_model "safety_checker"

echo "=====converter_lite over===== "
```

转换结果如下，其中safety\_checker模型转换成功了，但中间有ERROR日志，这个属于常量折叠失败，不影响结果。

图 6-61 转换结果



----结束

## 动态分档模型转换（可选）

### 说明

如果迁移的模型有多个shape档位的需求，可以通过如下方式对模型进行分档转换。

动态分档是指将模型输入的某一维或者某几维设置为“动态”可变，但是需要提前设置可变维度的“档位”范围。即转换得到的模型能够在指定的动态轴上使用预设的几种shape（保证模型支持的shape），相比于静态shape更加灵活，且性能不会有劣化。

动态分档模型转换需要使用配置文件，指定输入格式为“ND”，并在config文件中配置ge.dynamicDims和input\_shape使用，在input\_shape中将输入shape的动态维度设为-1，并在ge.dynamicDims中指定动态维度的档位，更多配置项可以参考[官方文档](#)。

- 如果网络模型只有一个输入：每个档位的dim值与input\_shape参数中的-1标识的参数依次对应，input\_shape参数中有几个-1，则每档必须设置几个维度。

以text\_encoder模型为例，修改配置文件text\_encoder.ini如下所示：

```
text_encoder.ini

[accl_build_options]
input_format="ND"
input_shape="input_ids:-1,-1"
ge.dynamicDims="77;33"
```

使用上述配置文件转换得到的模型，支持的输入shape为(1,77)和(1,33)。

然后使用converter\_lite执行模型转换，转换命令如下：

```
converter_lite --modelFile=./onnx_models/text_encoder/model.onnx --fmk=ONNX --saveType=MINDIR
--optimize=ascend_oriented --outputFile=./mindirs --configFile=./configs/text_encoder.ini
```

- 如果网络模型有多个输入：档位的dim值与网络模型输入参数中的-1标识的参数依次对应，网络模型输入参数中有几个-1，则每档必须设置几个维度。

以unet模型为例，该网络模型有三个输入，分别为“sample(1,4,64,64)”、“timestep(1)”、“encoder\_hidden\_states(1,77,768)”，修改unet.ini配置文件如下所示：

```
unet.ini

[accl_build_options]
input_format="ND"
input_shape="sample:-1,4,64,64;timestep:1;encoder_hidden_states:-1,77,768"
ge.dynamicDims="1,1;2,2;3,3"
```

转换得到的模型支持的输入dims组合档数分别为：

图 6-62 组合档数

```
[acl_build_options]
input_format="ND"
input_shape="sample:-1,4,64,64;timestep:1;encoder_hidden_states:-1,77,768"
ge.dynamicDims="1,1;2,2;3,3"
```

第0档: sample(1,4,64,64) + timestep(1) + encoder\_hidden\_states(1,77,768)

第1档: sample(2,4,64,64) + timestep(1) + encoder\_hidden\_states(2,77,768)

第2档: sample(3,4,64,64) + timestep(1) + encoder\_hidden\_states(3,77,768)

然后使用converter lite执行模型转换，转换命令如下：

```
converter_lite --modelFile=./onnx_models/unet/model.onnx --fmk=ONNX --saveType=MINDIR --
optimize=ascend_oriented --outputFile=./mindirs --configFile=./configs/unet.ini
```

### 说明

- 最多支持100档配置，每一档通过英文逗号分隔。
- 如果用户设置的dim数值过大或档位过多，可能会导致模型编译失败，此时建议用户减少档位或调低档位数值。
- 如果用户设置了动态维度，实际推理时，使用的输入数据的shape需要与设置的档位相匹配。

## 6.3.4.2 pipeline 代码适配

onnx pipeline的主要作用是将onnx模型进行一系列编排，并在onnx Runtime上按照编排顺序执行。因此，需要将转换得到的mindir模型按照相同的逻辑进行编排，并在MindSpore Lite上执行。只需要将原始onnx的pipeline中涉及到onnx模型初始化及推理的接口替换为MindSpore Lite的接口即可。

MindSpore Lite提供了Python、C++以及JAVA三种应用开发接口，此处以Python接口为例，介绍如何使用MindSpore Lite Python API构建并推理Stable Diffusion模型，更多信息请参考[MindSpore Lite应用开发](#)。

以官方onnx pipeline代码为例，其提供的onnx pipeline代码路径在“[\\${diffusers}/pipelines/stable\\_diffusion/pipeline\\_onnx\\_stable\\_diffusion\\_img2img.py](#)”，其中\${diffusers}表示diffusers包的安装路径，可以通过pip进行查看。

```
shell
pip show diffusers
```

## 修改代码依赖

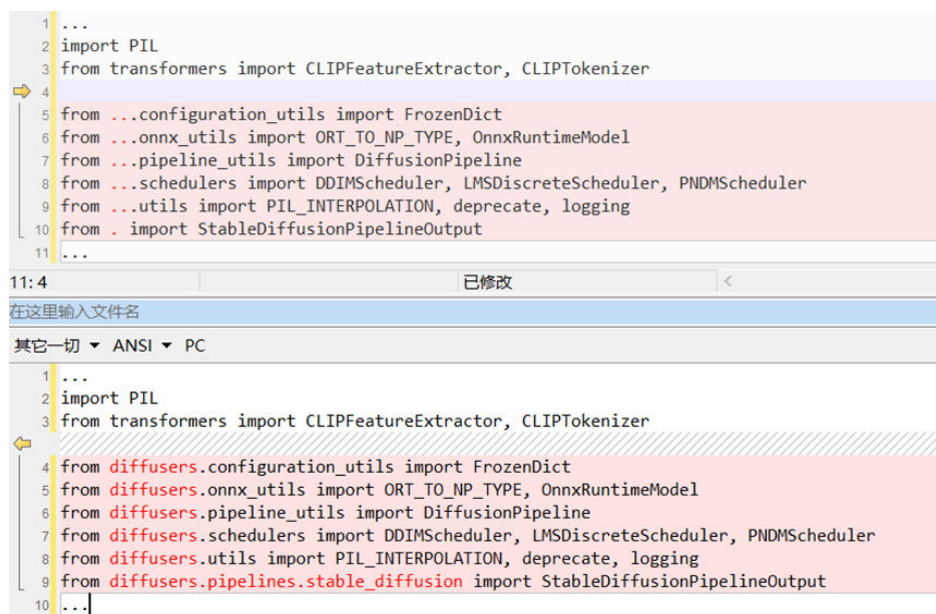
新建并进入/home\_host/work/pipeline目录。

```
mkdir -p /home_host/work/pipeline
cd /home_host/work/pipeline
```

将onnx pipeline依赖的图生图源码“pipeline\_onnx\_stable\_diffusion\_img2img.py”复制到该目录下，名称改为“pipeline\_onnx\_stable\_diffusion\_img2img\_mslite.py”，以便与源文件名称区分。但是这样也会导致无法正确找到源码中相对路径下的依赖，需要将对于diffusers包内的相对路径修改为绝对路径的形式。



图 6-63 代码依赖修改前与修改后



```
1 ...
2 import PIL
3 from transformers import CLIPFeatureExtractor, CLIPTokenizer
4
5 from ...configuration_utils import FrozenDict
6 from ...onnx_utils import ORT_TO_NP_TYPE, OnnxRuntimeModel
7 from ...pipeline_utils import DiffusionPipeline
8 from ...schedulers import DDIMScheduler, LMSDiscreteScheduler, PNDMScheduler
9 from ...utils import PIL_INTERPOLATION, deprecate, logging
10 from . import StableDiffusionPipelineOutput
11 ...
```

11:4 已修改

```
1 ...
2 import PIL
3 from transformers import CLIPFeatureExtractor, CLIPTokenizer
4
5 from diffusers.configuration_utils import FrozenDict
6 from diffusers.onnx_utils import ORT_TO_NP_TYPE, OnnxRuntimeModel
7 from diffusers.pipeline_utils import DiffusionPipeline
8 from diffusers.schedulers import DDIMScheduler, LMSDiscreteScheduler, PNDMScheduler
9 from diffusers.utils import PIL_INTERPOLATION, deprecate, logging
10 from diffusers.pipelines.stable_diffusion import StableDiffusionPipelineOutput
11 ...
```

将推理代码“modelarts-ascend/examples/AIGC/stable\_diffusion/onnx\_pipeline.py”也复制一份到该目录，名称改为“mslite\_pipeline.py”，迁移后的推理代码中的pipeline需要修改为从复制的onnx\_pipeline文件导入：

```
onnx_pipeline.py
from pipeline_onnx_stable_diffusion_img2img_mslite import OnnxStableDiffusionImg2imgPipeline
```

## 模型初始化

使用MindSpore Lite进行推理时一般需要先设置目标设备的上下文信息，然后构建推理模型，获取输入数据，模型预测并得到最终的结果。一个基础的推理框架写法如下所示：

```
base_mslite_demo.py
import mindspore_lite as mslite

设置目标设备上下文为Ascend，指定device_id为0
context = mslite.Context()
context.target = ["ascend"]
context.ascend.device_id = 0
构建模型
model = mslite.Model()
model.build_from_file("./model.mindir", mslite.ModelType.MINDIR, context)

输入数据到Device侧，针对于多输入场景可以通过list来指定输入
in_data = [np.array(data1), np.array(data2)]
inputs = model.get_inputs()
for i, _inputs in enumerate(inputs):
 _input.set_data_from_numpy(in_data[i])
前向推理，并将结果从device侧传到host侧
outputs = model.predict(inputs)
outputs = [output.get_data_to_numpy() for output in outputs]
后处理...
```

为了同时兼容onnx模型和mindir模型都能够在适配后的pipeline中运行，需要对于Model进行封装，MsliteModel各参数模型说明已给出，根据模型初始化参数设置当前模型使用onnx模型（运行在CPU上）或mindir模型（运行在昇腾设备上），也能够方便进行精度的校验。



```
mslite_model_proxy.py
import os
import mindspore_lite as mslite
class MsliteModel:
 def __init__(self, model_path, model_name='ms model', device_type='ascend', use_ascend=True,
 onnx_runtime_model=None, get_shape=False, resize_shape=False) -> None:
 """
 mindir模型代理类
 Args:
 model_path: mindir文件路径
 model_name: 模型名称
 device_type: 设备类型
 use_ascend: 是否使用Ascend
 onnx_runtime_model: onnx模型对象
 get_shape: 是否获取模型shape信息、输入数据shape信息
 resize_shape: resize shape开关, 分档模型需开启
 """
 print('model_path:{}'.format(model_path))
 self.model_name = model_name
 self.context = MsliteModel.init_context(device_type)
 self.model = mslite.Model()
 self.model.build_from_file(model_path, mslite.ModelType.MINDIR, self.context)
 self.ms_inputs = self.model.get_inputs()
 self.use_ascend = use_ascend
 self.onnx_runtime_model = onnx_runtime_model
 self.get_shape = get_shape
 self.resize_shape = resize_shape
 @staticmethod
 def init_context(device_type='ascend'):
 context = mslite.Context()
 context.target = [device_type]
 context.ascend.device_id = int(os.getenv('DEVICE_ID') or 0)
 context.cpu.thread_num = 1 if device_type == 'ascend' else 32
 context.cpu.thread_affinity_mode = 2
 return context
 def __call__(self, **kwargs):
 if not self.use_ascend:
 return self.onnx_runtime_model(**kwargs)
 inputs = list(kwargs.values())
 if len(inputs) <= 0:
 raise Exception('get tensor input info failed')
 ms_input = self.model.get_inputs()
 if self.get_shape:
 print(f'{self.model_name} shape info:')
 for index, val in enumerate(self.model.get_inputs()):
 print(f'{self.model_name}: param{index} shape -> {val.shape}')
 shapes = [list(input.shape) for input in inputs]
 print(f"inputs: input_shape -> {shapes}")
 if self.resize_shape:
 self.model.resize(ms_input, [list(input.shape) for input in inputs])
 for index, val in enumerate(ms_input):
 val.set_data_from_numpy(inputs[index])
 outputs = self.model.predict(ms_input)
 outputs = [output.get_data_to_numpy() for output in outputs]
 return outputs
```

适配MindSpore Lite Runtime到onnx pipeline，首先需要初始化MindSpore LiteModel对象，通过在OnnxStableDiffusionImg2ImgPipeline中增加mindir模型初始化函数，然后在pipeline类的\_\_init\_\_方法调用该函数，在pipeline初始化的时候直接初始化模型。可以参照如下样例，可以通过修改use\_ascend去修改该模型是否使用mindir运行，也可以编写代码通过环境变量指定。

```
pipeline_onnx_stable_diffusion_img2img_mslite.py
class OnnxStableDiffusionImg2ImgPipeline(DiffusionPipeline):
 ...
 def mslite_modules_init(self):
 self.text_encoder_ms = MsliteModel(
 model_path=os.environ['TEXT_ENCODER_PATH'],
```

```
 model_name='text_encoder', use_ascend=True,
 onnx_runtime_model=self.text_encoder)
self.vae_encoder_ms = MsliteModel(
 model_path=os.environ['VAE_ENCODER_PATH'],
 model_name='vae_encoder', use_ascend=True,
 onnx_runtime_model=self.vae_encoder)
self.unet_ms = MsliteModel(model_path=os.environ['UNET_PATH'],
 model_name='unet', use_ascend=True,
 onnx_runtime_model=self.unet)
self.vae_decoder_ms = MsliteModel(model_path=os.environ['VAE_DECODER_PATH'],
 model_name='vae_decoder', use_ascend=True,
 onnx_runtime_model=self.vae_decoder)
self.safety_checker_ms = MsliteModel(model_path=os.environ['SAFETY_CHECKER_PATH'],
 model_name='safety_checker', use_ascend=True,
 onnx_runtime_model=self.safety_checker)
...
```

## 模型推理适配

完成模型初始化后，需要将onnx模型推理的代码等价替换为对应的mindir模型推理接口。以vae\_encoder模型为例，在pipeline代码中查找vae\_encoder推理调用的地方，然后修改为对应的MindSpore Lite版本的推理接口模型。

- 使用MindSpore Lite Runtime接口替换onnx Runtime接口

```
pipeline_onnx_stable_diffusion_img2img_mslite.py
...
onnx模型
init_latents = self.vae_encoder(sample=image)[0]
-----修改点-----
mslite模型
init_latents = self.vae_encoder_ms(sample=image)[0]
...
```

- 替换内嵌模型

```
pipeline_onnx_stable_diffusion_img2img_mslite.py
...
onnx模型
image = np.concatenate([self.vae_decoder(latent_sample=latents[i : i + 1])[0] for i in
range(latents.shape[0])])
-----修改点-----
mslite模型
image = np.concatenate([self.vae_decoder_ms(latent_sample=latents[i : i + 1])[0] for i in
range(latents.shape[0])])
...
```

修改后的文件参考[Gitee代码库](#)中的如下两个文件：

- pipeline\_onnx\_stable\_diffusion\_img2img\_mslite.py
- mslite\_model\_proxy.py

## 运行 pipeline 代码

pipeline代码如下：

```
mslite_pipeline.py
import os

import requests
import torch
import numpy as np
from PIL import Image
from io import BytesIO

from pipeline_onnx_stable_diffusion_img2img_mslite import OnnxStableDiffusionImg2ImgPipeline

def setup_seed(seed):
```

```

torch.manual_seed(seed)
torch.cuda.manual_seed_all(seed)
np.random.seed(seed)
torch.backends.cudnn.deterministic = True

setup_seed(0)

指定mindir和onnx模型路径
mindir_dir = "/home_host/work/static_shape_convert/mindir_models"
onnx_model_path = "/home_host/work/runwayml/onnx_models"

os.environ['DEVICE_ID'] = "0"
os.environ['TEXT_ENCODER_PATH'] = f"{mindir_dir}/text_encoder.mindir"
os.environ['VAE_ENCODER_PATH'] = f"{mindir_dir}/vae_encoder.mindir"
os.environ['UNET_PATH'] = f"{mindir_dir}/UNET_graph.mindir"
os.environ['VAE_DECODER_PATH'] = f"{mindir_dir}/vae_decoder.mindir"
os.environ['SAFETY_CHECKER_PATH'] = f"{mindir_dir}/safety_checker.mindir"
pipe = OnnxStableDiffusionImg2ImgPipeline.from_pretrained(onnx_model_path,
 torch_dtype=torch.float32).to("cpu")
url = "https://raw.githubusercontent.com/CompVis/stable-diffusion/main/assets/stable-samples/img2img/
sketch-mountains-input.jpg"
response = requests.get(url, verify=False)
init_image = Image.open(BytesIO(response.content)).convert("RGB")
init_image = init_image.resize((512, 512))

prompt = "A fantasy landscape, trending on artstation"
images = pipe(prompt=prompt, image=init_image, strength=0.75, guidance_scale=7.5).images
images[0].save("fantasy_landscape_npu.png")

```

在运行pipeline时，默认的加速卡为0号卡，当机器有多人使用时，可能存在资源占用而无法正常运行情况，可以通过环境变量指定加速卡ID，如指定5号卡进行执行。

```

mslite_pipeline.py
...
os.environ['DEVICE_ID'] = "5"
...

```

最后执行python脚本进行推理：

```

#shell
python mslite_pipeline.py

```

图 6-64 执行推理脚本

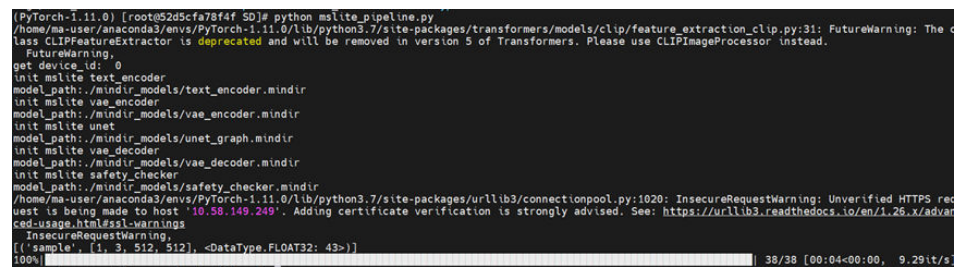


图 6-65 MindSpore Lite pipeline 输出的结果图片



### 6.3.5 迁移效果校验

在pipeline适配完成后，需要验证适配后的效果是否满足要求，通过对比原始onnx pipeline的最终输出结果确认迁移效果。如果精度和性能都没有问题，则代表迁移完成。

#### 对比图片生成效果

在CPU上推理onnx，将原始onnx和适配完成的MindSpore Lite pipeline输出的结果图片进行对比，在这里保证输入图片及文本提示词一致。如果差异较为明显可以进行[模型精度调优](#)。

#### 确认性能是否满足要求

在推理代码开始结尾处加入时间记录，并打印出推理执行耗时。根据用户需求判断性能是否满足要求，如果不满足可以进行[性能调优](#)。

```
import time
start_time = time.time()
推理代码
end_time = time.time()
print(f"infer time {end_time - start_time}")
```

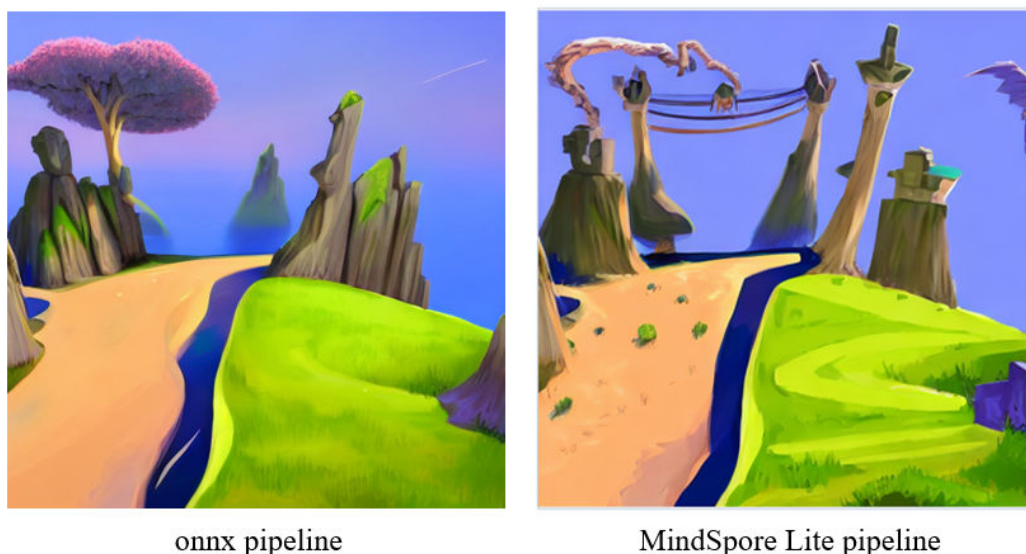
## 6.3.6 模型精度调优

### 6.3.6.1 场景介绍

本小节通过一个具体问题案例，介绍模型精度调优的过程。

如下图所示，使用MindSpore Lite生成的图像和onnx模型的输出结果有明显的差异，因此需要对MindSpore Lite pipeline进行精度诊断。

图 6-66 结果对比



#### 📖 说明

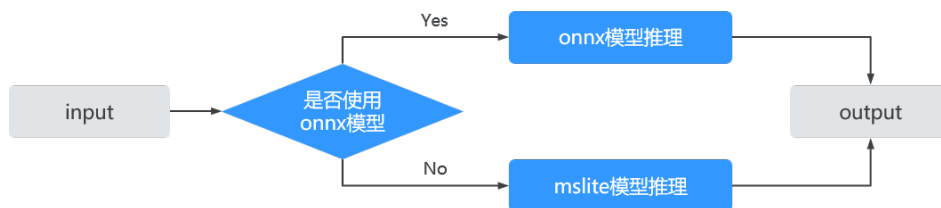
在MindSpore Lite 2.0.0版本中，Stable Diffusion的五个模型的精度都能够保证一致性，但是在最新的2.1.0版本中，会出现text\_encoder模型精度不一致的情况。该问题后续会发布补丁进行修复。

### 6.3.6.2 精度问题诊断

#### 逐个替换模型，检测有问题的模型

该方式主要是通过模型替换，先定位出具体哪个模型引入的误差，进一步诊断具体的模型中哪个算子或者操作导致效果问题，模型替换原理如下图所示。通过设置开关选项（是否使用onnx模型），控制模型推理时，模型使用的是onnx模型或是mindir的模型。

图 6-67 精度诊断流程



一般情况下，onnx模型推理的结果可以认为是标杆数据，单独替换某个onnx模型为MindSpore Lite模型，运行得到的结果再与标杆数据做对比，如果没有差异则说明pipeline的差异不是由当前替换的MindSpore Lite模型引入。

如果有差异，则说明当前模型与原始onnx的结果存在差异。依次单独替换onnx模型为对应的MindSpore Lite模型，从而定位出有差异的模型。在模型初始化的代码块已经添加了use\_ascend参数，修改参考如下：

图 6-68 代码修改

```

其它一切 ▾ ANSI ▾ PC
pipeline_onnx_stable_diffusion_img2img_mslite.py

class OnnxStableDiffusionImg2ImgPipeline(DiffusionPipeline):

 def mslite_modules_init(self):
 self.text_encoder_ms = MsliteModel(
 model_path=os.environ['TEXT_ENCODER_PATH'],
 model_name='text_encoder', use_ascend=True,
 onnx_runtime_model=self.text_encoder)
 self.vae_encoder_ms = MsliteModel(
 model_path=os.environ['VAE_ENCODER_PATH'],
 model_name='vae_encoder', use_ascend=True,
 onnx_runtime_model=self.vae_encoder)

8: 57 已修改

在这里输入文件名

其它一切 ▾ ANSI ▾ PC
pipeline_onnx_stable_diffusion_img2img_mslite.py

class OnnxStableDiffusionImg2ImgPipeline(DiffusionPipeline):

 def mslite_modules_init(self):
 self.text_encoder_ms = MsliteModel(
 model_path=os.environ['TEXT_ENCODER_PATH'],
 model_name='text_encoder', use_ascend=False,
 onnx_runtime_model=self.text_encoder)
 self.vae_encoder_ms = MsliteModel(
 model_path=os.environ['VAE_ENCODER_PATH'],
 model_name='vae_encoder', use_ascend=True,
 onnx_runtime_model=self.vae_encoder)

8: 58 已修改
⇒ model_name='text_encoder', use_ascend=True,
⇐ model_name='text_encoder', use_ascend=False,

```

以上述现象为例，通过修改use\_ascend参数值对模型替换，可以发现：当text\_encoder模型为onnx模型，其余模型为mindir模型时，能够得到和标杆数据相同的输出，因此可以判断出转换得到的text\_encoder模型是产生pipeline精度误差的根因。通过下一小节可以进一步确认模型精度的差异。

### 6.3.6.3 精度问题处理

#### 设置高精度并重新转换模型

在转换模型时，默认采用的精度模式是fp16，如果转换得到的模型和标杆数据的精度差异比较大，可以使用fp32精度模式提升模型的精度（这块无需全换成fp32，fp32相对于fp16性能较差，所以一般检测出来哪个模型精度有问题时，再尝试是否用fp32）。使用fp32精度模式的配置文件如下：

配置文件：

```

config.ini
[ascend_context]
precision_mode=enforce_fp32 #使用 fp32

```



## 其他方式

需要实际分析算子层面的差异，需要联系华为工程师进行具体分析。

### 6.3.7 性能调优

在模型精度对齐后，针对SD模型性能调优，可以通过AOE工具进行自助性能调优，进一步可以通过profiling工具对于性能瓶颈进行分析，并针对性的做一些调优操作。

#### 6.3.7.1 单模型性能测试工具 Mindspore lite benchmark

可以直接使用benchmark命令测试mindir模型性能，用来对比调优前后性能是否有所提升。

```
shell
cd /home_host/work
benchmark --modelFile=diffusers/scripts/mindir_models/text_encoder.mindir --device=Ascend
```

上述命令中：modelFile指定生成的mindir模型文件；device指定运行推理的设备。其他用法参考[benchmark文档](#)。

测试结果如下所示：

图 6-69 测试结果

```
[root@6861cf0c12ba work]# benchmark --modelFile=diffusers/scripts/mindir_models/text_encoder.mindir --device=Ascend
ModelPath = diffusers/scripts/mindir_models/text_encoder.mindir
ModelType = MindIR
InDataPath =
GroupInfoFile =
ConfigFilePath =
InDataType = bin
LoopCount = 10
DeviceType = Ascend
AccuracyThreshold = 0.5
CosineDistanceThreshold = -1.1
WarmUpLoopCount = 3
NumThreads = 2
InterOpParallelNum = 1
Fp16Priority = 0
EnableParallel = 0
calibDataPath =
EnableGLTexture = 0
cpuBindMode = HIGHER_CPU
CalibDataType = FLOAT
start unified benchmark run
PrepareTime = 2357.9 ms
Running warm up loops...
Running benchmark loops...
Model = text_encoder.mindir, NumThreads = 2, MinRunTime = 3.974000 ms, MaxRuntime = 3.995000 ms, AvgRunTime = 3.982000 ms
Run Benchmark text_encoder_mindir Success.
```

#### 6.3.7.2 单模型性能调优 AOE

使用AOE工具可以在模型转换阶段对于模型运行和后端编译过程进行执行调优，注意AOE只适合静态shape的模型调优。在AOE调优时，容易受当前缓存的一些影响，建议分两次进行操作，以达到较好的优化效果（第一次执行生成AOE的知识库，在第二次使用时可以复用）。在该场景中，AOE对text\_encoder等模型提升效果不大，性能主要瓶颈点在unet模型中，主要对unet模型做调优，整体的操作步骤如下：

**步骤1** 转换前先清理缓存，避免转换时的影响。

```
#shell
删除已有的aoe知识库，或者备份一份
rm -rf /root/Ascend/latest/data/aoe
删除编译缓存
rm -rf /root/atc_data/*
```

**步骤2** 新建并进入aoe工作目录

```
mkdir -p /home_host/work/aoe
cd /home_host/work/aoe
```

**步骤3** 在配置文件中启用AOE自动调优。



配置unet.ini，开启aoe调优 (aoe\_mode + op\_select\_impl\_mode)。

```
#unet.ini
[ascend_context]
input_shape=sample:[2,4,64,64];timestep:[1];encoder_hidden_states:[2,77,768]
input_format=NCHW

aoe_mode="subgraph tuning, operator tuning"
op_select_impl_mode=high_performance
```

配置打印ASCEND日志，其中ASCEND\_GLOBAL\_LOG\_LEVEL的值对应的日志级别分别为：0-debug、1-info、2-warning、3-error。

```
#shell
export ASCEND_GLOBAL_LOG_LEVEL=1
export ASCEND_SLOG_PRINT_TO_STDOUT=1
```

模型转换时指定AOE调优配置文件。

```
#shell
模型转换时指定AOE调优配置文件并将调优日志输出到aoe_unet.log
mkdir aoe_output
converter_lite --modelFile=/home_host/work/runwayml/onnx_models/unet/model.onnx --outputFile=./
aoe_output/aoe_unet --configFile=unet.ini --fmk=ONNX --saveType=MINDIR --optimize=ascend_oriented >
aoe_unet.log
```

启动AOE调优后，模型转换时长会延长到数小时，因为其中包含了AOE的转化过程耗时较长，也可以指定调优时间，一般情况下时间越长效果会越好，一般10h以内即可，推荐在后台执行。调优完成后，默认将AOE生成的知识库保存在“/root/Ascend/latest/data/aoe”路径下，同时会在aoe\_output路径下输出对应的mindir模型，由于当前模型并没有吸收知识库信息，所以性能不佳，因此需要在保留AOE知识库的情况下，再次进行转换，以达到较优性能。

#### 步骤4 删除编译缓存atc\_data。

##### 📖 说明

注意相比第一次清除缓存操作，本次保留了AOE知识库。

```
#shell
删除编译缓存
rm -rf /root/atc_data/*
```

#### 步骤5 再次执行模型转换命令，确保AOE能够命中知识库。

配置config.ini，关闭AOE调优：

```
unet.ini

[ascend_context]
input_shape=sample:[2,4,64,64];timestep:[1];encoder_hidden_states:[2,77,768]
input_format=NCHW
```

再次执行模型转换命令（此次运行关闭了AOE，速度会变快）：

```
#shell
converter_lite --modelFile=/home_host/work/runwayml/onnx_models/unet/model.onnx --outputFile=./
aoe_output/aoe_unet --configFile=unet.ini --fmk=ONNX --saveType=MINDIR --optimize=ascend_oriented >
aoe_unet2.log
```

此时，aoe\_output下面会有对应的mindir模型，包含了aoe知识库信息。使用benchmark工具测试新生成的mindir模型性能，同aoe调优前的模型进行对比，可以看到模型性能有所提升。

```
#shell
调优前命令如下：
benchmark --modelFile=/home_host/work/static_shape_convert/mindir_models/unet_graph.mindir --
device=Ascend --numThreads=1 --parallelNum=1 --workersNum=1 --warmUpLoopCount=100 --
loopCount=100
```

```
调优后命令如下：
benchmark --modelFile=/home_host/work/aoe/aoe_output/aoe_unet_graph.mindir --device=Ascend --
numThreads=1 --parallelNum=1 --workersNum=1 --warmUpLoopCount=100 --loopCount=100
```

图 6-70 调优前模型

```
[root@6861cf0c12ba aoe]# benchmark --modelFile=/home_host/work/static_shape_convert/mindir_models/UNET_graph.mindir --device=Ascend --numThreads=1 --parallelNum=1 --workersNum=1 --warmUpLoopCount=100 --loopCount=100
ModelPath = /home_host/work/static_shape_convert/mindir_models/UNET_graph.mindir
ModelType = MindIR
InDataPath =
GroupInfoFile =
ConfigFilePath =
InDataType = bin
LoopCount = 100
DeviceType = Ascend
AccuracyThreshold = 0.5
CosineDistanceThreshold = -1.1
WarmUpLoopCount = 100
NumThreads = 1
InterOpParallelNum = 1
Fp16Priority = 0
EnableParallel = 0
calibDataPath =
EnableGLTexture = 0
cpuBindMode = HIGHER_CPU
CalibDataType = FLOAT
start unified benchmark run
PrepareTime = 7756.27 ms
Running warm up loops...
Running benchmark loops...
Model = UNET_graph.mindir, NumThreads = 1, MinRuntime = 72.867996 ms, MaxRuntime = 77.177002 ms, AvgRuntime = 74.184998 ms
Run Benchmark UNET_graph.mindir Success.
```

图 6-71 调优后模型

```
[root@6861cf0c12ba aoe]# benchmark --modelFile=/home_host/work/aoe/aoe_output/aoe_UNET_graph.mindir --device=Ascend --numThreads=1 --parallelNum=1 --workersNum=1 --warmUpLoopCount=100 --loopCount=100
ModelPath = /home_host/work/aoe/aoe_output/aoe_UNET_graph.mindir
ModelType = MindIR
InDataPath =
GroupInfoFile =
ConfigFilePath =
InDataType = bin
LoopCount = 100
DeviceType = Ascend
AccuracyThreshold = 0.5
CosineDistanceThreshold = -1.1
WarmUpLoopCount = 100
NumThreads = 1
InterOpParallelNum = 1
Fp16Priority = 0
EnableParallel = 0
calibDataPath =
EnableGLTexture = 0
cpuBindMode = HIGHER_CPU
CalibDataType = FLOAT
start unified benchmark run
PrepareTime = 5907.39 ms
Running warm up loops...
Running benchmark loops...
Model = aoe_UNET_graph.mindir, NumThreads = 1, MinRuntime = 44.772999 ms, MaxRuntime = 46.356998 ms, AvgRuntime = 45.570999 ms
Run Benchmark aoe_UNET_graph.mindir Success.
```

AOE优化成功的mindir已经融合了优化的知识库，是一个独立可用的模型。即使AOE知识库删除，不影响该mindir的性能。可以备份这个模型优化产生的知识库，以后需要的话再使用。

----结束

## 6.3.8 常见问题

### 6.3.8.1 模型转换失败怎么办？

常见的模型转换失败原因可以通过查询转换失败错误码来确认具体失败的原因，Stable Diffusion新推出的模型在转换中可能会遇到算子不支持的问题，可以到华为云管理页面上提交工单来寻求帮助。

### 6.3.8.2 图片大 Shape 性能劣化严重怎么办？

在昇腾设备上，可能由于GPU内存墙导致在大shape下遇到性能问题，MindSpore Lite提供了Flash Attention编译优化机制，可以考虑升级最新版本的MindSpore Lite Convertor来进行编译期的算子优化，在大Shape场景下会有明显的改善。

### 6.3.8.3 同样功能的 PyTorch Pipeline，因为指导要求适配 onnx pipeline，两个 pipeline 本身功能就有差别，如何适配？

由于Diffusers社区的“single model file policy”设计原则，不同的pipeline是不同路径在独立演进的。先确保应用输出符合预期后，再进入到MindSpore Lite模型转换的过程，否则迁移昇腾后还是会遇到同样的问题。

### 6.3.8.4 AOE 的自动性能调优使用上完全没有效果怎么办？

在MindSpore Lite Convertor2.1版本之前可能出现的调优不生效的场景，建议直接使用MindSpore Lite Convertor2.1及以后的版本。配置文件指定选项进行AOE调优。使用转换工具配置config参数，具体如下所示，其中“subgraph tuning”表示子图调优，“operator tuning”表示算子调优。

其中，“ge.op\_compiler\_cache\_mode”在该场景下必须设置为“force”，表示该场景下要强制刷新缓存，保证AOE调优后的知识库能够命中，实现模型调优。示例如下：

```
config.ini
[ascend_context]
aoe_mode="subgraph tuning, operator tuning"
[acl_init_options]
ge.op_compiler_cache_mode="force"
```

### 6.3.8.5 迁移后应用出图效果相比 GPU 无法对齐怎么办

扩散模型在噪音和随机数上的生成，本身就有一定的随机性，GPU和NPU（Ascend）硬件由于存在一定细小的差别，很难确保完全一致，较难达成生成图片100%匹配，建议通过盲测的方式对效果进行验证。

### 6.3.8.6 模型精度有问题怎么办？

首先考虑通过FP16的方式进行转换和执行，再通过精度诊断工具来进行分析，更进一步可以到华为云官网上提交工单处理。

### 6.3.8.7 模型转换失败时如何查看日志和定位原因？

在模型转换的过程，如果出现模型转换失败，可以参考以下步骤查看日志并定位原因：

#### 步骤1 设置DEBUG日志。

设置MindSpore日志环境变量。

```
#shell
export GLOG_v=0 # 0-DEBUG、1-INFO、2-WARNING、3-ERROR
```

设置CANN日志环境变量。

```
#shell
export ASCEND_GLOBAL_LOG_LEVEL=1 # 0: 表示DEBUG、1: 表示INFO、2: 表示WARNING、3: 表示ERROR 4: 表示NONE
export ASCEND_SLOG_PRINT_TO_STDOUT=1 # 表示日志打印
```

#### 步骤2 设置DUMP模型转换中间图。

设置dDUMP中间图环境变量。

```
#shell
export DUMP_GE_GRAPH=2 # 1: 表示dump图全量内容、2: 表示不dump权重数据的基础图、3: 表示只dump节点关系的精简图
export DUMP_GRAPH_LEVEL=2 # 1: 表示dump图所有图、2: 表示dump除子图外的所有图、3: 表示只dump最后一张图
```

#### 步骤3 问题分析。

配置以上的环境变量之后，再重新转换模型，导出对应的日志和dump图进行分析：

1. 报错日志中搜到“not support onnx data type”，表示MindSpore暂不支持该算子。



图 6-73 修改内容

```

其它一切 ▾ ANSI ▾ PC
predict the noise residual
timestep = np.array([t], dtype=timestep_dtype)
unet

noise_pred = self.unet_ms(
sample=latent_model_input, timestep=timestep.astype("int32"), encoder_hidden_states=text_embeddings
)[0]

perform guidance
if do_classifier_free_guidance:
noise_pred_uncond, noise_pred_text = np.split(noise_pred, 2)

17: 74 默认文本 已修改 <
在这里输入文件名
其它一切 ▾ ANSI ▾ PC

predict the noise residual
timestep = np.array([t], dtype=timestep_dtype)
unet

noise_pred = self.unet_ms(
sample=latent_model_input, timestep=timestep.astype("float32"), encoder_hidden_states=text_embeddings
)[0]

perform guidance
if do_classifier_free_guidance:
noise_pred_uncond, noise_pred_text = np.split(noise_pred, 2)
noise_pred = noise_pred_uncond + guidance_scale * (noise_pred_text - noise_pred_uncond)

compute the previous noisy sample x_t -> x_{t-1}
scheduler_output = self.scheduler.step(
torch.from_numpy(noise_pred), t, torch.from_numpy(latents), **extra_step_kwargs
)
latents = scheduler_output.prev_sample.numov()

```

## 6.4 推理业务昇腾迁移通用指导

### 6.4.1 简介

#### 场景介绍

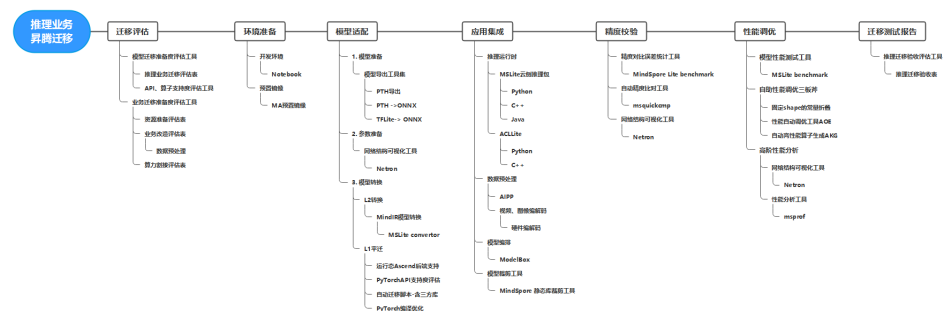
本文旨在指导客户将已有的推理业务迁移到昇腾设备上运行（单机单卡、单机多卡），并获得更好的推理性能收益。

ModelArts针对上述使用场景，在给出系统化推理业务昇腾迁移方案的基础上，提供了即开即用的云上集成开发环境，包含迁移所需要的算力资源和工具链，以及具体的Notebook代码运行示例和最佳实践，并对于实际的操作原理和迁移流程进行说明，包含迁移后的精度和性能验证、调试方法说明。

#### 核心概念

- 推理业务昇腾迁移整体流程及工具链

图 6-74 推理业务昇腾迁移整体路径



推理业务昇腾迁移整体分为七个大的步骤，并以完整工具链覆盖全链路：

- a. 迁移评估：针对迁移可行性、工作量，以及可能的性能收益进行大致的预估。
- b. 环境准备：利用ModelArts提供的开发环境一键式准备好迁移、调测需要的运行环境与工具链。
- c. 模型适配：针对昇腾迁移模型必要的转换和改造。
  - i. 模型准备，导出和保存确定格式的模型。
  - ii. 转换参数准备，准备模型业务相关的关键参数。
  - iii. 模型转换，包含模型转换、优化和量化等。
- d. 应用集成。
  - i. 针对转换的模型运行时应用层适配。
  - ii. 数据预处理。
  - iii. 模型编排。
  - iv. 模型裁剪。
- e. 精度校验。
  - i. 精度对比误差统计工具。
  - ii. 自动化精度对比工具。
  - iii. 网络结构可视化工具。
- f. 性能调优。
  - i. 性能测试。
  - ii. 性能调优三板斧。
  - iii. 性能分析与诊断。
- g. 迁移测试报告。
  - i. 推理迁移验收表。

- **ModelArts开发环境**

ModelArts作为华为云上的AI开发平台，提供交互式云上开发环境，包含标准化昇腾算力资源和完整的迁移工具链，帮助用户完成昇腾迁移的调测过程，进一步可在平台上将迁移的模型一键部署成为在线服务向外提供推理服务，或者运行到自己的运行环境中。

- **MindSpore Lite**

华为自研的AI推理引擎，后端对于昇腾有充分的适配，模型转换后可以在昇腾上获得更好的性能，配合丰富的适配工具链，降低迁移成本，该工具在推理迁移工作的预置镜像已安装，可在镜像中直接使用（见[环境准备](#)）。关于MindSpore Lite详细介绍可参考[MindSpore Lite文档](#)。

## 6.4.2 昇腾迁移快速入门案例

ModelArts提供了两个昇腾迁移案例，方便您快速了解并完成昇腾迁移过程。

### 约束限制

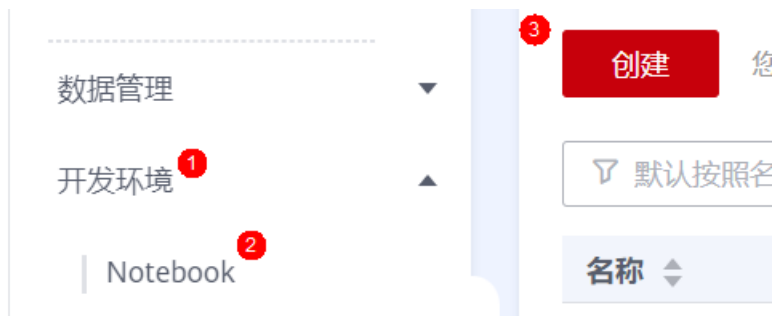
当前仅贵阳一区域支持选择本案例中的规格及镜像。

## 操作步骤

**步骤1** ModelArts管理控制台左侧导航栏中选择“开发环境 > Notebook”，进入“Notebook”管理页面。

**步骤2** 单击“创建”，进入“创建Notebook”页面。

图 6-75 实例创建入口



**步骤3** 请参见如下说明填写参数，并单击“立即创建”。

- 镜像：选择“公共镜像”，选择“mindspore\_2.2.0-cann\_7.0.1-py\_3.9-euler\_2.10.7-aarch64-snt9b”。
- 类型：Ascend。
- 规格：选择snt9b资源。
- 存储配置：云硬盘EVS。
- 磁盘规格：按照对应的存储使用情况可选择存储大小。
- SSH远程开发：如果需通过VS Code远程连接Notebook实例，可打开SSH远程开发，并选择自己的密钥对。

图 6-76 实例创建





**步骤4** 在Notebook列表，单击“操作列”的“打开”，打开Notebook示例。

图 6-77 运行实例

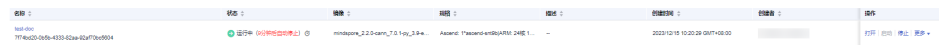
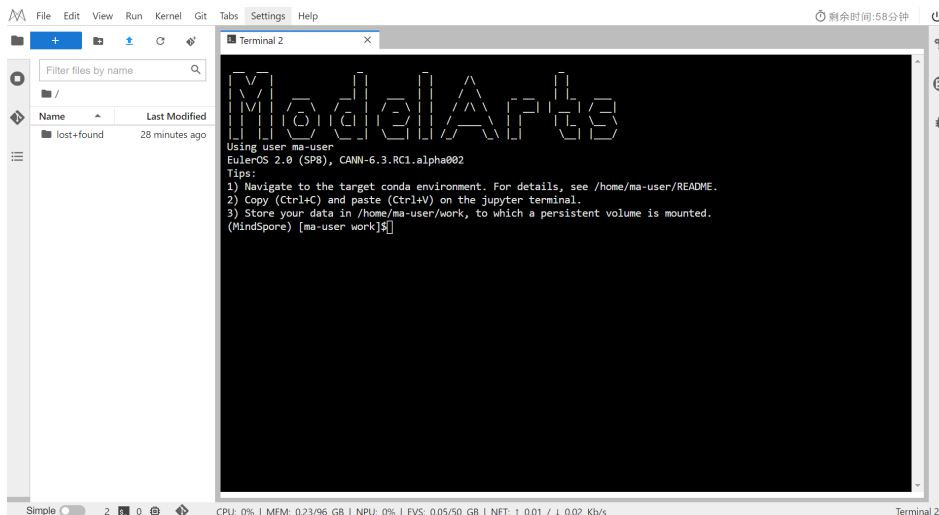


图 6-78 线上 Notebook 入口

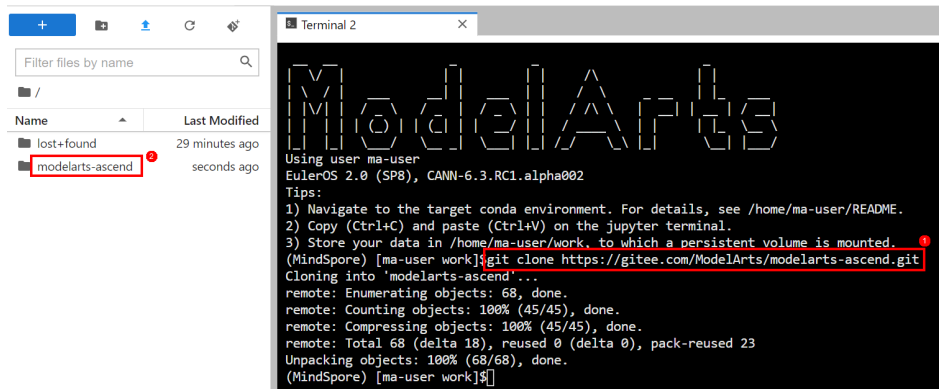


**步骤5** 克隆ModelArts Ascend代码库。

新建Terminal，执行下述命令将对应的repo克隆到Notebook实例。

```
git clone https://gitee.com/ModelArts/modelarts-ascend.git
```

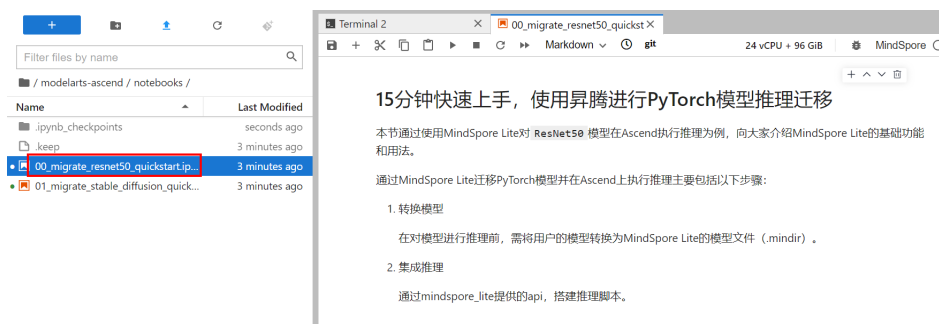
图 6-79 下载示例代码



**步骤6** 昇腾迁移案例在“~/work/modelarts-ascend/notebooks/”路径下，打开对应的“.ipynb”案例后运行即可。

- **ResNet50模型迁移到Ascend上进行推理**：通过使用MindSpore Lite对ResNet50模型在Ascend执行推理为例，向大家介绍MindSpore Lite的基础功能和用法。

图 6-80 ResNet50 模型迁移到 Ascend 上进行推理



- **Stable Diffusion模型迁移到Ascend上进行推理**：介绍如何将Stable Diffusion模型通过MSLite进行转换后，迁移在昇腾设备上运行。

图 6-81 Stable Diffusion 模型迁移到 Ascend 上进行推理



----结束

### 6.4.3 迁移评估

推理迁移包括模型迁移、业务迁移、精度性能调优等环节，是否能满足最终的迁移效果需要进行系统的评估。如果您仅需要了解迁移过程，可以先按照本文档的指导进行操作并熟悉迁移流程。如果您有实际的项目需要迁移，建议填写附录中的**推理业务迁移评估表**，并将该调研表提供给华为云技术支持人员进行迁移评估，以确保迁移项目能顺利实施。

### 6.4.4 环境准备

#### 迁移环境简介

ModelArts开发环境针对推理昇腾迁移的场景提供了云上可以直接访问的开发环境，具有如下优点：

- 利用云服务的资源使用便利性，可以直接使用到不同规格的昇腾设备。
- 通过指定对应的运行镜像，可以直接使用预置的、在迁移过程中所需的工具集，且已经适配到最新的版本可以直接使用。
- 开发者可以通过浏览器入口—Notebook方式访问，也可以通过VSCode远程开发的模式直接接入到云上环境中完成迁移开发与调测，最终生成适配昇腾的推理应用。

当前支持以下两种迁移环境搭建方式：

- ModelArts Standard：在Notebook中，使用预置镜像进行。

- ModelArts Lite DevServer: 在裸金属服务器中，自助配置好存储、安装固件、驱动、配置网络等。

## ModelArts Standard

ModelArts上昇腾规格如下。

表 6-1 昇腾规格

| 规格名称                                | 描述                                   |
|-------------------------------------|--------------------------------------|
| Ascend 1*ascend-snt9b ARM 24核 192GB | Snt9b单卡规格，配搭ARM处理器，适合深度学习场景下的模型训练和调测 |

ModelArts提供了面向推理迁移工作的预置镜像，其中包含了最新商用版驱动、昇腾软件开发库，迁移工具链等。预置镜像可以做到即开即用，用户也可以基于预置镜像构建自定义环境内容。

ModelArts支持的昇腾迁移预置镜像如下：

表 6-2 预置镜像

| 区域  | 镜像名称                                                         |
|-----|--------------------------------------------------------------|
| 贵阳一 | mindspore_2.2.0-cann_7.0.1-py_3.9-euler_2.10.7-aarch64-snt9b |
| 贵阳一 | mindspore_2.1.0-cann_6.3.2-py_3.7-euler_2.10.7-aarch64-snt9b |
| 贵阳一 | pytorch_1.11.0-cann_6.3.2-py_3.7-euler_2.10.7-aarch64-snt9b  |

可通过如下方式接入Notebook开发环境进行调试。

- JupyterLab: 在ModelArts管理控制台，直接打开Notebook示例的方式接入开发环境，详情请见[使用指导](#)。
- VS Code: 利用ModelArts插件，实现VS Code远程连接Notebook示例完成远程开发，详情请见[使用指导](#)。

下文将介绍如何在ModelArts Standard上使用预置镜像创建Notebook实例。

**步骤1** ModelArts管理控制台左侧导航栏中选择“开发环境 > Notebook”，进入“Notebook”管理页面。

**步骤2** 单击“创建”，进入“创建Notebook”页面。

图 6-82 实例创建入口



**步骤3** 请参见如下说明填写参数，并单击“立即创建”。

- 镜像：选择“公共镜像”，选择“mindspore\_2.2.0-cann\_7.0.1-py\_3.9-euler\_2.10.7-aarch64-snt9b”。
- 类型：Ascend。
- 规格：选择snt9b资源。
- 存储配置：云硬盘EVS。
- 磁盘规格：按照对应的存储使用情况可选择存储大小。
- SSH远程开发：如果需通过VS Code远程连接Notebook实例，可打开SSH远程开发，并选择自己的密钥对。

图 6-83 实例创建



**步骤4** 在Notebook列表，单击“操作列”的“打开”，打开Notebook示例。

图 6-84 运行实例

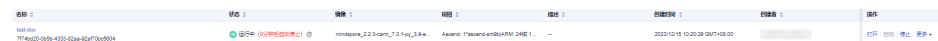
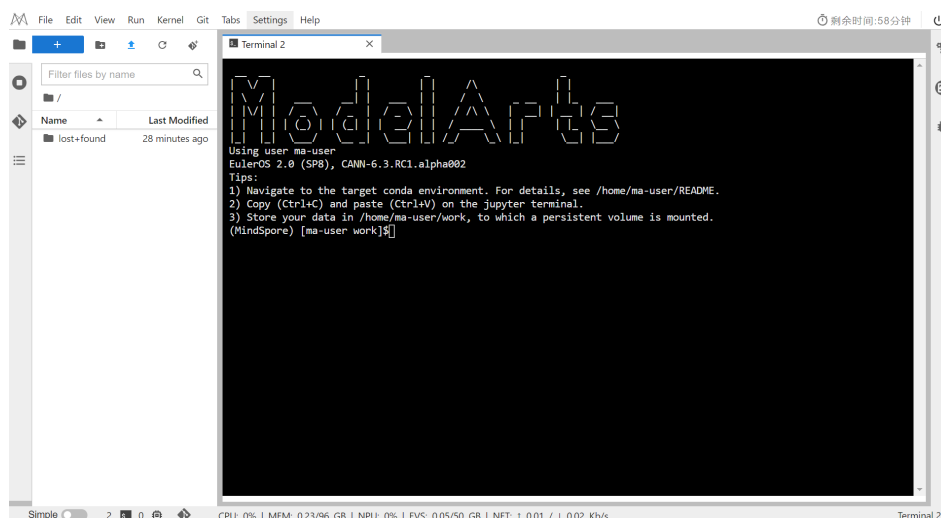


图 6-85 线上 Notebook 入口



---结束

## ModelArts Lite DevServer

开通裸金属服务器资源请见[DevServer资源开通](#)，在裸金属服务器上搭建迁移环境请见[裸金属服务器环境配置指导](#)。

## 6.4.5 模型适配

### 6.4.5.1 基于 MindSpore Lite 的模型转换

迁移推理业务的整体流程如下：

- [模型准备](#)
- [转换关键参数准备](#)
- [模型转换](#)
- [推理应用适配](#)

主要通过MindSpore Lite（简称MSLite）进行模型的转换，进一步通过MindSpore Runtime支持昇腾后端的能力来将推理业务运行到昇腾设备上。

## 模型准备

MindSpore Lite提供的模型convertor工具可以支持主流的模型格式到MindIR的格式转换，用户需要导出对应的模型文件，推荐导出为ONNX格式。

### 1. 如何导出ONNX模型

- PyTorch转ONNX，操作指导请见[此处](#)。
- PyTorch导出ONNX模型样例如下：

```
import torch
import torchvision
model = torchvision.models.resnet50(pretrained=True)
保存模型为ONNX格式
torch.onnx.export(model, torch.randn(1, 3, 224, 224), "resnet50.onnx")
```

- TensorFlow导出ONNX模型，操作指导请见[此处](#)。
2. 如何导出PTH模型
- PyTorch模型导出时需要包含模型的结构信息，需要利用jit.trace方式完成模型的导出与保存。

```
If you are instantiating the model with *from_pretrained* you can also easily set the TorchScript flag
model = BertModel.from_pretrained("bert-base-uncased", torchscript=True)

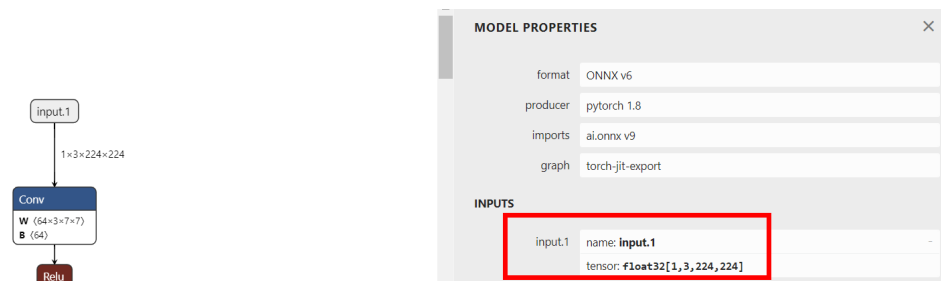
Creating the trace
traced_model = torch.jit.trace(model, [tokens_tensor, segments_tensors])
torch.jit.save(traced_model, "traced_bert.pt")
```

## 转换关键参数准备

对应的模型转换成MindIR格式，通过后端绑定的编译形式来运行以达到更好的性能（类似静态图的运行模式），所以需要提前准备以下几个重点参数。

1. 输入的inputShape，包含batch信息。  
MSLite涉及到编译优化的过程，不支持完全动态的权重模式，需要在转换时确定对应的inputShape，用于模型的格式的编译与转换，可以在[netron官网](#)进行查看，或者对于模型结构中的输入进行shape的打印，并明确输入的batch。  
一般来说，推理时指定的inputShape是和用户的业务及推理场景是紧密相关的，可以通过原始模型推理脚本或者网络模型进行判断。需要把Notebook中的模型下载到本地后，再放入netron官网中，查看其inputShape。  
如果netron中没有显示inputShape，可能由于使用了动态shape模型导致，请确保使用的是静态shape模型，静态shape模型文件导出方法请参考[模型准备](#)。

图 6-86 netron 中查看 inputShape



2. 精度选择。  
精度选择需要在模型转换阶段进行配置，执行converter\_lite命令式通过--configFile参数指定配置文件路径，配置文件通过precision\_mode参数指定精度模式。可选的参数有"enforce\_fp32", "preferred\_fp32", "enforce\_fp16", "enforce\_origin"或者"preferred\_optimal", 默认为"enforce\_fp16"

```
[ascend_context]
precision_mode= preferred_fp32
```

## 模型转换

在ModelArts开发环境中，通过对应的转换预置镜像，直接执行对应的转换过程，对应的转换和评估工具都已经预置了最新版本，详细介绍请见[使用说明](#)。inputShape查看方法请见[转换关键参数准备](#)。

```
!converter_lite --modelFile=resnet50.onnx --fmk=ONNX --outputFile=resnet50 --saveType=MINDIR --inputShape="input.1:1,3,224,224" --device=Ascend
```

## 推理应用适配

MindSpore Lite提供了JAVA/C++/Python API，进行推理业务的适配，并且在构建模型时，通过上下文的参数来确定运行时的具体配置，例如运行后端的配置等。下文以Python接口为例。

使用MindSpore Lite推理框架执行推理并使用昇腾后端主要包括以下步骤：

- 创建运行上下文：创建**Context**，保存需要的一些基本配置参数，用于指导模型编译和模型执行，在昇腾迁移时需要特别指定target为“Ascend”，以及对应的device\_id。

```
context = mslite.Context()
context.target = ["ascend"]
context.ascend.device_id = 0
```

- 模型加载与编译：执行推理之前，需要调用**Model**的**build\_from\_file**接口进行模型加载和模型编译。模型加载阶段将文件缓存解析成运行时的模型。模型编译阶段会耗费较多时间所以建议Model创建一次，编译一次，多次推理。

```
model = mslite.Model()
model.build_from_file("./resnet50.mindir", mslite.ModelType.MINDIR, context)
```

- 输入数据：编译后的模型提供了predict接口用户执行模型推理任务，Inputs输入为List Tensor，这里的Tensor是MSLite的概念，具体的列表长度和tensor类型由转换时的InputShape来确定，由于后端指定了ascend，这些tensor都是在昇腾设备的显存中，用户需要在对应的tensor中填入数据，这些数据也会被搬移到显存中，进一步对于Inputs输入的内容进行处理。

```
data = convert_img(input_image)
in_data = [np.array(data)]
inputs = model.get_inputs()
for i, _input in enumerate(inputs):
 _input.set_data_from_numpy(in_data[i])
```

- 执行推理：使用**Model**的**predict**进行模型推理，返回值为Outputs，也是List Tensor类型，具体的长度和类别由模型定义，对应的Tensor数据由于指定了ascend后端，Output的内容在显存中，通过tesnor的get\_data\_to\_numpy方法来获取，并将数据读取到内存中使用

```
outputs = model.predict(inputs)
outputs = [output.get_data_to_numpy() for output in outputs]
```

更多Python接口的高级用法与示例，请参考[Python API](#)。

### 6.4.5.2 动态 shape

在某些推理场景中，模型输入的shape可能是不固定的，因此需要支持用户指定模型的动态shape，并能够在推理中接收多种shape的输入。在CPU上进行模型转换时无需考虑动态shape问题，因为CPU算子支持动态shape；而在Ascend场景上，算子需要指定具体的shape信息，并且在模型转换的编译阶段完成对应shape的编译任务，从而能够在推理时支持多种shape的输入。

### 动态 batch

在模型转换阶段通过--configFile参数指定配置文件，并且在配置文件中配置input\_shape及dynamic\_dims动态参数。其中input\_shape的-1表示动态shape所在的维度，dynamic\_dims指定动态维度的取值范围，比如“[1~4],[8],[16]”表示该动态维度支持1、2、3、4、8、6共六种大小。

```
config.ini
[ascend_context]
input_shape=input.1:[-1,3,224,224]
dynamic_dims=[1~4],[8],[16]
```



在执行convert\_lite命令时，指定--configFile=config.ini即可自动编译指定的动态shape。

```
#shell
converter_lite --modelFile=resnet50.onnx --fmk=ONNX --device=Ascend --outputFile=resnet50_dynamic --
saveType=MINDIR --configFile=config.ini
```

**注意：**推理应用开发时，需要使用模型的Resize功能，改变输入的shape。而且Resize操作需要在数据从host端复制到device端之前执行，下面是一个简单的示例，展示如何在推理应用时使用动态Shape。

```
import mindspore_lite as mslite
import numpy as np
from PIL import Image
设置目标设备上下文为Ascend，指定device_id为0
context = mslite.Context()
context.target = ["ascend"]
context.ascend.device_id = 0
构建模型
model = mslite.Model()
model.build_from_file("./resnet50_dynamic.mindir", mslite.ModelType.MINDIR, context)
data = np.random.rand(8, 3, 224, 224).astype(np.float32)
inputs = model.get_inputs()
model.resize(inputs, [list(data.shape)])
inputs[0].set_data_from_numpy(data)
前向推理，并将结果从device侧传到host侧
outputs = model.predict(inputs)[0].get_data_to_numpy()
print(outputs.shape) # (8, 1000)
```

## 动态分辨率

动态分辨率可以用于设置输入图片的动态分辨率参数。适用于执行推理时，每次处理图片宽和高不固定的场景，该参数需要与input\_shape配合使用，input\_shape中-1的位置为动态分辨率所在的维度。使用方法可参考[Ascend配置文件说明](#)。

### 6.4.6 精度校验

转换模型后执行推理前，可以使用benchmark工具对MindSpore Lite云侧推理模型进行基准测试。它不仅可以对MindSpore Lite云侧推理模型前向推理执行耗时进行定量分析（性能），还可以通过指定模型输出进行可对比的误差分析（精度）。

## 精度测试

benchmark工具用于精度验证，主要工作原理是：固定模型的输入，通过benchmark工具进行推理，并将推理得到的输出与标杆数据进行相似度度量（余弦相似度和平均相对误差），得到模型转换后的精度偏差信息。使用benchmark进行精度比对的基本流程如下：

1. 将模型输入保存二进制文件。

```
数据读取，预处理
image = img_preprocess(image_path)
image = np.array(image, dtype=np.float32)
image = np.frombuffer(image.tobytes(), np.float32)
保存网络输入为二进制文件
image.tofile("input_data.bin")
```

2. 将基准模型的输出保存到文本文件。

本例中输出节点名称为output\_node\_name，输出节点的shape为“(1, 1000)”，因此一共有两维，对应的输出文件为“output\_node\_name 2 1 1000”，再加上输出的值即可。

```
基于原始pth模型前向推理
output = model_inference(input_data)
```

```
保存网络输出节点名称、维度、shape及输出到本地文件
with open("output_data.txt", "w") as f:
 f.write("output_node_name 2 1 1000\n")
 f.write(" ".join([str(i) for i in output]))
```

3. 使用benchmark工具进行精度对比。

```
#shell
benchmark --modelFile=model.mindir --inputShapes=1,3,224,224 --inDataFile=input_data.bin --
device=Ascend --benchmarkDataFile=output_data.txt --accuracyThreshold=5 --
cosineDistanceThreshold=0.99
```

其中, --accuracyThreshold=5表示平均绝对误差的容忍度最大为5%, --cosineDistanceThreshold =0.99表示余弦相似度至少为99%, --inputShapes可将模型放入到[netron官网](#)中查看。

图 6-87 benchmark 对接结果输出示例图

```
MarkAccuracy
InData 0: -0.559551 -0.559551 -0.508177 -0.782173 -0.422553 0.211063 0.330936 -0.0458888 -0.217056 -0.251306 0.348061 0.125439 0.142564 -0.371179 0.262437 -0.525302 -0.62805 -0.542427 -0.525302 -0.131433
----- Comparing Output data -----
Data of node 495 : 1.73535 -0.799316 0.40332 -0.526367 -2.2832 -0.32666 -1.96484 -0.309326 -0.524902 -1.40625 -2.53125 0.010025 -1.91797 -3.63281 0.98584 -3.35547 -2.19922 -3.04492 -1.16699 -3.12891 0.322266 -1.2041 -0.265625 1.20312 -1.43555 2.54492 -2.02539 -1.69434 -0.932129 -1.88672 -2.37109 -0.712402 -1.66602 0.773438 0.3396 -0.0042383 1.9209 -0.0312347 -2.23633 -0.97998 -3.23047 -3.54883 -3.17383 -3.23828 -2.72656 0.18811 -2.19727 -1.21387 1.15723 1.97266
Mean bias of node/tensor 495 : 0.645113%
Mean bias of all nodes/tensors: 0.645113%
----- Comparing Output data -----
Data of node 495 : 1.73535 -0.799316 0.40332 -0.526367 -2.2832 -0.32666 -1.96484 -0.309326 -0.524902 -1.40625 -2.53125 0.010025 -1.91797 -3.63281 0.98584 -3.35547 -2.19922 -3.04492 -1.16699 -3.12891 0.322266 -1.2041 -0.265625 1.20312 -1.43555 2.54492 -2.02539 -1.69434 -0.932129 -1.88672 -2.37109 -0.712402 -1.66602 0.773438 0.3396 -0.0042383 1.9209 -0.0312347 -2.23633 -0.97998 -3.23047 -3.54883 -3.17383 -3.23828 -2.72656 0.18811 -2.19727 -1.21387 1.15723 1.97266
Mean cosine distance of node/tensor 495 : 99.9999%
Cosine distance of all nodes/tensors: 0.999999403953552
```

## 自动精度对比

在某些场景下, 比如算子溢出、误差累积等都可能会导致模型转换前后的模型存在误差, 通过[精度测试](#)节的精度校验工具可以度量模型输出的精度误差的大小。当误差较大时, 可以使用精度对比工具对比转换前后的ONNX模型和OM模型。其中OM模型在使用converter\_lite工具进行模型转换时会同步生成。

```
shell
cd /usr/local/Ascend/ascend-toolkit/latest/tools/msquickcmp
mkdir -p ~/work/output
python main.py -m ~/work/resnet50.onnx -om ~/work/resnet50.om -o ~/work/output --input-shape
"input.1:1,3,224,224"
```

精度对比命令执行成功后, 将会在指定的输出目录中生成result\_{timestamp}.csv文件。

图 6-88 精度对比生成文件

/ output / 20230625200320 /

| Name                      | Last Modified |
|---------------------------|---------------|
| dump_data                 | 13 hours ago  |
| input                     | 13 hours ago  |
| model                     | 13 hours ago  |
| result_20230625200337.csv | 13 hours ago  |

打开CSV文件后可以通过CosineSimilarity列和MaxAbsoluteError列排查第一个数值发生突变的行, 这种情况一般表明: 该突变行对应的Ascend算子和ONNX算子的执行结果存在较大差异, 从而将排查重点锁定在对应的算子中。

图 6-89 执行结果

| #     | A      | B         | C                               | D       | E           | F                                  | G           | H                       | I                | J                | K        | L |
|-------|--------|-----------|---------------------------------|---------|-------------|------------------------------------|-------------|-------------------------|------------------|------------------|----------|---|
| Index | OpType | NPUDump   | DataTy                          | Address | GroundTruth | DataTy                             | TensorIndex | Shape                   | CosineSimilarity | MaxAbsoluteError | Accum    | R |
| 117   | 110    | Conv2D    | /conv1/Conv/relu/Relu           | float16 | 2.01E+13    | /conv1/Conv/relu/Relu              | float32     |                         | 0.001355         | 554.8636         |          |   |
| 118   | 111    | MaxPoolV3 | /maxpool/MaxPool                | float16 | 2.01E+13    | /maxpool/MaxPool                   | float32     |                         | 0.001355         | 554.8636         |          |   |
| 119   | 111    | MaxPoolV3 | /maxpool/MaxPool                | float16 | 2.01E+13    | /maxpool/MaxPool                   | float32     |                         | 0.001355         | 60.18948         |          |   |
| 120   | 112    | Conv2D    | /layer1/layer1.0/downsample/d   | float16 | 2.01E+13    | /layer1/layer1.0/downsample/down   | float32     |                         | 0.001355         | 60.18948         |          |   |
| 123   | 112    | Conv2D    | /layer1/layer1.0/downsample/d   | float16 | 2.01E+13    | /layer1/layer1.0/downsample/down   | float32     |                         | 0.002095         | 8587.116         |          |   |
| 124   | 113    | Conv2D    | /layer1/layer1.0/conv1/Conv/iaj | float16 | 2.01E+13    | /layer1/layer1.0/conv1/Conv/layer1 | float32     |                         | 0.001355         | 60.18948         |          |   |
| 127   | 113    | Conv2D    | /layer1/layer1.0/conv1/Conv/iaj | float16 | 2.01E+13    | /layer1/layer1.0/conv1/Conv/layer1 | float32     |                         | 0.000725         | 560.5277         |          |   |
| 128   | 114    | Conv2D    | /layer1/layer1.0/conv2/Conv/iaj | float16 | 2.01E+13    | /layer1/layer1.0/conv2/Conv/layer1 | float32     |                         | 0.000725         | 560.5277         |          |   |
| 131   | 114    | Conv2D    | /layer1/layer1.0/conv2/Conv/iaj | float16 | 2.01E+13    | /layer1/layer1.0/conv2/Conv/layer1 | float32     |                         | 0.000888         | 298.3357         |          |   |
| 132   | 115    | Conv2D    | /layer1/layer1.0/conv3/Conv/iaj | float16 | 2.01E+13    | /layer1/layer1.0/conv3/Conv/layer1 | float32     |                         | 0.000888         | 298.3357         |          |   |
| 135   | 115    | Conv2D    | /layer1/layer1.0/conv3/Conv/iaj | float16 | 2.01E+13    | /layer1/layer1.0/conv3/Conv/layer1 | float32     |                         | 0.002095         | 8587.116         |          |   |
| 136   | 115    | Conv2D    | /layer1/layer1.0/conv3/Conv/iaj | float16 | 2.01E+13    | /layer1/layer1.0/conv3/Conv/layer1 | float32     |                         | 0.002163         | 2484.736         |          |   |
| 137   | 116    | Conv2D    | /layer1/layer1.1/conv1/Conv/iaj | float16 | 2.01E+13    | /layer1/layer1.1/conv1/Conv/layer1 | float32     |                         | 0.002163         | 2484.736         |          |   |
| 140   | 116    | Conv2D    | /layer1/layer1.1/conv1/Conv/iaj | float16 | 2.01E+13    | /layer1/layer1.1/conv1/Conv/layer1 | float32     |                         | 0.001353         | 646.2149         |          |   |
| 141   | 117    | Conv2D    | /layer1/layer1.1/conv2/Conv/iaj | float16 | 2.01E+13    | /layer1/layer1.1/conv2/Conv/layer1 | float32     |                         | 0.001353         | 646.2149         |          |   |
| 144   | 117    | Conv2D    | /layer1/layer1.1/conv2/Conv/iaj | float16 | 2.01E+13    | /layer1/layer1.1/conv2/Conv/layer1 | float32     |                         | 0.001664         | 562.9119         |          |   |
| 145   | 118    | Conv2D    | /layer1/layer1.1/conv3/Conv/iaj | float16 | 2.01E+13    | /layer1/layer1.1/conv3/Conv/layer1 | float32     |                         | 0.001664         | 562.9119         |          |   |
| 148   | 118    | Conv2D    | /layer1/layer1.1/conv3/Conv/iaj | float16 | 2.01E+13    | /layer1/layer1.1/conv3/Conv/layer1 | float32     |                         | 0.002163         | 2484.736         |          |   |
| 149   | 118    | Conv2D    | /layer1/layer1.1/conv3/Conv/iaj | float16 | 2.01E+13    | /layer1/layer1.1/conv3/Conv/layer1 | float32     |                         | 0.002357         | 2643.976         |          |   |
| 150   | 119    | Conv2D    | /layer1/layer1.2/conv1/Conv/iaj | float16 | 2.01E+13    | /layer1/layer1.2/conv1/Conv/layer1 | float32     |                         | 0.002357         | 2643.976         |          |   |
| 153   | 119    | Conv2D    | /layer1/layer1.2/conv1/Conv/iaj | float16 | 2.01E+13    | /layer1/layer1.2/conv1/Conv/layer1 | float32     |                         | 0.002458         | 1824.055         |          |   |
| 154   | 120    | Conv2D    | /layer1/layer1.2/conv2/Conv/iaj | float16 | 2.01E+13    | /layer1/layer1.2/conv2/Conv/layer1 | float32     |                         | 0.002458         | 1824.055         |          |   |
| 157   | 120    | Conv2D    | /layer1/layer1.2/conv2/Conv/iaj | float16 | 2.01E+13    | /layer1/layer1.2/conv2/Conv/layer1 | float32     |                         | 0.00262          | 1375.012         |          |   |
| 158   | 121    | Conv2D    | /layer1/layer1.2/conv3/Conv/iaj | float16 | 2.01E+13    | /layer1/layer1.2/conv3/Conv/layer1 | float32     |                         | 0.00262          | 1375.012         |          |   |
| 161   | 121    | Conv2D    | /layer1/layer1.2/conv3/Conv/iaj | float16 | 2.01E+13    | /layer1/layer1.2/conv3/Conv/layer1 | float32     |                         | 0.002357         | 2643.976         |          |   |
| 162   | 121    | Conv2D    | /layer1/layer1.2/conv3/Conv/iaj | float16 | 2.01E+13    | /layer1/layer1.2/conv3/Conv/layer1 | float32     |                         | 0.003499         | 3222.975         |          |   |
| 163   | 122    | Conv2D    | /layer2/layer2.0/conv1/Conv/iaj | float16 | 2.01E+13    | /layer2/layer2.0/conv1/Conv/layer2 | float32     | /layer2/iaj[1,256,56,1] | 0.999999         | 0.003499         | 3222.975 |   |
| 166   | 122    | Conv2D    | /layer2/layer2.0/conv1/Conv/iaj | float16 | 2.01E+13    | /layer2/layer2.0/conv1/Conv/layer2 | float32     | /layer2/iaj[1,128,56,1] | 0.999997         | 0.003788         | 2983.306 |   |
| 167   | 123    | Conv2D    | /layer2/layer2.0/conv2/Conv/iaj | float16 | 2.01E+13    | /layer2/layer2.0/conv2/Conv/layer2 | float32     | /layer2/iaj[1,128,56,1] | 0.999997         | 0.003788         | 2983.306 |   |
| 170   | 123    | Conv2D    | /layer2/layer2.0/conv2/Conv/iaj | float16 | 2.01E+13    | /layer2/layer2.0/conv2/Conv/layer2 | float32     | /layer2/iaj[1,128,28,1] | 0.999998         | 0.002365         | 671.003  |   |
| 171   | 124    | Conv2D    | /layer2/layer2.0/conv3/Conv     | float16 | 2.01E+13    | /layer2/layer2.0/conv3/Conv        | float32     | /layer2/iaj[1,128,28,1] | 0.999998         | 0.002365         | 671.003  |   |
| 174   | 124    | Conv2D    | /layer2/layer2.0/conv3/Conv     | float16 | 2.01E+13    | /layer2/layer2.0/conv3/Conv        | float32     | /layer2/iaj[1,512,28,1] | 0.999997         | 0.004326         | 8056.16  |   |
| 175   | 125    | Conv2D    | /layer2/layer2.0/downsample/d   | float16 | 2.01E+13    | /layer2/layer2.0/downsample/down   | float32     | /layer2/iaj[1,256,56,1] | 0.999999         | 0.003499         | 3222.975 |   |

如下图所示，最大绝对误差在295行发生了突变，且突变值约为65504，说明softmax算子输出的结果发生了溢出（FP16的最大值为65504），需要重点分析softmax算子为什么会执行出错，也可以联系华为工程师进行分析。

图 6-90 最大绝对误差

| #   | Index | OpType      | NPUDump                         | DataTy  | Ground    | DataTy  | TensorIndex                            | Shape         | CosineSimilarity | MaxAbsoluteError |
|-----|-------|-------------|---------------------------------|---------|-----------|---------|----------------------------------------|---------------|------------------|------------------|
| 290 | 250   | BatchMatMul | MatMul_52Add_97                 | float16 | Add_97.M  | float32 | MatMul_52Add_97.input0                 | [32,200,64]   | 1                | 0.000106         |
| 291 | 250   | BatchMatMul | MatMul_52Add_97                 | float16 | Add_97.M  | float32 | MatMul_52Add_97.input1                 | [32,64,200]   | 1                | 0.001112         |
| 292 | 250   | BatchMatMul | MatMul_52Add_97                 | float32 | Add_97.M  | float32 | MatMul_52Add_97.input2                 | [32,200,200]  | 1                | 0                |
| 293 | 250   | BatchMatMul | MatMul_52Add_97                 | float32 | Add_97.M  | float32 | MatMul_52Add_97.output0                | [32,200,200]  | 1                | 0                |
| 294 | 251   | SoftmaxV2   | Softmax_99trans_Cast_32         | float32 | Softmax_9 | float32 | Softmax_99trans_Cast_32.input0         | [32,200,200]  | 1                | 0                |
| 295 | 251   | SoftmaxV2   | Softmax_99trans_Cast_32         | float16 | Softmax_9 | float32 | Softmax_99trans_Cast_32.output0        | [32,200,200]  | 1                | 65503.995        |
| 296 | 252   | BatchMatMul | MatMul_100                      | float16 | MatMul_1  | float32 | MatMul_100.input0                      | [32,200,200]  | 1                | 65503.995        |
| 297 | 252   | BatchMatMul | MatMul_100                      | float16 | MatMul_1  | float32 | MatMul_100.input1                      | [32,200,64]   | 1                | 0.000579         |
| 298 | 252   | BatchMatMul | MatMul_100                      | float16 | MatMul_1  | float32 | MatMul_100.output0                     | [32,200,64]   | 1                | 65503.99501      |
| 299 | 253   | TransData   | trans_Cast_39trans_TransData_36 | float16 | *         | float32 | trans_Cast_39trans_TransData_36.input  | [32,200,64]   | 0.748848         | 65503.99501      |
| 300 | 253   | TransData   | trans_Cast_39trans_TransData_36 | float16 | *         | float32 | trans_Cast_39trans_TransData_36.output | [1,32,200,64] | 0.748848         | 65503.99501      |

## 6.4.7 性能调优

### 性能测试

benchmark工具也可用于性能测试，其主要的测试指标为模型单次前向推理的耗时。在性能测试任务中，与精度测试不同，并不需要用户指定对应的输入（inDataFile）和输出的标杆数据（benchmarkDataFile），benchmark工具会随机生成一个输入进行推理，并统计推理时间。执行的示例命令行如下。

```
#shell
benchmark --modelFile=resnet50.mindir --device=Ascend
```

在某些推理场景中，模型输入的shape可能是不固定的，因此需要支持用户指定模型的动态shape，并能够在推理中接收多种shape的输入。在CPU上进行模型转换时无需考虑动态shape问题，因为CPU算子支持动态shape；而在昇腾场景上，算子需要指定具体的shape信息，并且在模型转换的编译阶段完成对应shape的编译任务，从而能够在推理时支持多种shape的输入。

绝大多数情况下，昇腾芯片推理性能相比于CPU会好很多，但是也可能会遇到和CPU推理性能并无太大差别甚至出现劣化的情况。造成这种情况的原因可能有如下几种：

1. 模型中存在大量的类似于Pad或者Strided\_Slice等算子，其在CPU和Ascend上的实现方法存在差异（硬件结构不同），后者在运算此类算子时涉及到数组的重排，性能较差；

2. 模型的部分算子在昇腾上不支持，或者存在Transpose操作，会导致模型切分为多个子图，整体的推理耗时随着子图数量的增多而增长；
3. 模型没有真正的调用昇腾后端，而是自动切换到了CPU上执行，这种情况可以通过输出日志来进行判断。

## 自助性能调优三板斧

基于上一步完成的性能测试，为了最大化模型推理性能，首先确保当前使用的CANN版本是最新版本（最新版本请见[此处](#)），每个迭代的CANN版本都有一定的性能收益。在此基础上，可以进行三板斧自助工具式性能调优。这些调优过程由大量的项目交付经验总结，帮助您获得模型最佳推理性能，重复[性能测试](#)章节可以验证对应的收益情况。

自助性能调优三板斧分别为：[通过固定shape获取更好的常量折叠](#)、[AOE性能自动调优](#)、[自动高性能算子生成工具](#)。

- **通过固定shape获取更好的常量折叠**

在MindIR格式转换时（即执行converter\_lite命令时），通过指定具体的静态shape，并且打开--optimize参数指定“ascend\_oriented”能够获得更好的常量折叠优化效果。inputShape查看方法请见[转换关键参数准备](#)。

```
Ascend Optimization Engine
converter_lite --modelFile=resnet50.onnx --fmk=ONNX --outputFile=resnet50 --saveType=MINDIR --inputShape="input.1:1,3,224,224" --optimize=ascend_oriented
```

常量折叠是编译器优化中的通用技术之一，在编译节点简化常量表达。通过多数的现代编译器不会真的产生两个乘法的指令再将结果存储下来，取而代之的是会识别出语句的结构，并在编译时期将数值计算出来而不是运行时去计算（在本例子，结果为2,048,000）。

```
i = 320 * 200 * 32;
```

AI编译器中，常量折叠是将计算图中预先可以确定输出值的节点替换成常量，并对计算图进行一些结构简化的操作，例如ADDN操作，以及在推理过程中的batch normalization操作等。

以BN折叠为例，如下表示折叠后获得的性能收益。

图 6-91 BN 折叠下前向运算性能收益

| 模型             | CPU 前向时间 | GPU 前向时间 |
|----------------|----------|----------|
| Resnet50 (合并前) | 176.17ms | 11.03ms  |
| Resnet50 (合并后) | 161.69ms | 7.3ms    |
| 提升             | ~8%      | ~34%     |

- **AOE性能自动调优**

自动性能调优工具AOE(Ascend Optimization Engine)，可以对于模型的图和算子运行通过内置的知识库进行自动优化，以提升模型的运行效率。开启AOE调优后，模型转换时会自动进行性能调优操作，该过程耗时较长，可能需要数小时。

AOE性能自动优化在模型转换阶段进行配置（即执行converter\_lite命令时），通过--configFile参数指定配置文件aoe\_config.ini，配置文件通过aoe\_mode参数指定调优模式。可选值有：

- “subgraph tuning”：子图调优。
- “operator tuning”：算子调优。

- “subgraph tuning, operator tuning”：先进行子图调优，再进行算子调优。

推荐先进行子图调优，再进行算子调优，因为先进行子图调优会生成图的切分方式，子图调优后算子已经被切分成最终的shape了，再进行算子调优时，会基于这个最终shape去做算子调优。如果优先算子调优，这时调优的算子shape不是最终切分后的算子shape，不符合实际使用场景。

本例同时指定了子图调优和算子调优，工具会先进行子图调优，再进行算子调优。

```
aoe_config.ini
[ascend_context]
aoe_mode="subgraph tuning, operator tuning"
```

指定--configFile=aoe\_config.ini即可自动进行性能优化。

```
#shell
converter_lite --modelFile=resnet50.onnx --fmk=ONNX --device=Ascend --outputFile=resnet50_aoe --saveType=MINDIR --configFile=aoe_config.ini
```

命令执行成功后，性能自动优化前后的性能对比会打印到控制台上，同时会生成更为详细的json格式调优报告。

图 6-92 自动调优输出文件

```
📄 aoe_result_opat_20230504193536546863_pid105831.json
📄 aoe_result_sgat_20230428143248403871_pid24201.json
```

需要注意的是，并不是所有的模型使用性能自动调优都是有收益的，在本例中，ResNet50模型自动调优收益甚微（模型转换时已经做了部分针对性优化），在有些比较复杂的模型场景下可能会有较好的收益。比如VAE\_ENCODER模型使用算子调优收益为11.15%。

图 6-93 VAE\_ENCODER 模型使用 AOE 自动调优在屏幕上显示日志

```
Start to subgraph tuning
.....[Aoe][vae_encoder_aoe] Model tuning process finished. No performance improvement.
[Aoe]Aoe process finished, cost time 152 s.

Start to operator tuning
.....[Aoe][vae_encoder_aoe] Operator tuning process finished. Performance improved by 11.15%
[Aoe]Aoe process finished, cost time 2353 s.
```



图 6-94 AOE 自动调优的输出样例

```
▼ root: [] 2 items
 ▼ 0:
 ► basic:
 ▼ 1:
 ▼ OPAT:
 model_baseline_performance(ms): 23.059152
 model_performance_improvement: "11.15%"
 model_result_performance(ms): 20.746701
 opat_tuning_result: "tuning successful"
 ▼ repo_modified_operators:
 ► add_repo_operators: [] 19 items
 ▼ repo_summary:
 repo_add_num: 19
 repo_hit_num: 3
 repo_reserved_num: 3
 repo_unsatisfied_num: 5
 repo_update_num: 0
 total_num: 27
```

其中：

- model\_baseline\_performance表示调优前模型执行时间，单位为ms。
- model\_performance\_improvement表示调优后模型执行时间减少百分比。
- model\_result\_performance表示调优后模型执行时间。
- repo\_summary中的信息表示调优过程中使用到的知识库算子个数或者追加到知识库的算子个数。

AOE自动调优更多介绍可参考[Ascend转换工具功能说明](#)。

#### ● 自动高性能算子生成工具

自动高性能算子生成工具AKG(Auto Kernel Generator)，可以对神经网络模型中的算子进行优化，并提供特定模式下的算子自动融合功能，可提升在昇腾硬件后端上运行模型的性能。

AKG的配置也是在模型转换阶段进行配置（即执行converter\_lite命令时），通过指定对应的配置文件akg.cfg，设置对应的akg优化级别，并且在模型转换时参考样例进行对应的配置。

```
akg.cfg
[graph_kernel_param]
opt_level=2
```

执行命令：

```
shell
converter_lite --fmk=ONNX --modelFile=model.onnx --outputFile=model --configFile=akg.cfg --
optimize=ascend_oriented
```

自动高性能算子生成工具AKG更多介绍可参考[图算融合配置说明](#)和[MindSpore AKG](#)。

## 6.4.8 迁移过程使用工具概览

基础的开发工具在迁移的预置镜像和开发环境中都已经进行预置，用户原则上不需要重新安装和下载，如果预置的版本不满足要求，用户可以执行下载和安装与覆盖操作。

## 模型转换工具

离线转换模型功能的工具**MSLite Convertor**，支持onnx、pth、tensorflowLite多种类型的模型转换，转换后的模型可直接运行在MindSpore运行时后端，用于昇腾推理。

## 精度性能检查工具

**Benchmark**精度检查工具，可以转换模型后执行推理前，使用其对MindSpore Lite模型进行基准测试，它不仅可以对MindSpore Lite模型前向推理执行耗时进行定量分析（性能），还可以通过指定模型输出进行可对比的误差分析（精度）。

## 模型自动调优工具

**AOE**(Ascend Optimization Engine)是一个昇腾设备上模型运行自动调优工具，作用是充分利用有限的硬件资源，以满足算子和整网的性能要求。在推理场景下使用，可以对于模型的图和算子运行内置的知识库进行自动优化，以提升模型的运行效率。

## 自动高性能算子生成工具 AKG

**AKG**(Auto Kernel Generator)对神经网络中的算子进行优化，并提供特定模式下的算子自动融合功能。提升在昇腾硬件后端上运行网络的性能。

AKG由三个基本的优化模块组成：规范化、自动调度和后端优化。

- 规范化：为了解决polyhedral表达能力的局限性（只能处理静态的线性程序），需要首先对计算公式IR进行规范化。规范化模块中的优化主要包括自动运算符inline、自动循环融合和公共子表达式优化等。
- 自动调度：自动调度模块基于polyhedral技术，主要包括自动向量化、自动切分、thread/block映射、依赖分析和数据搬移等。
- 后端优化：后端优化模块的优化主要包括TensorCore使能、双缓冲区、内存展开和同步指令插入等。

## 性能分析工具

**msprof**命令行工具提供了采集通用命令以及AI任务运行性能数据、昇腾AI处理器系统数据、Host侧系统数据和采集和解析能力。面向推理的场景，可以对于模型的性能数据进行收集，可基于收集的性能数据进行性能分析。

## 6.4.9 常见问题

### 6.4.9.1 MindSpore Lite 问题定位指南

在使用MindSpore Lite过程中遇到问题时，可参考MindSpore Lite官网提供的[问题定位指南](#)进行问题定位。

### 6.4.9.2 模型转换报错如何查看日志和定位？

通过如下的配置项打开对应的模型转换日志，可以看到更底层的报错。如配置以下的环境变量之后，再重新转换模型，导出对应的日志和dump图进行分析：

1. 报错日志中搜到“not support onnx data type”，表示MindSpore暂不支持该算子。



- 报错日志中搜到“Convert graph to om failed”，表示CANN模块进行图编译存在保存，需要结合CANN的报错日志和dump图进行具体分析。

配置方式参考如下：

- 打开DEBUG日志。

- 设置MindSpore日志环境变量。  
export GLOG\_v=0  
# 0-DEBUG、1-INFO、2-WARNING、3-ERROR
- 设置CANN日志环境变量。  
# 0：表示DEBUG。1：表示INFO。2：表示WARNING。3：表示ERROR。4：表示NONE。  
export ASCEND\_GLOBAL\_LOG\_LEVEL=1  
# 表示日志打印  
export ASCEND\_SLOG\_PRINT\_TO\_STDOUT=1

- DUMP模型转换中间图。

设置DUMP中间图环境变量。

- # 1：表示dump图全部内容。2：表示不dump权重数据的基础图。3：表示只dump节点关系的精简图。  
export DUMP\_GE\_GRAPH=2
- # 1：表示dump图所有图。2：表示dump除子图外的所有图。3：表示只dump最后一张图。  
export DUMP\_GRAPH\_LEVEL=2

### 6.4.9.3 日志提示” Compile graph failed.”

#### 问题现象

日志提示“Compile graph failed。”

图 6-95 报错提示

```
[ERROR] ME(103674,ffff8d790b0,python):2023-04-24-11:12:26.235.526 [mindspore/lite/src/extendrt/session/single_op_session.cc:242] CompileGraph] Only support CustomAscend, but got Reshape, node Reshape_9
[ERROR] ME(103674,ffff8d790b0,python):2023-04-24-11:12:26.235.617 [mindspore/lite/src/extendrt/cxx_api/model/model_impl.cc:288] BuildByBufferImpl] compile graph failed.
```

#### 原因分析

模型转换时未指定Ascend后端。

#### 处理方法

需要在模型转换阶段指定“--device=Ascend”。

### 6.4.9.4 日志提示“Custom op has no reg\_op\_name attr.”

#### 问题现象

日志提示“Custom op has no reg\_op\_name attr。”

图 6-96 报错提示

```
[ERROR] GE_ADP7(151711,ffffb4840b0,python):2023-04-24-11:42:46.677.198 [mindspore/ccsrc/transform/graph_ir/op_adapter.cc:179] GetCustomOpType] Custom op has no reg_op_name attr.
[ERROR] GE_ADP7(151711,ffffb4840b0,python):2023-04-24-11:42:46.677.262 [mindspore/ccsrc/transform/graph_ir/op_adapter.cc:179] GetCustomOpType] Custom op has no reg_op_name attr.
[WARNING] GE_ADP7(151711,ffffb4840b0,python):2023-04-24-11:42:46.677.292 [mindspore/ccsrc/transform/graph_ir/op_adapter.cc:202] GenerateCustomOp] Custom op node has no input_names, op[Custom].
[ERROR] GE_ADP7(151711,ffffb4840b0,python):2023-04-24-11:42:46.677.307 [mindspore/ccsrc/transform/graph_ir/op_adapter.cc:179] GetCustomOpType] Custom op has no reg_op_name attr.
[WARNING] GE_ADP7(151711,ffffb4840b0,python):2023-04-24-11:42:46.677.324 [mindspore/ccsrc/transform/graph_ir/op_adapter.cc:206] GenerateCustomOp] Custom op node has no output_names, op[Custom].
[ERROR] CORE(151711,ffffb4840b0,python):2023-04-24-11:42:46.677.445 [mindspore/core/utills/log_adapter.cc:388] operator~] Runtime error for null exception handler.
[ERROR] ME(151711,ffffb4840b0,python):2023-04-24-11:42:46.706.388 [mindspore/lite/src/extendrt/cxx_api/model/model.cc:100] Build] Catch exception: Cast failed, original value: (3, 1, 1, 7, 7, 6, 8, 2, 1, 7, 6, 8,), type: ValueTuple

- C++ Call Stack: (For framework developers)

mindspore/core/ir/anf.h:1085 GetValue
```

## 处理方法

定义context时无需指定：

```
context.ascend.provider = "ge"
```

### 6.4.10 附录

#### 6.4.10.1 推理业务迁移评估表

通用的推理业务及LLM推理可提供下表进行业务迁移评估：

| 收集项           | 说明                                                                                                                          | 实际情况（请填写） |
|---------------|-----------------------------------------------------------------------------------------------------------------------------|-----------|
| 项目名称          | 项目名称，例如：XXX项目。                                                                                                              | -         |
| 使用场景          | 例如： <ul style="list-style-type: none"> <li>使用YOLOv5算法对工地的视频流帧后进行安全帽检测。</li> <li>使用BertBase算法对用户app上购买商品后的评论进行理解。</li> </ul> | -         |
| CPU架构         | X86/ARM，自有软件是否支持ARM。<br>例如：4个推理模型在ARM上运行，6个推理模型在X86上运行。                                                                     | -         |
| 当前使用的操作系统及版本  | 当前推理业务的操作系统及版本，如：Ubuntu 22.04。<br>是否使用容器化运行业务，以及容器中OS版本，HostOS中是否有业务软件以及HostOS的类型和版本。<br>需要评估是否愿意迁移到华为云的通用OS。               | -         |
| AI引擎及版本       | 当前引擎（TF/PT/LibTorch），是否接受切换MindSpore。<br>例如：当前使用TF 2.6, PyTorch 1.10, 可以接受切换MindSpore。                                      | -         |
| 业务编程语言、框架、版本。 | C++/Python/JAVA等。<br>例如：业务逻辑使用JAVA，推理服务模块使用C++自定义实现推理框架，Python 3.7等。                                                        | -         |
| CPU使用率        | 业务中是否有大量使用CPU的代码，以及日常运行过程中CPU的占用率（占用多少个核心），以及使用CPU计算的业务功能说明和并发机制。                                                           | -         |
| 是否有Linux内核驱动  | 是否有业务相关的Linux内核驱动代码。                                                                                                        | -         |

| 收集项             | 说明                                                                                                                                                                                                                                                                     | 实际情况（请填写） |
|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|
| 依赖第三方组件列表       | 当前业务依赖的第三方软件列表（自行编译的第三方软件列表）。<br>例如：Faiss等。                                                                                                                                                                                                                            | -         |
| 推理框架            | TensorRT/Triton/MSLite等。<br>例如：<br><ul style="list-style-type: none"> <li>2个推理模型使用TensorRT框架，5个使用Triton框架。</li> <li>通过stable-diffusion的WebUI提供AIGC推理服务。</li> </ul>                                                                                                     | -         |
| GPU卡的类型         | Vnt1/Ant1/Ant03/Tnt004等。<br>例如：<br>20卡Ant1，运行Bert Large推理。<br>10卡Tnt004运行YOLOv5。                                                                                                                                                                                       | -         |
| Backbone类型      | ResNet/DarkNet/Transformer等。<br>例如：<br><ul style="list-style-type: none"> <li>5个模型使用ResNet Backbone，应用与监控。</li> <li>3个模型使用Transformer，应用于自然语言处理xxx。</li> <li>使用stable-diffusion的典型模型：TextEncoder、VaeEncoder、unet、VaeDecoder、SafetyChecker，没有使用LoRA等动态加载的诉求。</li> </ul> | -         |
| 模型训练方式          | 关于推理业务中使用的模型，填写该模型训练时使用的框架以及套件。<br>例如：模型使用PyTorch+Megatron+DeepSpeed进行训练。                                                                                                                                                                                              | -         |
| 自定义算子           | 是否有自定义算子，CPU还是CUDA，复杂程度。<br>例如：有5个CUDA自定义算子。1个高复杂度算子，基于C++开发2000行代码。4个中等复杂度算子，基于C++开发，平均每个自定义算子约500行代码。                                                                                                                                                                | -         |
| 动态shape         | 是否需要支持动态shape。<br>例如：需要动态Shape，需要动态Shape的模型有ResNet-50、YOLOv5。                                                                                                                                                                                                          | -         |
| 参数类型（FP32/FP16） | FP32还是FP16混合，判断精度调优难度。<br>例如：ResNet-50、YOLOv5模型使用FP16。BertLarge使用FP32。                                                                                                                                                                                                 | -         |

| 收集项              | 说明                                                                                                                                                                                                                                                                                | 实际情况（请填写） |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|
| 模型变更频率           | <p>模型变更场景如下：</p> <ul style="list-style-type: none"> <li>数据增量，模型算子未变更。</li> <li>数据增量，模型算子变化，例如：                             <ul style="list-style-type: none"> <li>网络结构变化。</li> <li>AI框架版本升级，使用了新版本算子。</li> </ul> </li> </ul> <p>例如：每半年对模型进行一次变更，变更的内容包含模型结构，并升级AI框架。</p>          | -         |
| 是否使用华为MDC产品      | <p>如果使用华为MDC产品，请填写MDC版本号，如果没有可以不填。</p> <p>例如：使用了C83版本。</p>                                                                                                                                                                                                                        | -         |
| 性能指标与预期          | <ul style="list-style-type: none"> <li>例1：<br/>模型：YOLOv5<br/>运行环境：Vnt1 单卡<br/>性能指标：QPS 100/s（两进程）<br/>性能约束：单次请求最大可以接受时延需小于100ms<br/>性能预期：QPS 130/s</li> <li>例2：<br/>模型：OCR<br/>运行环境：6348（单核48U超线程）<br/>性能指标：QPS 10/s（四进程）<br/>性能约束：单次请求最大可以接受时延需小于1s<br/>性能预期：QPS 20/s</li> </ul> | -         |
| 业务访问方式           | <p>推理业务访问：“客户端 -&gt; 云服务”或“云客户端 -&gt; 云服务”。</p> <p>推理业务时延要求，客户端到云服务端到端可接受时延。</p> <p>例如：当前是“客户端 -&gt; 云服务”模式，客户端请求应答可接受的最长时延为2秒。</p>                                                                                                                                               | -         |
| 模型参数规模，是否涉及分布式推理 | 10B/100B，单机多卡推理。                                                                                                                                                                                                                                                                  | -         |

| 收集项                    | 说明                                                                                                                                             | 实际情况（请填写） |
|------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|-----------|
| 能否提供实际模型、网络验证的代码和数据等信息 | <p>提供实际模型、网络验证的代码和数据。</p> <p>提供与业务类型类似的开源模型，例如GPT3 10B/13B。</p> <p>提供测试模型以及对应的Demo代码路径（开源或共享）。</p> <p>可以提前的完成POC评估，例如框架、算子支持度，以及可能的一些性能指标。</p> | -         |

如果是AIGC场景的业务例如Stable Diffusion，请在上表的基础上，再提供以下信息：

| 收集项                | 说明                                                                                                                                                                                                                                                                                                                                                                       | 实际情况（请填写） |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|
| 使用场景               | <p>例如：</p> <ol style="list-style-type: none"> <li>1. 业务是文生图，图生图等。</li> <li>2. 业务是否需要频繁更新模型，或者需要动态加载Lora。</li> </ol>                                                                                                                                                                                                                                                      | -         |
| stable-diffusion套件 | <ol style="list-style-type: none"> <li>1. 使用diffusers（<a href="https://github.com/huggingface/diffusers">https://github.com/huggingface/diffusers</a>）。</li> <li>2. stable-diffusion-webui（<a href="https://github.com/AUTOMATIC1111/stable-diffusion-webui">https://github.com/AUTOMATIC1111/stable-diffusion-webui</a>）。</li> <li>3. 如果是基于其他开源，需要附带开源代码仓地址。</li> </ol> | -         |
| 具体使用库              | <p>例如：</p> <ol style="list-style-type: none"> <li>1. 使用了哪个pipeline（例如lpw_stable_diffusion.py）。</li> <li>2. 使用了哪个huggingface的模型（例如digiplay/majicMIX_realistic_v6）。</li> <li>3. 如果有预处理，后处理，对应的模型是什么（例如后处理的超分模型）。</li> </ol>                                                                                                                                                | -         |
| Lora/TextInversion | <ol style="list-style-type: none"> <li>1. 是否有动态加载Lora的需求，可否接受把Lora固定到模型内。</li> <li>2. 是否使用了TextInversion，是否需要动态加载。</li> </ol>                                                                                                                                                                                                                                            | -         |
| 动态shape            | 是否可接受分档shape（固定n个挡位的shape）。                                                                                                                                                                                                                                                                                                                                              | -         |

| 收集项    | 说明                                                                                                                                                                                 | 实际情况 (请填写) |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|
| 模型变更频率 | 模型变更场景如下：<br>1. 数据增量，模型算子未变更。<br>2. 数据增量，模型算子变化，例如： <ul style="list-style-type: none"> <li>● 网络结构变化。</li> <li>● AI框架版本升级，使用了新版本算子。</li> </ul> 例如：每半年对模型进行一次变更，变更的内容包含模型结构，并升级AI框架。 | -          |
| 尺寸要求   | 超分前产生的图片尺寸要求： <ol style="list-style-type: none"> <li>1. 512*512</li> <li>2. 720*720</li> <li>3. 1080 *1080</li> <li>4. 1920*1920 ( shape过大可能导致性能下降 )</li> </ol>                    | -          |

# 7 权限管理

## 7.1 ModelArts 权限管理基本概念

ModelArts作为一个完备的AI开发平台，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。这类特性在大型企业用户的使用场景下很常见，但对个人用户则显得复杂而意义不足，所以建议个人用户在使用ModelArts时，参照[个人用户快速配置ModelArts访问权限](#)来进行初始权限设置。

### 📖 说明

#### 您是否需要阅读本文档？

如果下述问题您的任何一个回答为“是”，则需要阅读此文档

- 您是企业用户，且
  - 存在多个部门，且需要限定不同部门的用户只能访问其专属资源、功能
  - 存在多种角色（如管理员、算法开发者、应用运维），希望限制不同角色只能使用特定功能
  - 逻辑上存在多套“环境”且相互隔离（如开发环境、预生产环境、生产环境），并限定不同用户在不同环境上的操作权限
  - 其他任何需要对特定子用户（组）做出特定权限限制的情况
- 您是个人用户，但已经在IAM创建多个子用户，且期望限定不同子用户所能使用的ModelArts功能、资源不同
- 希望了解ModelArts的权限控制能力细节，期望理解其概念和实操方法

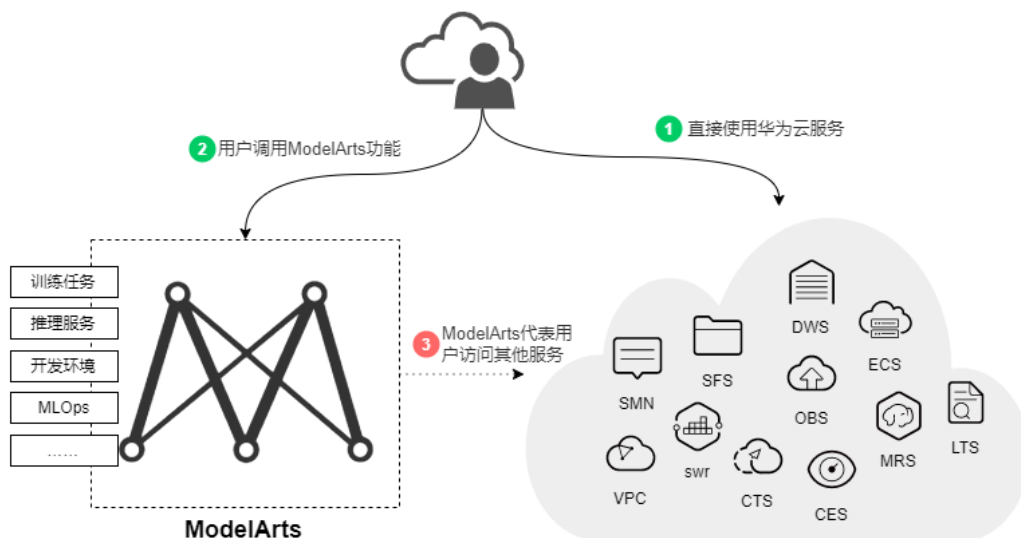
ModelArts的大部分权限管理能力均基于统一身份认证服务（Identity and Access Management，简称IAM）来实现，在您继续往下阅读之前，强烈建议您先行熟悉[IAM基本概念](#)，如果能完整理解IAM的所有概念，将更加有助于您理解本文档。

为了支持客户对ModelArts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 ModelArts 的权限与委托

图 7-1 权限管理抽象



ModelArts与其他服务类似，对外暴露的每个功能，都通过IAM的权限来进行控制。比如，用户（此处指IAM子用户，而非租户）希望在ModelArts创建训练作业，则该用户必须拥有 "modelarts:trainJob:create" 的权限才可以完成操作（无论界面操作还是API调用）。关于如何给用户赋权（准确讲是需要先将用户加入用户组，再面向用户组赋权），可以参考IAM的文档《[权限管理](#)》。

而ModelArts还有一个特殊的地方在于，为了完成AI计算的各种操作，AI平台在任务执行过程中需要访问用户的其他服务，典型的例子就是训练过程中，需要访问OBS读取用户的训练数据。在这个过程中，就出现了ModelArts“代表”用户去访问其他云服务的情形。从安全角度出发，ModelArts代表用户访问任何云服务之前，均需要先获得用户的授权，而这个动作就是一个“委托”的过程。用户授权ModelArts再代表自己访问特定的云服务，以完成其在ModelArts平台上执行的AI计算任务。

综上，对于图1 权限管理抽象可以做如下解读：

- 用户访问任何云服务，均是通过标准的IAM权限体系进行访问控制。用户首先需要具备相关云服务的权限（根据您具体使用的功能不同，所需的相关服务权限多寡亦有差异）。
- **权限**：用户使用ModelArts的任何功能，亦需要通过IAM权限体系进行正确权限授权。
- **委托**：ModelArts上的AI计算任务执行过程中需要访问其他云服务，此动作需要获得用户的委托授权。

## ModelArts 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，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，用户就可以基于授予的权限对云服务进行操作。

**注意**

ModelArts部署时通过物理区域划分，为项目级服务，授权时“选择授权范围方案”可以选择“指定区域项目资源”，如果授权时指定了区域（如华北-北京4）对应的项目（cn-north-4），则该权限仅对此项目生效；简单的做法是直接选择“所有资源”。

ModelArts也支持企业项目，所以选择授权范围方案时，也可以指定企业项目。具体操作参见《[创建用户组并授权](#)》。

图 7-2 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。

表7-1列出了ModelArts的所有预置系统策略。

表 7-1 ModelArts 系统策略

| 策略名称                        | 描述                                            | 类型   |
|-----------------------------|-----------------------------------------------|------|
| ModelArts FullAccess        | ModelArts管理员用户，拥有所有ModelArts服务的权限             | 系统策略 |
| ModelArts CommonOperations  | ModelArts操作用户，拥有所有ModelArts服务操作权限除了管理专属资源池的权限 | 系统策略 |
| ModelArts Dependency Access | ModelArts服务的常用依赖服务的权限                         | 系统策略 |

通常来讲，只给管理员开通“ModelArts FullAccess”，如果不需要太精细的控制，直接给所有用户开通“ModelArts CommonOperations”即可满足大多数小团队的开发场景诉求。如果您希望通过自定义策略做深入细致的权限控制，请阅读[ModelArts的IAM权限控制详解](#)。

### 📖 说明

ModelArts的权限不会凌驾于其他服务的权限之上，当您给用户进行ModelArts赋权时，系统不会自动对其他相关服务的相关权限进行赋权。这样做的好处是更加安全，不会出现预期外的“越权”，但缺点是，您必须同时给用户赋予不同服务的权限，才能确保用户可以顺利完成某些ModelArts操作。

举例，如果用户需要用OBS中的数据进行训练，当已经为IAM用户配置ModelArts训练权限时，仍需同时为其配置对应的OBS权限（读、写、列表），才可以正常使用。其中OBS的列表权限用于支持用户从ModelArts界面上选择要进行训练的数据路径；读权限主要用于数据的预览以及训练任务执行时的数据读取；写权限则是为了保存训练结果和日志。

- 对于个人用户或小型组织，一个简单做法是为IAM用户配置“作用范围”为“全局级服务”的“Tenant Administrator”策略，这会使用户获得除了IAM以外的所有用户权限。在获得便利的同时，由于用户的权限较大，会存在相对较大的安全风险，需谨慎使用。（对于个人用户，其默认IAM账号就已经属于admin用户组，且具备Tenant Administrator权限，无需额外操作）
- 当您需要限制用户操作，仅为ModelArts用户配置OBS相关的最小化权限项，具体操作请参见[OBS权限管理](#)。对于其他云服务，也可以进行精细化权限控制，具体请参考对应的云服务文档。

## ModelArts 委托授权

前文已经介绍，ModelArts在执行AI计算任务过程中，需要“代表”用户去访问其他云服务，而此动作需要提前获得用户的授权。在IAM权限体系下，此类授权动作是通过“委托”来完成。

关于委托的基本概念及操作可以参考对应的IAM文档《[委托其他云服务管理资源](#)》。

为了简化用户的委托授权操作，ModelArts增加了自动配置委托授权的支持，用户仅需在ModelArts控制台的“全局配置”页面中，为自己或特定用户配置委托即可。

### 📖 说明

- 只有具备IAM委托管理权限的用户才可以进行此项操作，通常是IAM admin用户组的成员才具备此权限。
- 目前ModelArts的委托授权操作是分区域操作的，这意味着您需要在每个您所用到的区域均执行委托授权操作。

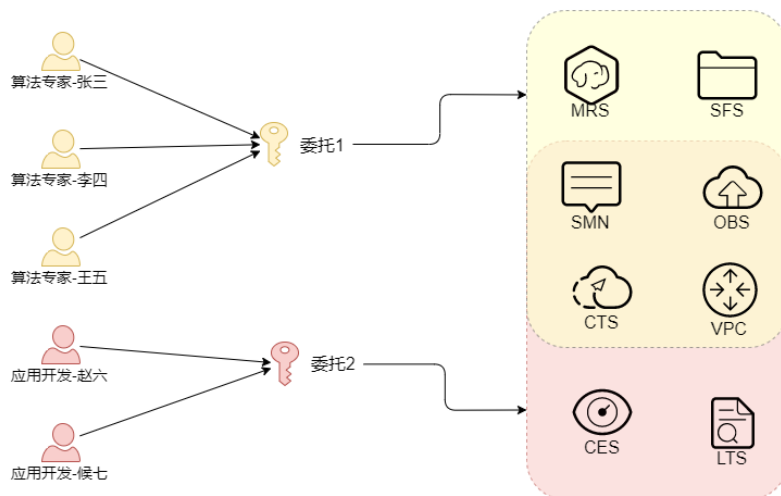
图 7-3 全局配置



在ModelArts控制台的“全局配置”页面，单击“添加授权”后，系统会引导您为特定用户或所有用户进行委托配置，通常默认会创建一个名为“modelarts\_agency\_<用户名>\_随机ID”的委托条目。在权限配置的区域，您可以选择ModelArts提供的预置配置，也可以自定义选择您所授权的策略。当然如果这两种形态对于您的诉求均过于粗犷，您也可以直接在IAM管理页面里创建完全由您进行精细化配置的委托（需要委托给ModelArts服务），然后在此页面的委托选择里使用“已有委托”“”（而非“新增委托”）。

至此，您应该已经发现了一个细节，ModelArts在使用委托时，是将其与用户进行关联的，用户与委托的关系是多对1的关系。这意味着，如果两个用户需要配置的委托一致，那么不需要为每个用户都创建一个独立的委托项，只需要将两个用户都“指向”同一个委托项即可。

图 7-4 用户与委托对应关系



**说明**

每个用户必须关联委托才可以使用ModelArts，但即使委托所赋之权限不足，在API调用之初也不会报错，只有到系统具体使用到该功能时，才会发生问题。例如，用户在创建训练任务时打开了“消息通知”，该功能依赖SMN委托授权，但只有训练任务运行过程中，真正需要发送消息时，系统才会“出错”，而有些错误系统会选择“忽略”，另一些错误则可能导致任务直接失败。当您做深入的“权限最小化”限制时，请确保您在ModelArts上将要执行的操作仍旧有足够的权限。

### 严格授权模式

严格授权模式是指在IAM中创建的子用户必须由账号管理员显式在IAM中授权，才能访问ModelArts服务，管理员用户可以通过授权策略为普通用户精确添加所需使用的ModelArts功能的权限。

相对的，在非严格授权模式下，子用户不需要显式授权就可以使用ModelArts，管理员需要在IAM上为子用户配置Deny策略来禁止子用户使用ModelArts的某些功能。

账号的管理员用户可以在“全局配置”页面修改授权模式。

**须知**

如无特殊情况，建议优先使用严格授权模式。在严格授权模式下，子用户要使用ModelArts的功能都需经过授权，可以更精确的控制子用户的权限范围，达成权限最小化的安全策略。

### 用工作空间限制资源访问

工作空间是ModelArts面向企业客户提供的的一个高阶功能，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。目前工作空间功能是“受邀开通”状态，作为企业用户您可以通过您对口的技术支持经理申请开通。

在开通工作空间后，系统会默认为您创建一个“default”空间，您之前所创建的所有资源，均在该空间下。当您创建新的工作空间之后，相当于您拥有了一个新的

“ModelArts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。

创建工作空间时，必须绑定一个企业项目。多个工作空间可以绑定到同一个企业项目，但一个工作空间**不可以**绑定多个企业项目。借助工作空间，您可以对不同用户的资源访问和权限做更加细致的约束，具体为如下两种约束：

- 只有被授权的用户才能访问特定的工作空间（在创建、管理工作空间的页面进行配置），这意味着，像数据集、算法等AI资产，均可以借助工作空间做访问的限制。
- 在前文提到的权限授权操作中，如果“选择授权范围方案”时设定为“指定企业项目资源”，那么该授权仅对绑定至该企业项目的工作空间生效。

#### 📖 说明

- 工作空间的约束与权限授权的约束是叠加生效的，意味着对于一个用户，必须同时拥有工作空间的访问权和训练任务的创建权限（且该权限覆盖至当前的工作空间），他才可以在这个空间里提交训练任务。
- 对于已经开通企业项目但没有开通工作空间的用户，其所有操作均相当于在“default”企业项目里进行，请确保对应权限已覆盖了名为default的企业项目。
- 对于未开通企业项目的用户，不受上述约束限制。

## 本章小结

对于ModelArts的权限管理，总结了如下几条关键点：

- 如果您是个人用户，则不需要考虑细粒度权限问题，您的账户默认具备使用ModelArts的所有权限。
- ModelArts平台的所有功能均通过IAM体系进行了权限管控，您可以通过标准的IAM**授权**动作，来对特定用户进行精细化的权限管控。
- 对于所有用户（包括个人用户），需要完成对ModelArts的**委托授权**（ModelArts > 全局配置 > 添加授权），才能使用特定的功能，否则会造成您的操作出现不可预期的错误。
- 对于开通了企业项目的用户，可以进一步申请开通ModelArts的**工作空间**，通过组合使用基础授权和工作空间，来达成更加复杂的权限控制目的。

## 7.2 权限控制方式

### 7.2.1 IAM

介绍ModelArts所有功能涉及到的IAM权限配置。

#### IAM 权限简介

如果您需要对华为云云服务平台上购买创建的ModelArts资源，为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云服务资源的访问。如果华为账号已经能满足您的要求，不需要通过IAM对用户进行权限管理，您可以跳过本章节，不影响您使用ModelArts服务的其他功能。



IAM是华为云云服务平台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。

通过IAM，您可以通过授权控制他们对华为云云服务资源的访问范围。例如您的员工中有负责软件开发的人员，您希望他们拥有ModelArts的使用权限，但是不希望他们拥有删除ModelArts等高危操作的权限，那么您可以使用IAM进行权限分配，通过授予用户仅能使用ModelArts，但是不允许删除ModelArts的权限，控制他们对ModelArts资源的使用范围。

关于IAM的详细介绍，请参见[IAM产品介绍](#)。

## 角色与策略权限管理

ModelArts服务支持角色与策略授权。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。

ModelArts部署时通过物理区域划分，为项目级服务。授权时，“授权范围”需要选择“指定区域项目资源”，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“授权范围”选择“所有资源”，则该权限在所有区域项目中都生效。访问ModelArts时，需要先切换至授权区域。

如表7-2所示，包括了ModelArts的所有系统策略权限。如果系统预置的ModelArts权限，不满足您的授权要求，可以创建自定义策略，可参考[策略JSON格式字段介绍](#)。

表 7-2 ModelArts 系统策略

| 策略名称                        | 描述                                             | 类型   |
|-----------------------------|------------------------------------------------|------|
| ModelArts FullAccess        | ModelArts管理员用户，拥有所有ModelArts服务的权限。             | 系统策略 |
| ModelArts CommonOperations  | ModelArts操作用户，拥有所有ModelArts服务操作权限除了管理专属资源池的权限。 | 系统策略 |
| ModelArts Dependency Access | ModelArts服务的常用依赖服务的权限。                         | 系统策略 |

ModelArts对其他云服务有依赖关系，因此在ModelArts控制台的各项功能需要配置相应的服务权限后才能正常查看或使用，依赖服务及其预置的权限如下。

表 7-3 ModelArts 控制台依赖服务的角色或策略

| 控制台功能 | 依赖服务           | 需配置角色/策略          |
|-------|----------------|-------------------|
| 数据管理  | 对象存储服务OBS      | OBS Administrator |
|       | 数据湖探索DLI       | DLI FullAccess    |
|       | MapReduce服务MRS | MRS Administrator |



| 控制台功能    | 依赖服务                | 需配置角色/策略                                                  |
|----------|---------------------|-----------------------------------------------------------|
|          | 数据仓库服务 GaussDB(DWS) | DWS Administrator                                         |
|          | 云审计服务CTS            | CTS Administrator                                         |
|          | AI开发平台ModelArts     | ModelArts CommonOperations<br>ModelArts Dependency Access |
| 开发环境     | 对象存储服务OBS           | OBS Administrator                                         |
|          | 凭据管理服务CSMS          | CSMS ReadOnlyAccess                                       |
|          | 云审计服务CTS            | CTS Administrator                                         |
|          | 弹性云服务器ECS           | ECS FullAccess                                            |
|          | 容器镜像服务SWR           | SWR Administrator                                         |
|          | 弹性文件服务SFS           | SFS Turbo FullAccess                                      |
|          | 应用运维管理服务 AOM        | AOM FullAccess                                            |
|          | 密钥管理服务KMS           | KMS CMKFullAccess                                         |
|          | AI开发平台ModelArts     | ModelArts CommonOperations<br>ModelArts Dependency Access |
| 训练管理     | 对象存储服务OBS           | OBS Administrator                                         |
|          | 消息通知服务SMN           | SMN Administrator                                         |
|          | 云审计服务CTS            | CTS Administrator                                         |
|          | 弹性文件服务SFS Turbo     | SFS Turbo ReadOnlyAccess                                  |
|          | 容器镜像服务SWR           | SWR Administrator                                         |
|          | 应用运维管理服务 AOM        | AOM FullAccess                                            |
|          | 密钥管理服务KMS           | KMS CMKFullAccess                                         |
|          | AI开发平台ModelArts     | ModelArts CommonOperations<br>ModelArts Dependency Access |
| Workflow | 对象存储服务OBS           | OBS Administrator                                         |
|          | 云审计服务CTS            | CTS Administrator                                         |
|          | AI开发平台ModelArts     | ModelArts CommonOperations<br>ModelArts Dependency Access |
| 自动学习     | 对象存储服务OBS           | OBS Administrator                                         |

| 控制台功能      | 依赖服务            | 需配置角色/策略                                                  |
|------------|-----------------|-----------------------------------------------------------|
|            | 云审计服务CTS        | CTS Administrator                                         |
|            | AI开发平台ModelArts | ModelArts CommonOperations<br>ModelArts Dependency Access |
| AI应用管理     | 对象存储服务OBS       | OBS Administrator                                         |
|            | 企业项目管理服务EPS     | EPS FullAccess                                            |
|            | 云审计服务CTS        | CTS Administrator                                         |
|            | 容器镜像服务SWR       | SWR Administrator                                         |
|            | AI开发平台ModelArts | ModelArts CommonOperations<br>ModelArts Dependency Access |
| 部署上线       | 对象存储服务OBS       | OBS Administrator                                         |
|            | 云监控服务CES        | CES ReadOnlyAccess                                        |
|            | 消息通知服务SMN       | SMN Administrator                                         |
|            | 企业项目管理服务EPS     | EPS FullAccess                                            |
|            | 云审计服务CTS        | CTS Administrator                                         |
|            | 云日志服务LTS        | LTS FullAccess                                            |
|            | 虚拟私有云VPC        | VPC FullAccess                                            |
|            | AI开发平台ModelArts | ModelArts CommonOperations<br>ModelArts Dependency Access |
| AI Gallery | 对象存储服务OBS       | OBS Administrator                                         |
|            | 云审计服务CTS        | CTS Administrator                                         |
|            | 容器镜像服务SWR       | SWR Administrator                                         |
|            | AI开发平台ModelArts | ModelArts CommonOperations<br>ModelArts Dependency Access |
| 专属资源池      | 云审计服务CTS        | CTS Administrator                                         |
|            | 云容器引擎CCE        | CCE Administrator                                         |
|            | 裸金属服务器BMS       | BMS FullAccess                                            |
|            | 镜像服务IMS         | IMS FullAccess                                            |
|            | 数据加密服务DEW       | DEW KeypairReadOnlyAccess                                 |
|            | 虚拟私有云VPC        | VPC FullAccess                                            |
|            | 弹性云服务器ECS       | ECS FullAccess                                            |
|            | 弹性文件服务SFS       | SFS Turbo FullAccess                                      |

| 控制台功能 | 依赖服务            | 需配置角色/策略             |
|-------|-----------------|----------------------|
|       | 对象存储服务OBS       | OBS Administrator    |
|       | 应用运维管理服务AOM     | AOM FullAccess       |
|       | 标签管理服务TMS       | TMS FullAccess       |
|       | AI开发平台ModelArts | ModelArts FullAccess |
|       | 费用中心            | BSS Administrator    |

如果系统预置的权限，不满足您的授权要求，可以创建自定义策略。自定义策略中可以添加的授权项（Action）请参考[ModelArts资源权限项](#)。

目前华为云云服务平台支持以下两种方式创建自定义策略：

- 可视化视图创建自定义策略：无需了解策略语法，按可视化视图导航栏选择云服务、操作、资源、条件等策略内容，可自动生成策略。
- JSON视图创建自定义策略：可以在选择策略模板后，根据具体需求编辑策略内容；也可以直接在编辑框内编写JSON格式的策略内容。

具体创建步骤请参见：[创建自定义策略](#)。下面为您介绍常用的ModelArts自定义策略样例。

- 示例1：授权镜像管理的权限。

```
{
 "Version": "1.1",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": [
 "modelarts:image:register",
 "modelarts:image:listGroup"
]
 }
]
}
```

- 示例2：拒绝用户创建、更新、删除专属资源池。

拒绝策略需要同时配合其他策略使用，否则没有实际作用。用户被授予的策略中，一个授权项的作用如果同时存在Allow和Deny，则遵循**Deny优先原则**。

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

```
 "smn:*:*"
],
 "Effect": "Allow"
 },
 {
 "Action": [
 "modelarts:pool:create",
 "modelarts:pool:update",
 "modelarts:pool:delete"
],
 "Effect": "Deny"
 }
]
}
```

- 示例3：多个授权项策略。

一个自定义策略中可以包含多个授权项，且除了可以包含本服务的授权项外，还可以包含其他服务的授权项，可以包含的其他服务必须跟本服务同属性，即都是项目级服务或都是全局级服务。多个授权语句策略描述如下：

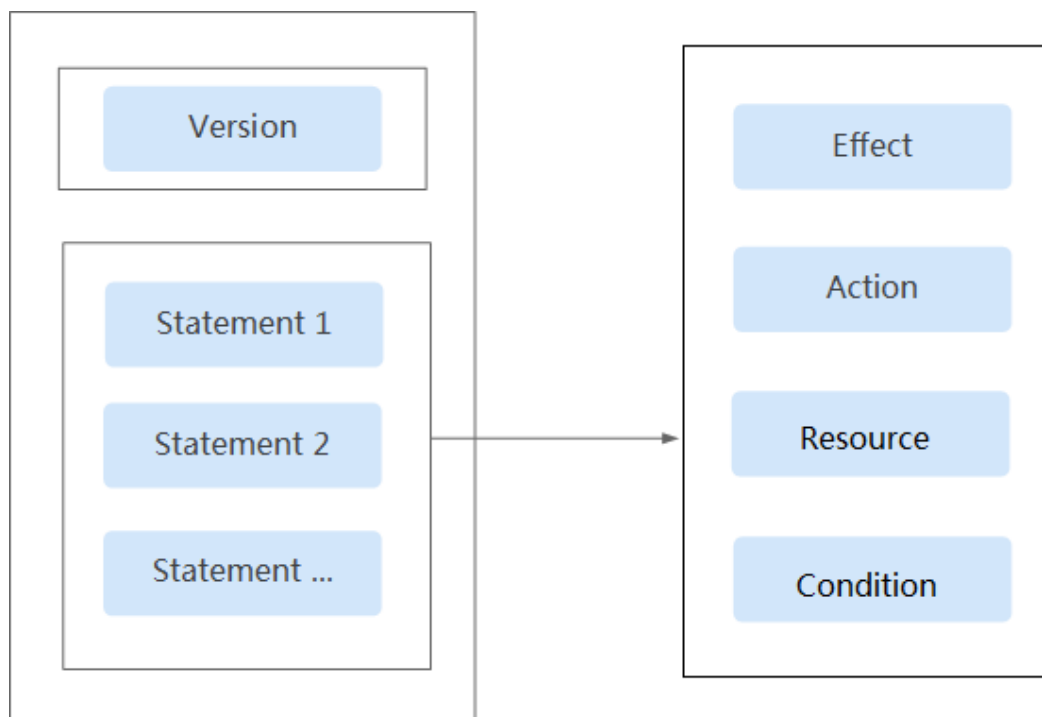
```
{
 "Version": "1.1",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": [
 "modelarts:service:*"
]
 },
 {
 "Effect": "Allow",
 "Action": [
 "lts:logs:list"
]
 }
]
}
```

## 策略 JSON 格式字段介绍

### 策略结构

策略结构包括Version（策略版本号）和Statement（策略权限语句）两部分，其中Statement可以有多个，表示不同的授权项。

图 7-5 策略结构



### 策略参数

下面介绍策略参数详细说明。了解策略参数后，您可以根据场景自定义策略。具体可以参考文档[自定义策略使用样例](#)。

表 7-4 策略参数说明

| 参数                    | 含义             | 值                                                                                                                                                                                  |
|-----------------------|----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Version               | 策略的版本。         | 1.1：代表基于策略的访问控制。                                                                                                                                                                   |
| Statement<br>：策略的授权语句 | Effect：<br>作用  | 定义Action中的操作权限是否允许执行。<br><br><b>说明</b><br>当同一个Action的Effect既有Allow又有Deny时，遵循Deny优先的原则。                                                                                             |
|                       | Action：<br>授权项 | 操作权限。<br><br>格式为“服务名:资源类型:操作”。授权项支持通配符号*，通配符号*表示所有。<br>示例：<br>"modelarts:notebook:list"：表示查看Notebook实例列表权限，其中modelarts为服务名，notebook为资源类型，list为操作。<br>您可以在对应服务“API参考”资料中查看该服务所有授权项。 |

| 参数 |                | 含义                                       | 值                                                                                                                                                                                       |
|----|----------------|------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|    | Condition: 条件  | 使策略生效的特定条件, 包括 <b>条件键</b> 和 <b>运算符</b> 。 | 格式为“条件运算符:{条件键: [条件值1, 条件值2]}”。<br>如果您设置多个条件, 同时满足所有条件时, 该策略才生效。<br>示例:<br>"StringEndWithIfExists":{"g:UserName":["specialCharacter"]}: 表示当用户输入的用户名以"specialCharacter"结尾时该条statement生效。 |
|    | Resource: 资源类型 | 策略所作用的资源。                                | 格式为“服务名:<region><account-id>:资源类型:资源路径”, 资源类型支持通配符号*, 通配符号*表示所有。<br><b>说明</b><br>ModelArts的授权不支持指定具体资源路径。                                                                               |

## ModelArts 资源类型

管理员可以按ModelArts的资源类型选择授权范围。ModelArts支持的资源类型如下表:

表 7-5 ModelArts 资源类型 (角色与策略授权)

| 资源类型                | 说明              |
|---------------------|-----------------|
| notebook            | 开发环境的Notebook实例 |
| exemlProject        | 自动学习项目          |
| exemlProjectInf     | 自动学习项目的在线推理服务   |
| exemlProjectTrain   | 自动学习项目的训练作业     |
| exemlProjectVersion | 自动学习项目的版本       |
| workflow            | Workflow项目      |
| pool                | 专属资源池           |
| network             | 专属资源池网络连接       |
| trainJob            | 训练作业            |
| trainJobLog         | 训练作业的运行日志       |
| trainJobInnerModel  | 系统预置模型          |
| model               | 模型              |
| service             | 在线服务            |
| nodeservice         | 边缘服务            |

| 资源类型           | 说明       |
|----------------|----------|
| workspace      | 工作空间     |
| dataset        | 数据集      |
| dataAnnotation | 数据集的标注信息 |
| aiAlgorithm    | 训练算法     |
| image          | 镜像       |
| devserver      | 弹性裸金属    |

## ModelArts 资源权限项

参考《ModelArts API参考》中的权限策略和授权项。

- [数据管理权限](#)
- [开发环境权限](#)
- [训练作业权限](#)
- [模型管理权限](#)
- [服务管理权限](#)
- [工作空间管理权限](#)

## 7.2.2 委托和依赖

### 功能依赖

#### 功能依赖策略项

您在使用ModelArts服务中开发算法、管理训练作业过程中，需要和其他云服务交互，比如需要在提交训练作业时选择指定数据集OBS路径和日志存储OBS路径。因此管理员在为用户配置细粒度授权策略时，需要同时配置依赖的权限项，用户才能使用完整的功能。

#### 📖 说明

- 如果您使用根用户（与账户同名的缺省子用户）使用ModelArts，根用户默认拥有所有权限，不再需要单独授权。
- 请用户确保当前用户具备委托授权中包含的依赖策略项权限。例如，用户给ModelArts的委托需要授权SWR Admin权限，需要保证用户本身具备SWR Admin权限。

表 7-6 基本配置

| 业务场景 | 依赖的服务 | 依赖策略项               | 支持的功能          |
|------|-------|---------------------|----------------|
| 全局配置 | IAM   | iam:users:listUsers | 查询用户列表（仅管理员需要） |



| 业务场景 | 依赖的服务 | 依赖策略项             | 支持的功能                         |
|------|-------|-------------------|-------------------------------|
| 基本功能 | IAM   | iam:tokens:assume | 使用委托获取用户临时认证凭据（必需）            |
| 基本功能 | BSS   | bss:balance:view  | 在ModelArts控制台创建资源后，页面展示账号当前余额 |

表 7-7 管理工作空间

| 业务场景 | 依赖的服务     | 依赖策略项                | 支持的功能              |
|------|-----------|----------------------|--------------------|
| 工作空间 | IAM       | iam:users:listUsers  | 按用户进行工作空间授权        |
|      | ModelArts | modelarts:*:*delete* | 删除工作空间时，同时清理空间内的资源 |

表 7-8 管理开发环境 Notebook

| 业务场景         | 依赖的服务     | 依赖策略项                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | 支持的功能                    |
|--------------|-----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|
| 开发环境实例生命周期管理 | ModelArts | modelarts:notebook:create<br>modelarts:notebook:list<br>modelarts:notebook:get<br>modelarts:notebook:update<br>modelarts:notebook:delete<br>modelarts:notebook:start<br>modelarts:notebook:stop<br>modelarts:notebook:updateStopPolicy<br>modelarts:image:delete<br>modelarts:image:list<br>modelarts:image:create<br>modelarts:image:get<br>modelarts:pool:list<br>modelarts:tag:list<br>modelarts:network:get<br>aom:metric:get<br>aom:metric:list<br>aom:alarm:list | 实例的启动、停止、创建、删除、更新等依赖的权限。 |
| 动态挂载存储配置     | ModelArts | modelarts:notebook:listMountedStorages<br>modelarts:notebook:mountStorage<br>modelarts:notebook:getMountedStorage<br>modelarts:notebook:unmountStorage                                                                                                                                                                                                                                                                                                                 | 动态挂载存储配置。                |
|              | OBS       | obs:bucket:ListAllMyBuckets<br>obs:bucket:ListBucket                                                                                                                                                                                                                                                                                                                                                                                                                   |                          |

| 业务场景         | 依赖的服务     | 依赖策略项                                                                                                       | 支持的功能                                                                                                                      |
|--------------|-----------|-------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------|
| 镜像管理         | ModelArts | modelarts:image:register<br>modelarts:image:listGroup                                                       | 在镜像管理中注册和查看镜像。                                                                                                             |
| 保存镜像         | SWR       | SWR Admin                                                                                                   | SWR Admin为SWR最大权限，用于： <ul style="list-style-type: none"> <li>开发环境运行的实例，保存成镜像。</li> <li>使用自定义镜像创建开发环境Notebook实例。</li> </ul> |
| 使用SSH功能      | ECS       | ecs:serverKeypairs:list<br>ecs:serverKeypairs:get<br>ecs:serverKeypairs:delete<br>ecs:serverKeypairs:create | 为开发环境Notebook实例配置登录密钥。                                                                                                     |
|              | DEW       | kps:domainKeypairs:get<br>kps:domainKeypairs:list                                                           |                                                                                                                            |
| 挂载SFS Turbo盘 | SFS Turbo | SFS Turbo FullAccess                                                                                        | 子用户对SFS目录的读写操作权限。专属池Notebook实例挂载SFS（公共池不支持），且挂载的SFS不是当前子用户创建的。                                                             |
| 查看所有实例       | ModelArts | modelarts:notebook:listAllNotebooks                                                                         | ModelArts开发环境界面上，查询所有用户的实例列表，适用于给开发环境的实例管理员配置该权限。                                                                          |
|              | IAM       | iam:users:listUsers                                                                                         |                                                                                                                            |

| 业务场景                                 | 依赖的服务     | 依赖策略项                                                                                                                                                                                                                                                                                             | 支持的功能                             |
|--------------------------------------|-----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------|
| VSCode插件 (本地) / PyCharm Toolkit (本地) | ModelArts | modelarts:notebook:listAllNotebooks<br>modelarts:trainJob:create<br>modelarts:trainJob:list<br>modelarts:trainJob:update<br>modelarts:trainJobVersion:delete<br>modelarts:trainJob:get<br>modelarts:trainJob:logExport<br>modelarts:workspace:getQuotas (如果开通了 <a href="#">工作空间</a> 功能,则需要配置此权限。) | 从本地VSCode连接云上的Notebook实例、提交训练作业等。 |

| 业务场景 | 依赖的服务 | 依赖策略项                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 支持的功能                       |
|------|-------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------|
|      | OBS   | obs:bucket:ListAllMybuckets<br>obs:bucket:HeadBucket<br>obs:bucket:ListBucket<br>obs:bucket:GetBucketLocation<br>obs:object:GetObject<br>obs:object:GetObjectVersion<br>obs:object:PutObject<br>obs:object>DeleteObject<br>obs:object>DeleteObjectVersion<br>obs:object:ListMultipartUploadParts<br>obs:object:AbortMultipartUpload<br>obs:object:GetObjectAcl<br>obs:object:GetObjectVersionAcl<br>obs:bucket:PutBucketAcl<br>obs:object:PutObjectAcl<br>obs:object:ModifyObjectMetadata |                             |
|      | IAM   | iam:projects:listProjects                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | 从本地PyCharm查询IAM项目列表，完成连接配置。 |

表 7-9 管理训练作业

| 业务场景 | 依赖的服务                               | 依赖策略项                                                                                                                                                  | 支持的功能                                            |
|------|-------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------|
| 训练管理 | ModelArts                           | modelarts:trainJob:*<br>modelarts:trainJobLog:*<br>modelarts:aiAlgorithm:*<br>modelarts:image:list<br>modelarts:network:get<br>modelarts:workspace:get | 创建训练作业和查看训练日志。                                   |
|      |                                     | modelarts:workspace:getQuota                                                                                                                           | 查询工作空间配额。如果开通了 <a href="#">工作空间</a> 功能，则需要配置此权限。 |
|      |                                     | modelarts:tag:list                                                                                                                                     | 在训练作业中使用标签管理服务TMS。                               |
|      | IAM                                 | iam:credentials:listCredentials<br>iam:agencies:listAgencies                                                                                           | 使用配置的委托授权项。                                      |
|      | SFS Turbo                           | sfsturbo:shares:getShare<br>sfsturbo:shares:getAllShares                                                                                               | 在训练作业中使用SFS Turbo。                               |
|      | SWR                                 | swr:repository:listTags<br>swr:repository:getRepository<br>swr:repository:listRepositories                                                             | 使用自定义镜像运行训练作业。                                   |
| SMN  | smn:topic:publish<br>smn:topic:list | 通过SMN通知训练作业状态变化事件。                                                                                                                                     |                                                  |

| 业务场景 | 依赖的服务 | 依赖策略项                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 支持的功能                    |
|------|-------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|
|      | OBS   | obs:bucket:ListAllMybuckets<br>obs:bucket:HeadBucket<br>obs:bucket:ListBucket<br>obs:bucket:GetBucketLocation<br>obs:object:GetObject<br>obs:object:GetObjectVersion<br>obs:object:PutObject<br>obs:object:DeleteObject<br>obs:object:DeleteObjectVersion<br>obs:object:ListMultipartUploadParts<br>obs:object:AbortMultipartUpload<br>obs:object:GetObjectAcl<br>obs:object:GetObjectVersionAcl<br>obs:bucket:PutBucketAcl<br>obs:object:PutObjectAcl<br>obs:object:ModifyObjectMetadata | 使用OBS桶中的数据<br>数据集运行训练作业。 |

表 7-10 使用 Workflow

| 业务场景  | 依赖的服务     | 依赖策略项                                                                                                                                                                                                                                                                                                   | 支持的功能                           |
|-------|-----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------|
| 使用数据集 | ModelArts | modelarts:dataset:getDataset<br>modelarts:dataset:createDataset<br>modelarts:dataset:createDatasetVersion<br>modelarts:dataset:createImportTask<br>modelarts:dataset:updateDataset<br>modelarts:processTask:createProcessTask<br>modelarts:processTask:getProcessTask<br>modelarts:dataset:listDatasets | 在 workflow 中使用<br>ModelArts 数据集 |



| 业务场景   | 依赖的服务     | 依赖策略项                                                                                                                                                                                                                                                   | 支持的功能                 |
|--------|-----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|
| 管理AI应用 | ModelArts | modelarts:model:list<br>modelarts:model:get<br>modelarts:model:create<br>modelarts:model:delete<br>modelarts:model:update                                                                                                                               | 在工作流中管理ModelArts AI应用 |
| 部署上线   | ModelArts | modelarts:service:get<br>modelarts:service:create<br>modelarts:service:update<br>modelarts:service:delete<br>modelarts:service:getLogs                                                                                                                  | 在工作流中管理ModelArts在线服务  |
| 训练作业   | ModelArts | modelarts:trainJob:get<br>modelarts:trainJob:create<br>modelarts:trainJob:list<br>modelarts:trainJobVersion:list<br>modelarts:trainJobVersion:create<br>modelarts:trainJob:delete<br>modelarts:trainJobVersion:delete<br>modelarts:trainJobVersion:stop | 在工作流中管理ModelArts训练作业  |
| 工作空间   | ModelArts | modelarts:workspace:get<br>modelarts:workspace:getQuotas                                                                                                                                                                                                | 在工作流中使用ModelArts工作空间  |

| 业务场景  | 依赖的服务 | 依赖策略项                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | 支持的功能                   |
|-------|-------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|
| 管理数据  | OBS   | obs:bucket:ListAllMybuckets ( 获取桶列表 )<br>obs:bucket:HeadBucket ( 获取桶元数据 )<br>obs:bucket:ListBucket ( 列举桶内对象 )<br>obs:bucket:GetBucketLocation ( 获取桶区域位置 )<br>obs:object:GetObject ( 获取对象内容、获取对象元数据 )<br>obs:object:GetObjectVersion ( 获取对象内容、获取对象元数据 )<br>obs:object:PutObject ( PUT上传、POST上传、复制对象、追加写对象、初始化上传段任务、上传段、合并段 )<br>obs:object:DeleteObject ( 删除对象、批量删除对象 )<br>obs:object:DeleteObjectVersion ( 删除对象、批量删除对象 )<br>obs:object:ListMultipartUploadParts ( 列举已上传的段 )<br>obs:object:AbortMultipartUpload ( 取消多段上传任务 )<br>obs:object:GetObjectAcl ( 获取对象ACL )<br>obs:object:GetObjectVersionAcl ( 获取对象ACL )<br>obs:bucket:PutBucketAcl ( 设置桶ACL )<br>obs:object:PutObjectAcl ( 设置对象ACL ) | 在工作流中使用OBS数据            |
| 工作流运行 | IAM   | iam:users:listUsers ( 查询用户列表 )<br>iam:agencies:getAgency ( 查询指定委托详情 )<br>iam:tokens:assume ( 获取委托Token )                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | 在工作流运行时，调用ModelArts其他服务 |
| 集成DLI | DLI   | dli:jobs:get ( 查询作业详情 )<br>dli:jobs:list_all ( 查询作业列表 )<br>dli:jobs:create ( 创建新作业 )                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | 在工作流中集成DLI              |

| 业务场景  | 依赖的服务 | 依赖策略项                                                                                                                                                                  | 支持的功能      |
|-------|-------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|
| 集成MRS | MRS   | mrs:job:get ( 查询作业详情 )<br>mrs:job:submit ( 创建并执行作业 )<br>mrs:job:list ( 查询作业列表 )<br>mrs:job:stop ( 停止作业 )<br>mrs:job:batchDelete ( 批量删除作业 )<br>mrs:file:list ( 查询文件列表 ) | 在工作流中集成MRS |

表 7-11 管理 AI 应用

| 业务场景   | 依赖的服务 | 依赖策略项                                                                                                                  | 支持的功能                          |
|--------|-------|------------------------------------------------------------------------------------------------------------------------|--------------------------------|
| 管理AI应用 | SWR   | swr:repository:deleteRepository<br>swr:repository:deleteTag<br>swr:repository:getRepository<br>swr:repository:listTags | 从自定义镜像导入<br>从OBS导入时使用<br>自定义引擎 |

| 业务场景 | 依赖的服务 | 依赖策略项                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | 支持的功能                   |
|------|-------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|
|      | OBS   | obs:bucket:ListAllMybuckets ( 获取桶列表 )<br>obs:bucket:HeadBucket ( 获取桶元数据 )<br>obs:bucket:ListBucket ( 列举桶内对象 )<br>obs:bucket:GetBucketLocation ( 获取桶区域位置 )<br>obs:object:GetObject ( 获取对象内容、获取对象元数据 )<br>obs:object:GetObjectVersion ( 获取对象内容、获取对象元数据 )<br>obs:object:PutObject ( PUT上传、POST上传、复制对象、追加写对象、初始化上传段任务、上传段、合并段 )<br>obs:object:DeleteObject ( 删除对象、批量删除对象 )<br>obs:object:DeleteObjectVersion ( 删除对象、批量删除对象 )<br>obs:object:ListMultipartUploadParts ( 列举已上传的段 )<br>obs:object:AbortMultipartUpload ( 取消多段上传任务 )<br>obs:object:GetObjectAcl ( 获取对象ACL )<br>obs:object:GetObjectVersionAcl ( 获取对象ACL )<br>obs:bucket:PutBucketAcl ( 设置桶ACL )<br>obs:object:PutObjectAcl ( 设置对象ACL ) | 从OBS导入模型<br>模型转换指定OBS路径 |

表 7-12 管理部署上线

| 业务场景 | 依赖的服务 | 依赖策略项                    | 支持的功能      |
|------|-------|--------------------------|------------|
| 在线服务 | LTS   | lts:logs:list ( 查询日志列表 ) | 查询和展示LTS日志 |

| 业务场景 | 依赖的服务 | 依赖策略项                                                                                                                                                                                                              | 支持的功能          |
|------|-------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------|
|      | OBS   | obs:bucket:GetBucketPolicy (获取桶策略)<br>obs:bucket:HeadBucket (获取桶元数据)<br>obs:bucket:ListAllMyBuckets (获取桶列表)<br>obs:bucket:PutBucketPolicy (设置桶策略)<br>obs:bucket>DeleteBucketPolicy (删除桶策略)                         | 服务运行时容器挂载外部存储卷 |
| 批量服务 | OBS   | obs:object:GetObject (获取对象内容、获取对象元数据)<br>obs:object:PutObject (PUT上传、POST上传、复制对象、追加写对象、初始化上传段任务、上传段、合并段)<br>obs:bucket>CreateBucket (创建桶)<br>obs:bucket:ListBucket (列举桶内对象)<br>obs:bucket:ListAllMyBuckets (获取桶列表) | 创建批量服务，批量推理。   |
| 边缘服务 | CES   | ces:metricData:list (查询指标数据)                                                                                                                                                                                       | 查看服务的监控指标      |
|      | IEF   | ief:deployment:delete (删除应用部署)                                                                                                                                                                                     | 管理边缘服务         |

表 7-13 管理数据集

| 业务场景     | 依赖的服务 | 依赖策略项                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | 支持的功能                             |
|----------|-------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------|
| 管理数据集和标注 | OBS   | obs:bucket:ListBucket (列举桶内对象)<br>obs:object:GetObject (获取对象内容、获取对象元数据)<br>obs:object:PutObject (PUT上传、POST上传、复制对象、追加写对象、初始化上传段任务、上传段、合并段)<br>obs:object:DeleteObject (删除对象、批量删除对象)<br>obs:bucket:HeadBucket (获取桶元数据)<br>obs:bucket:GetBucketAcl (获取桶ACL)<br>obs:bucket:PutBucketAcl (设置桶ACL)<br>obs:bucket:GetBucketPolicy (获取桶策略)<br>obs:bucket:PutBucketPolicy (设置桶策略)<br>obs:bucket:DeleteBucketPolicy (删除桶策略)<br>obs:bucket:PutBucketCORS (设置桶的CORS配置、删除桶的CORS配置)<br>obs:bucket:GetBucketCORS (获取桶的CORS配置)<br>obs:object:PutObjectAcl (设置对象ACL) | 管理OBS中的数据集<br>标注OBS数据<br>创建数据管理作业 |
| 管理表格数据集  | DLI   | dli:database:displayAllDatabases<br>dli:database:displayAllTables<br>dli:table:describe_table                                                                                                                                                                                                                                                                                                                                                                                                                                                        | 在数据集中管理 DLI 数据                    |
| 管理表格数据集  | DWS   | dws:openAPICluster:list<br>dws:openAPICluster:getDetail                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | 在数据集中管理 DWS 数据                    |
| 管理表格数据集  | MRS   | mrs:job:submit<br>mrs:job:list<br>mrs:cluster:list<br>mrs:cluster:get                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | 在数据集中管理 MRS 数据                    |

| 业务场景 | 依赖的服务     | 依赖策略项                                                                                                                                                                                       | 支持的功能  |
|------|-----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------|
| 智能标注 | ModelArts | modelarts:service:list<br>modelarts:model:list<br>modelarts:model:get<br>modelarts:model:create<br>modelarts:trainJobInnerModel:list<br>modelarts:workspace:get<br>modelarts:workspace:list | 使用智能标注 |
| 团队标注 | IAM       | iam:projects:listProjects ( 查询租户项目 )<br>iam:users:listUsers ( 查询用户列表 )<br>iam:agencies:createAgency ( 创建委托 )<br>iam:quotas:listQuotasForProject ( 查询指定项目的配额 )                               | 管理标注团队 |

表 7-14 资源管理

| 业务场景  | 依赖的服务 | 依赖策略项                                                                                                                                                                                                                       | 支持的功能                                     |
|-------|-------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------|
| 资源池管理 | BSS   | bss:coupon:view<br>bss:order:view<br>bss:balance:view<br>bss:discount:view<br>bss:renewal:view<br>bss:bill:view<br>bss:contract:update<br>bss:order:pay<br>bss:unsubscribe:update<br>bss:renewal:update<br>bss:order:update | 资源池的创建、续费、退订等与计费相关的功能。依赖权限需要配置在IAM项目视图中。  |
|       | CCE   | cce:cluster:list<br>cce:cluster:get                                                                                                                                                                                         | 获取CCE集群列表、集群详情、集群证书等信息。依赖权限需要配置在IAM项目视图中。 |



| 业务场景 | 依赖的服务 | 依赖策略项                                                                                                                                                                                                                      | 支持的功能                             |
|------|-------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------|
|      | KMS   | kms:cmk:list<br>kms:cmk:getMaterial                                                                                                                                                                                        | 获取用户创建的密钥对列表信息。依赖权限需要配置在IAM项目视图中。 |
|      | AOM   | aom:metric:get                                                                                                                                                                                                             | 获取资源池的监控数据。依赖权限需要配置在IAM项目视图中。     |
|      | OBS   | obs:bucket:ListAllMybuckets<br>obs:bucket:HeadBucket<br>obs:bucket:ListBucket<br>obs:bucket:GetBucketLocation<br>obs:object:GetObject<br>obs:object:PutObject<br>obs:object:DeleteObject<br>obs:object:DeleteObjectVersion | 获取AI诊断日志。依赖权限需要配置在IAM项目视图中。       |
|      | ECS   | ecs:availabilityZones:list                                                                                                                                                                                                 | 查询可用区列表。依赖权限需要配置在IAM项目视图中。        |

| 业务场景 | 依赖的服务     | 依赖策略项                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | 支持的功能                                         |
|------|-----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------|
| 网络管理 | VPC       | vpc:routes:create<br>vpc:routes:list<br>vpc:routes:get<br>vpc:routes:delete<br>vpc:peerings:create<br>vpc:peerings:accept<br>vpc:peerings:get<br>vpc:peerings:delete<br>vpc:routeTables:update<br>vpc:routeTables:get<br>vpc:routeTables:list<br>vpc:vpcs:create<br>vpc:vpcs:list<br>vpc:vpcs:get<br>vpc:vpcs:delete<br>vpc:subnets:create<br>vpc:subnets:get<br>vpc:subnets:delete<br>vpcep:endpoints:list<br>vpcep:endpoints:create<br>vpcep:endpoints:delete<br>vpcep:endpoints:get<br>vpc:ports:create<br>vpc:ports:get<br>vpc:ports:update<br>vpc:ports:delete<br>vpc:networks:create<br>vpc:networks:get<br>vpc:networks:update<br>vpc:networks:delete | ModelArts网络资源创建和删除、VPC网络打通。依赖权限需要配置在IAM项目视图中。 |
|      | SFS Turbo | sfsturbo:shares:addShareNic<br>sfsturbo:shares:deleteShareNic<br>sfsturbo:shares:showShareNic<br>sfsturbo:shares:listShareNics                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 用户的网络和SFS Turbo资源打通。依赖权限需要配置在IAM项目视图中。        |

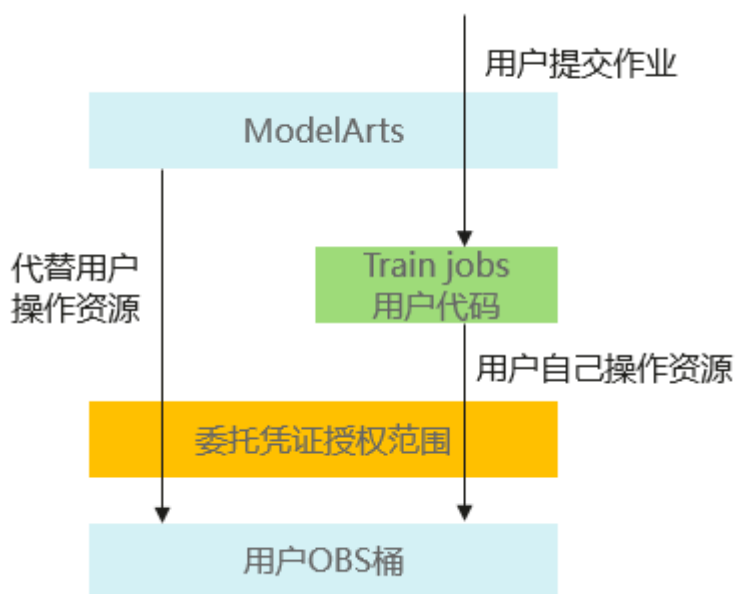
| 业务场景  | 依赖的服务 | 依赖策略项                                                                                                                                                                                                                                                                    | 支持的功能     |
|-------|-------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|
| 边缘资源池 | IEF   | ief:node:list<br>ief:group:get<br>ief:application:list<br>ief:application:get<br>ief:node:listNodeCert<br>ief:node:get<br>ief:IEFInstance:get<br>ief:deployment:list<br>ief:group:listGroupInstanceState<br>ief:IEFInstance:list<br>ief:deployment:get<br>ief:group:list | 边缘池增删改查管理 |

## 委托授权

用户在使用ModelArts服务运行作业过程中，为了简化用户的操作，ModelArts后台可以代替用户完成一些工作，如训练作业启动前自动下载用户OBS桶中的数据集到作业空间、自动转储训练作业日志到用户OBS桶中。

ModelArts服务不会保存用户的Token认证凭据，在后台异步作业中操作用户的资源（如OBS桶）前，需要用户通过IAM委托向ModelArts显式授权，ModelArts在需要时使用用户的委托获取临时认证凭据用于操作用户资源，见“[添加授权](#)”。

图 7-6 委托授权



如图7-6所示，用户向ModelArts授权后，ModelArts使用委托授权的临时凭证访问和操作用户资源，协助用户自动化一些繁琐和耗时的操作。同时，委托凭证会同步到用户的作业中（Notebook实例和训练作业），客户在作业中可以使用委托凭证自行访问自己的资源。

### 在ModelArts服务中委托授权有两种方式：

#### 1、一键式委托授权

ModelArts提供了一键式自动授权功能，用户可以在ModelArts的全局配置功能中，快速完成委托授权，由ModelArts为用户自动创建委托并配置到ModelArts服务中。

这种方式为保证使用业务过程中有足够的权限，基于依赖服务的预置系统策略指定授权范围，创建的委托的权限比较大，基本覆盖了依赖服务的全部权限。如果您需要对委托授权的权限范围进行精确控制，请使用第二种方式。

#### 2、定制化委托授权

管理员在IAM中为不同用户创建不同的委托授权策略，再到ModelArts中为用户配置已创建好的委托。管理员在IAM中为用户创建委托时，根据用户的实际权限范围为委托指定最小权限范围，控制用户在使用ModelArts过程中可访问的资源内容。具体参考[配置ModelArts基本使用权限](#)。

### 委托授权的越权风险

可以看到用户的委托授权是独立的，理论上用户的委托授权范围是可以超出用户自身用户组的授权策略的授权范围，如果配置不当就会出现用户越权的问题。

为了控制委托授权的越权风险，ModelArts服务的全局配置功能要求只有租户管理员才能为用户配置委托，由管理员保证委托授权的安全性。

### 委托授权的最小化

管理员在配置委托授权时，应严格控制授权的范围。

ModelArts为用户异步自动化完成作业的准备、清理等操作，所需的委托授权内容是基础授权范围。如果用户只使用ModelArts的部分功能，管理员可以依据委托授权表格的说明屏蔽不使用的基础权限项。相反地，如果用户需要在作业中使用基础授权范围外的资源权限，管理员也可以为用户在委托授权中增加新的权限项。总之，委托授权的范围应该基于实际业务场景所需权限范围来进行定制，保持委托授权范围的最小化。

### 委托基础授权范围

当您需要定制委托授权的权限列表时，请参考下面表格，根据实际业务选择授权项。

表 7-15 开发环境基础委托授权

| 业务场景       | 依赖的服务 | 委托授权项                                                                                                                                                                                                                                                                       | 说明                                                    | 配置建议  |
|------------|-------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------|-------|
| JupyterLab | OBS   | obs:object:DeleteObject<br>obs:object:GetObject<br>obs:object:GetObjectVersion<br>obs:bucket>CreateBucket<br>obs:bucket:ListBucket<br>obs:bucket:ListAllMyBuckets<br>obs:object:PutObject<br>obs:bucket:GetBucketAcl<br>obs:bucket:PutBucketAcl<br>obs:bucket:PutBucketCORS | 通过ModelArts的Notebook，在JupyterLab中使用OBS上传下载数据。         | 建议配置。 |
| 开发环境监控功能   | AOM   | aom:alarm:put                                                                                                                                                                                                                                                               | 调用AOM的接口，获取Notebook相关的监控数据和事件，展示在ModelArts的Notebook中。 | 建议配置。 |

表 7-16 训练作业基础委托授权

| 业务场景 | 依赖的服务 | 委托授权项                                                                 | 说明                                    |
|------|-------|-----------------------------------------------------------------------|---------------------------------------|
| 训练作业 | OBS   | obs:bucket:ListBucket<br>obs:object:GetObject<br>obs:object:PutObject | 训练作业启动前下载数据、模型、代码。<br>训练作业运行中上传日志、模型。 |

表 7-17 部署上线基础委托授权

| 业务场景 | 依赖的服务 | 委托授权项                                                                                             | 说明            |
|------|-------|---------------------------------------------------------------------------------------------------|---------------|
| 在线服务 | LTS   | lts:groups:create<br>lts:groups:list<br>lts:topics:create<br>lts:topics:delete<br>lts:topics:list | 在线服务配置LTS日志上报 |

| 业务场景 | 依赖的服务 | 委托授权项                                                                                                                                                              | 说明          |
|------|-------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|
| 批量服务 | OBS   | obs:bucket:ListBucket<br>obs:object:GetObject<br>obs:object:PutObject                                                                                              | 运行批量服务      |
| 边缘服务 | IEF   | ief:deployment:list<br>ief:deployment:create<br>ief:deployment:update<br>ief:deployment:delete<br>ief:node:createNodeCert<br>ief:iefInstance:list<br>ief:node:list | 通过IEF部署边缘服务 |

表 7-18 数据管理基础委托授权

| 业务场景     | 依赖的服务       | 委托授权项                                                                                                                                                                                                                                                                                                                                                           | 说明                    |
|----------|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|
| 数据集和数据标注 | OBS         | obs:object:GetObject<br>obs:object:PutObject<br>obs:object:DeleteObject<br>obs:object:PutObjectAcl<br>obs:bucket:ListBucket<br>obs:bucket:HeadBucket<br>obs:bucket:GetBucketAcl<br>obs:bucket:PutBucketAcl<br>obs:bucket:GetBucketPolicy<br>obs:bucket:PutBucketPolicy<br>obs:bucket:DeleteBucketPolicy<br>obs:bucket:PutBucketCORS<br>obs:bucket:GetBucketCORS | 管理OBS桶中的数据集           |
| 数据标注     | ModelArts推理 | modelarts:service:get<br>modelarts:service:create<br>modelarts:service:update                                                                                                                                                                                                                                                                                   | 基于ModelArts推理进行智能数据标注 |

表 7-19 专属资源池管理基础委托授权

| 业务场景             | 依赖的服务     | 委托授权项                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | 说明                                              |
|------------------|-----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------|
| 资源池网络管理<br>(新版本) | VPC       | vpc:routes:create<br>vpc:routes:list<br>vpc:routes:get<br>vpc:routes:delete<br>vpc:peerings:create<br>vpc:peerings:accept<br>vpc:peerings:get<br>vpc:peerings:delete<br>vpc:routeTables:update<br>vpc:routeTables:get<br>vpc:routeTables:list<br>vpc:vpcs:create<br>vpc:vpcs:list<br>vpc:vpcs:get<br>vpc:vpcs:delete<br>vpc:subnets:create<br>vpc:subnets:get<br>vpc:subnets:delete<br>vpcep:endpoints:list<br>vpcep:endpoints:create<br>vpcep:endpoints:delete<br>vpcep:endpoints:get<br>vpc:ports:create<br>vpc:ports:get<br>vpc:ports:update<br>vpc:ports:delete<br>vpc:networks:create<br>vpc:networks:get<br>vpc:networks:update<br>vpc:networks:delete | ModelArts网络资源创建和删除、VPC网络打通。此处依赖权限需要配置在IAM项目视图中。 |
|                  | SFS Turbo | sfsturbo:shares:addShareNic<br>sfsturbo:shares:deleteShareNic<br>sfsturbo:shares:showShareNic<br>sfsturbo:shares:listShareNics                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 用户的网络和SFS Turbo资源打通。依赖权限需要配置在IAM项目视图中。          |

| 业务场景  | 依赖的服务 | 委托授权项                                                                                                                                                                                                                       | 说明                                       |
|-------|-------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------|
| 资源池管理 | BSS   | bss:coupon:view<br>bss:order:view<br>bss:balance:view<br>bss:discount:view<br>bss:renewal:view<br>bss:bill:view<br>bss:contract:update<br>bss:order:pay<br>bss:unsubscribe:update<br>bss:renewal:update<br>bss:order:update | 资源池的创建、续费、退订等与计费相关的功能。依赖权限需要配置在IAM项目视图中。 |
| 资源池管理 | ECS   | ecs:availabilityZones:list                                                                                                                                                                                                  | 查询可用区列表。依赖权限需要配置在IAM项目视图中。               |

表 7-20 workflow 基础委托授权

| 业务场景   | 依赖的服务     | 委托授权项                                                                                                                                                                                                                                                                                                   | 说明                    |
|--------|-----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|
| 使用数据集  | ModelArts | modelarts:dataset:getDataset<br>modelarts:dataset:createDataset<br>modelarts:dataset:createDatasetVersion<br>modelarts:dataset:createImportTask<br>modelarts:dataset:updateDataset<br>modelarts:processTask:createProcessTask<br>modelarts:processTask:getProcessTask<br>modelarts:dataset:listDatasets | 在工作流中使用ModelArts数据集   |
| 管理AI应用 | ModelArts | modelarts:model:list<br>modelarts:model:get<br>modelarts:model:create<br>modelarts:model:delete<br>modelarts:model:update                                                                                                                                                                               | 在工作流中管理ModelArts AI应用 |



| 业务场景  | 依赖的服务     | 委托授权项                                                                                                                                                                                                                                                   | 说明                      |
|-------|-----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|
| 部署上线  | ModelArts | modelarts:service:get<br>modelarts:service:create<br>modelarts:service:update<br>modelarts:service:delete<br>modelarts:service:getLogs                                                                                                                  | 在工作流中管理ModelArts在线服务    |
| 训练作业  | ModelArts | modelarts:trainJob:get<br>modelarts:trainJob:create<br>modelarts:trainJob:list<br>modelarts:trainJobVersion:list<br>modelarts:trainJobVersion:create<br>modelarts:trainJob:delete<br>modelarts:trainJobVersion:delete<br>modelarts:trainJobVersion:stop | 在工作流中管理ModelArts训练作业    |
| 工作空间  | ModelArts | modelarts:workspace:get<br>modelarts:workspace:getQuotas                                                                                                                                                                                                | 在工作流中使用ModelArts工作空间    |
| 管理数据  | OBS       | obs:bucket:GetBucketPolicy<br>obs:bucket:PutBucketPolicy<br>obs:bucket:GetBucketAcl<br>obs:bucket:PutBucketAcl<br>obs:object:GetObject<br>obs:object:PutObject<br>obs:bucket:ListBucket<br>obs:object:PutObjectAcl<br>obs:object:DeleteObject           | 在工作流中使用OBS数据            |
| 工作流运行 | IAM       | iam:users:listUsers ( 查询用户列表 )<br>iam:agencies:getAgency ( 查询指定委托详情 )<br>iam:tokens:assume ( 获取委托Token )                                                                                                                                                | 在工作流运行时,调用ModelArts其他服务 |
| 集成DLI | DLI       | dli:jobs:get<br>dli:jobs:listAll<br>dli:jobs:create<br>dli:jobs:stop                                                                                                                                                                                    | 在工作流中集成DLI              |

| 业务场景  | 依赖的服务 | 委托授权项                                                                                                 | 说明         |
|-------|-------|-------------------------------------------------------------------------------------------------------|------------|
| 集成MRS | MRS   | mrs:job:get<br>mrs:job:submit<br>mrs:job:list<br>mrs:job:stop<br>mrs:job:batchDelete<br>mrs:file:list | 在工作流中集成MRS |

## 7.2.3 工作空间

ModelArts的用户需要为不同的业务目标开发算法、管理和部署模型，此时可以创建多个工作空间，把不同应用开发过程的输出内容划分到不同工作空间中，便于管理和使用。

工作空间支持3种访问控制：

- PUBLIC：租户（主账号和所有子账号）内部公开访问。
- PRIVATE：仅创建者和主账号可访问。
- INTERNAL：创建者、主账号、指定IAM子账号可访问当授权类型为INTERNAL时需要指定可访问的子账号的账号名，可选择多个。

每个账号每个IAM项目都会分配1个默认工作空间，默认工作空间的访问控制为PUBLIC。

通过工作空间的访问控制能力，可限制仅允许部分人访问对应的工作空间。通过此功能可实现类似如下场景：

- **教育场景**：老师可给每个学生分配1个INTERNAL的工作空间并且限制该工作空间被指定学生访问，这样可使得学生可独立完成在ModelArts上的实验。
- **企业场景**：管理者可创建用于生产任务的工作空间并限制仅让运维人员使用，用于日常调试的工作空间并限制仅让开发人员使用。通过这种方式让不同的企业角色只能在指定工作空间下使用资源。

目前工作空间功能是“受邀开通”状态，作为企业用户您可以通过您对口的技术支持申请开通。

## 7.3 典型场景配置实践

### 7.3.1 个人用户快速配置 ModelArts 访问权限

ModelArts使用过程中涉及到OBS、SWR等服务交互，需要用户配置委托授权，允许ModelArts访问这些依赖服务。如果没有授权，ModelArts的部分功能将不能正常使用。

## 约束与限制

- 只有主账号可以使用委托授权，可以为当前账号授权，也可以为当前账号下的所有IAM用户授权。
- 多个IAM用户或账号，可使用同一个委托。
- 一个账号下，最多可创建50个委托。
- 对于首次使用ModelArts新用户，请直接新增委托即可。一般用户新增普通用户权限即可满足使用要求。如果有精细化权限管理的需求，可以自定义权限按需设置。
- 如果未获得委托授权，当打开“访问授权”页面时，ModelArts会提醒您当前用户未配置授权，需联系此IAM用户的管理员账号进行委托授权。

## 添加授权

1. 登录ModelArts管理控制台，在左侧导航栏选择“全局配置”，进入“全局配置”页面。
2. 单击“添加授权”，进入“访问授权”配置页面，根据参数说明进行配置。

表 7-21 参数说明

| 参数       | 说明                                                                                                                                                                                                                                                                                                                                                                                                       |
|----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| “授权对象类型” | <p>包括IAM子用户、联邦用户、委托用户和所有用户。</p> <ul style="list-style-type: none"> <li>● IAM子用户：由主账号在IAM中创建的用户，是服务的使用人员，具有独立的身份凭证（密码和访问密钥），根据账号授予的权限使用资源。IAM子用户相关介绍请参见<a href="#">IAM用户介绍</a>。</li> <li>● 联邦用户：又称企业虚拟用户。联邦用户相关介绍请参见<a href="#">联邦身份认证</a>。</li> <li>● 委托用户：IAM中创建的一个委托。IAM创建委托相关介绍请参见<a href="#">创建委托</a>。</li> <li>● 所有用户：该选项表示会将委托的权限授权到当前账号下的所有子账号、包括未来创建的子账号，授权范围较大，需谨慎使用。个人用户选择“所有用户”即可。</li> </ul> |

| 参数            | 说明                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| “授权对象”        | <p>“授权对象类型”选择“所有用户”时不涉及此参数。</p> <ul style="list-style-type: none"> <li>IAM子用户：选择指定的IAM子用户，给指定的IAM子用户配置委托授权。</li> </ul> <p><b>图 7-7 选择 IAM 子用户</b></p>  <ul style="list-style-type: none"> <li>联邦用户：输入联邦用户的用户名或用户ID。</li> </ul> <p><b>图 7-8 选择联邦用户</b></p>  <ul style="list-style-type: none"> <li>委托用户：选择委托名称。使用账号A创建一个权限委托，在此处将该委托授权给账号B拥有的委托。在使用账号B登录控制台时，可以在控制台右上角的个人账号切换角色到账号A，使用账号A的委托权限。</li> </ul> <p><b>图 7-9 委托用户切换角色</b></p>  |
| “委托选择”        | <ul style="list-style-type: none"> <li>已有委托：列表中如果已有委托选项，则直接选择一个可用的委托为上述选择的用户授权。单击委托名称查看该委托的权限详情。</li> <li>新增委托：如果没有委托可选，可以在新增委托中创建委托权限。对于首次使用ModelArts的用户，需要新增委托。</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| “新增委托 > 委托名称” | 系统自动创建委托名称，用户可以手动修改。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |

| 参数                   | 说明                                                                                                                                                                                                                                                                                                                                                            |
|----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| “新增委托 > 授权方式”        | <ul style="list-style-type: none"> <li>角色授权：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。由于华为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。</li> <li>策略授权：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。</li> </ul> <p>角色与策略相关介绍请参考<a href="#">权限基本概念</a>。</p> |
| “新增委托 > 权限配置 > 普通用户” | <p>普通用户包括用户使用ModelArts完成AI开发的所有必要功能权限，如数据的访问、训练任务的创建和管理等。一般用户选择此项即可。</p> <p>可以单击“查看权限列表”，查看普通用户权限。</p>                                                                                                                                                                                                                                                        |
| “新增委托 > 权限配置 > 自定义”  | <p>如用户有精细化权限管理的需求，可使用自定义模式灵活按需配置ModelArts创建的委托权限。可以根据实际需要在权限列表中勾选要配置的权限。</p>                                                                                                                                                                                                                                                                                  |

- 然后勾选“我已经仔细阅读并同意《ModelArts服务声明》”，单击“创建”，即可完成委托配置。

## 查看授权的权限列表

用户可以在“全局配置”页面的授权列表中，查看已经配置的委托授权内容。单击授权内容列的“查看权限”，可以查看该授权的权限详情。

图 7-10 查看权限

| 授权对象 | 授权对象类型 | 授权类型 | 授权内容 | 创建时间                          | 操作                   |
|------|--------|------|------|-------------------------------|----------------------|
|      | IAM子用户 | 委托   |      | 2023-12-28 09:31:54 GMT+08:00 | <a href="#">查看权限</a> |

图 7-11 普通用户权限列表

| 权限名称                       | 使用模块                                        | 描述                                 |
|----------------------------|---------------------------------------------|------------------------------------|
| OBS Administrator          | 数据管理   开发环境   训练管理   AI应用管理   部署上线   AI ... | 对象存储服务管理员                          |
| DLI FullAccess             | 数据管理                                        | 数据湖探索的所有执行权限                       |
| MRS Administrator          | 数据管理                                        | MapReduce服务 (MRS) 管理员，拥有该服务下的所有权限  |
| DWS Administrator          | 数据管理                                        | 数据仓库服务 (DWS) 管理员，拥有该服务下的所有权限       |
| VPC Administrator          | 训练管理   AI应用管理   部署上线   专属资源池                | 虚拟私有云管理员                           |
| CES ReadOnlyAccess         | AI应用管理   部署上线                               | 云监控服务只读权限                          |
| SMN Administrator          | 训练管理   AI应用管理   部署上线                        | 消息通知服务管理员                          |
| EPS FullAccess             | 训练管理   AI应用管理   部署上线                        | 企业项目管理服务所有权限                       |
| CTS Administrator          | 数据管理   开发环境   训练管理   AI应用管理   部署上线   AI ... | 云审计服务 (CTS) 管理员，拥有该服务下的所有权限        |
| SFS ReadOnlyAccess         | 训练管理                                        | 弹性文件服务只读权限                         |
| LTS FullAccess             | AI应用管理   部署上线                               | 云日志服务所有权限                          |
| ModelArts CommonOperations | 数据管理   开发环境   训练管理   AI应用管理   部署上线   AI ... | ModelArts服务普通用户权限 (不包括创建、更新、删除专... |

## 7.3.2 配置 ModelArts 基本使用权限

### 7.3.2.1 场景描述

ModelArts作为顶层服务，其部分功能依赖于其他服务的访问权限。本章节主要介绍对于IAM子用户使用ModelArts时，如何根据需要开通的功能配置子用户相应权限。

### 权限列表

子用户的权限，由主用户来控制，主用户通过IAM的权限配置功能设置用户组的权限，从而控制用户组内的子用户的权限。此处的授权列表均按照ModelArts和其他服务的系统预置策略来举例。

表 7-22 服务授权列表

| 待授权的服务    | 授权说明                                                                                         | IAM权限设置                    | 是否必选                                                                  |
|-----------|----------------------------------------------------------------------------------------------|----------------------------|-----------------------------------------------------------------------|
| ModelArts | 授予子用户使用ModelArts服务的权限。<br>ModelArts CommonOperations没有任何专属资源池的创建、更新、删除权限，只有使用权限。推荐给子用户配置此权限。 | ModelArts CommonOperations | 必选                                                                    |
|           | 如果需要给子用户开通专属资源池的创建、更新、删除权限，此处要勾选ModelArts FullAccess，请谨慎配置。                                  | ModelArts FullAccess       | 可选<br>ModelArts FullAccess权限和ModelArts CommonOperations权限只能二选一，不能同时选。 |
| OBS对象存储服务 | 授予子用户使用OBS服务的权限。ModelArts的数据管理、开发环境、训练作业、模型推理部署均需要通过 <b>OBS进行数据中转</b> 。                      | OBS OperateAccess          | 必选                                                                    |
| SWR容器镜像仓库 | 授予子用户使用SWR服务权限。ModelArts的 <b>自定义镜像功能</b> 依赖镜像服务SWR FullAccess权限。                             | SWR OperateAccess          | 必选                                                                    |
| 密钥管理服务    | 当子用户使用ModelArts <b>Notebook的SSH远程功能</b> 时，需要配置子用户密钥管理服务的使用权限。                                | KMS CMKFullAccess          | 可选                                                                    |

| 待授权的服务    | 授权说明                                                                   | IAM权限设置                                | 是否必选 |
|-----------|------------------------------------------------------------------------|----------------------------------------|------|
| IEF智能边缘平台 | 授予子用户智能边缘平台使用权限，ModelArts的边缘服务依赖智能边缘平台，要求配置Tenant Administrator权限。     | Tenant Administrator                   | 可选   |
| CES云监控    | 授予子用户使用CES云监控服务的权限。通过CES云监控可以查看ModelArts的在线服务和对应模型负载运行状态的整体情况，并设置监控告警。 | CES FullAccess                         | 可选   |
| SMN消息服务   | 授予子用户使用SMN消息服务的权限。SMN消息通知服务配合CES监控告警功能一起使用。                            | SMN FullAccess                         | 可选   |
| VPC虚拟私有云  | 子用户在创建ModelArts的专属资源池过程中，如果需要开启自定义网络配置，需要配置VPC权限。                      | VPC FullAccess                         | 可选   |
| SFS弹性文件服务 | 授予子用户使用SFS服务的权限，ModelArts的专属资源池中可以挂载SFS系统作为开发环境或训练的存储。                 | SFS Turbo FullAccess<br>SFS FullAccess | 可选   |

### 7.3.2.2 Step1 创建用户组并加入用户

主用户账号下面可以创建多个子用户，并对子用户的权限进行分组管理。此步骤介绍如何创建用户组、子用户、并将子用户加入用户组中。

1. 主用户登录管理控制台，单击右上角用户名，在下拉框中选择“统一身份认证”，进入IAM服务。

图 7-12 登录控制台



2. 创建用户组。在左侧菜单栏中，选择“用户组”。单击右上角“创建用户组”，在“用户组名称”中填入“用户组02”，然后单击“确定”完成用户组创建。

图 7-13 创建用户组

用户组 / 创建用户组

\* 用户组名称

描述

0/255

创建完成后，返回用户组列表。通过用户组管理，将已有子用户加入到用户组中。如果没有子用户账号，可以创建子用户并加入用户组。

3. 创建子用户账号并加入用户组。在IAM左侧菜单栏中，选择“用户”，单击右上角“创建用户”，在“创建用户”页面中，添加多个用户。请根据界面提示，填写必选参数，然后单击“下一步”。

图 7-14 创建多个用户

用户 / 创建用户

1 配置用户基本信息

2 加入用户组 (可选)

\* 用户信息 用户名、邮件地址、手机号均可作为IAM用户的登录凭证，建议您完整填写。

| * 用户名                                    | * 邮件地址                        | 手机号                   |
|------------------------------------------|-------------------------------|-----------------------|
| <input type="text" value="test-user01"/> | <input type="text"/>          | +86 (中...   手机号 (选填)) |
| <input type="text" value="test-user02"/> | <input type="text" value=""/> | +86 (中...   手机号 (选填)) |

添加用户 您本次还可以创建8个用户。

4. 在“加入用户组”步骤中，选择“用户组02”，然后单击“创建用户”。



图 7-15 加入用户组



系统将逐步创建好前面设置的2个用户。

### 7.3.2.3 Step2 为用户配置云服务使用权限

主用户为子用户授予ModelArts、OBS等云服务的使用权限后，子用户才可以使用这些云服务。此步骤介绍如何为用户组中的所有子用户授予使用ModelArts、OBS、SWR等各类云服务的权限。

1. 主用户在IAM服务的用户组列表页面，单击“授权”，进入到授权页面，为子用户配置权限。

图 7-16 为用户组授权

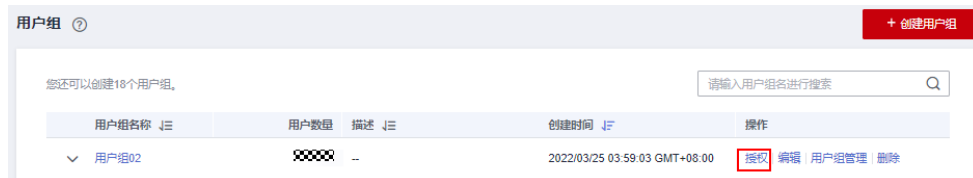


图 7-17 进入授权页面



2. 配置授权前，请先了解ModelArts各模块使用到的最小权限要求，如表7-22所示。
3. 配置ModelArts使用权限。如下图，搜索ModelArts。ModelArts FullAccess权限和ModelArts CommonOperations权限只能二选一，不能同时选。

选择说明如下：

- ModelArts CommonOperations没有任何专属资源池的创建、更新、删除权限，只有使用权限。推荐给子用户配置此权限。
- 如果需要给子用户开通专属资源池的创建、更新、删除权限，此处要勾选ModelArts FullAccess，请谨慎配置。

图 7-18 配置 ModelArts 使用权限



4. 配置OBS使用权限。如下图，搜索OBS，勾选“OBS Administrator”。ModelArts训练作业中需要依赖OBS作为数据中转站，需要配置OBS的使用权限。

图 7-19 配置 OBS 使用权限



5. 配置SWR使用权限。如下图，搜索SWR，勾选“SWR FullAccess”。ModelArts的自定义镜像功能依赖镜像服务SWR FullAccess权限。

图 7-20 配置 SWR 使用权限



6. （可选）配置密钥管理权限。如果需要使用ModelArts Notebook的SSH访问功能，依赖密钥管理权限。如下图，搜索DEW，勾选“DEW KeypairFullAccess”。

此处需要注意以下Region配置的是DEW密钥管理权限：华北-北京一、华北-北京四、华东-上海一、华东-上海二、华南-广州、西南-贵阳一、中国-香港、亚太-新加坡。其他Region配置的是KMS密钥管理权限。本示例中使用“华南-广州”Region举例，所以需要配置DEW密钥管理权限。

图 7-21 DEW 密钥管理权限



图 7-22 KMS 密钥管理权限



7. (可选) 配置智能边缘平台使用权限。ModelArts的边缘服务依赖智能边缘平台，要求配置Tenant Administrator权限。

注意：Tenant Administrator权限比较大，包含全部云服务的管理权限，而不仅是使用ModelArts服务。请谨慎配置。

图 7-23 配置智能边缘平台使用权限



8. (可选) 配置CES云监控和SMN消息通知使用权限。ModelArts推理部署的在线服务详情页面内有调用次数详情，单击可查看该在线服务的调用次数随时间详细分布的情况。如果想进一步通过CES云监控查看ModelArts的在线服务和对应模型负载运行状态的整体情况，需要给予用户授予CES权限。

如果只是查看监控，给予用户授予CES ReadOnlyAccess权限即可。

图 7-24 CES 云监控 CES ReadOnlyAccess 权限



如果还需要在CES上设置监控告警，则需要再加上CES FullAccess权限，以及SMN消息通知权限。

图 7-25 CES 云监控设置监控告警权限



图 7-26 SMN 消息通知权限



- (可选) 配置VPC权限。如果用户在创建专属资源池过程中，需要开启自定义网络配置，此处需要授予用户VPC权限。

图 7-27 配置 VPC 权限



- (可选) 配置SFS和SFS Turbo权限。如果用户在专属资源池中挂载SFS系统作为开发环境或训练的存储时，需要授予使用权限。

图 7-28 配置 SFS 和 SFS Turbo 权限



- 单击左上角的“查看已选”，确认已勾选的权限。

图 7-29 查看已选权限

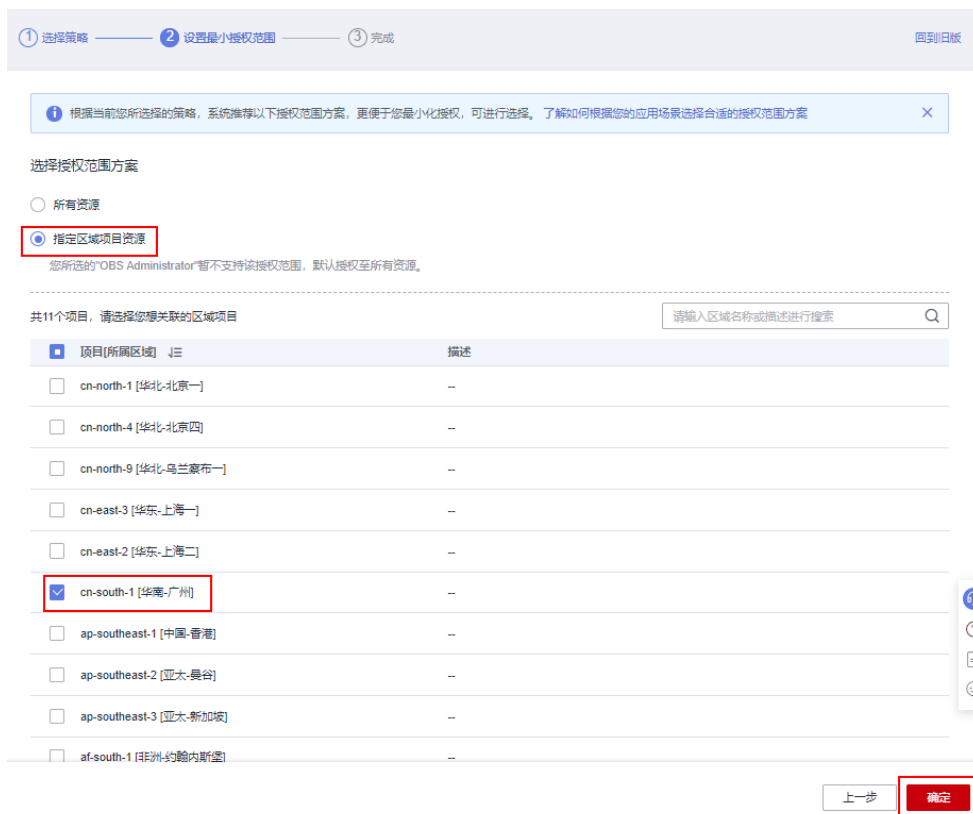
用户组“用户组02”将拥有所选策略



- 再单击“下一步”，设置最小授权范围。单击“指定区域项目资源”，勾选待授权使用的区域，单击“确定”。

本示例以只允许用户使用“华南-广州”Region的服务为例。

图 7-30 选择授权的区域范围



13. 提示授权成功，查看授权信息，单击“完成”。此处的授权生效需要15-30分钟。

### 7.3.2.4 Step3 为用户配置 ModelArts 的委托访问授权

配置完IAM权限之后，需要在ModelArts页面为子用户设置ModelArts访问授权，允许ModelArts访问OBS、SWR、IEF等依赖服务。

此方式只允许主用户为子用户进行配置。因此，本示例中，管理员账号需为所有用户完成访问授权的配置。

1. 使用主用户的账号登录ModelArts服务管理控制台。请注意选择左上角的区域，例如“华南-广州”。

图 7-31 ModelArts 控制台



2. 在左侧导航栏单击“全局配置”，进入“全局配置”页面。
3. 单击“添加授权”。在“授权”页面，在“授权对象类型”下面选择“所有用户”，选择“新增委托”，为该主用户下面的所有子用户配置委托访问授权。
  - 普通用户：普通用户的委托权限包括了用户使用ModelArts完成AI开发的所有必要功能权限，如数据的访问、训练任务的创建和管理等。一般用户选择此项即可。
  - 自定义：如果对用户有更精细化的权限管理需求，可使用自定义模式灵活按需配置ModelArts创建的委托权限。可以根据实际需在权限列表中勾选要配置的权限。

图 7-32 普通用户委托权限

| 权限名称                       | 使用模块                                        | 描述                                 |
|----------------------------|---------------------------------------------|------------------------------------|
| OBS Administrator          | 数据管理   开发环境   训练管理   AI应用管理   部署上线   AI ... | 对象存储服务管理员                          |
| DLI FullAccess             | 数据管理                                        | 数据湖探索的所有执行权限                       |
| MRS Administrator          | 数据管理                                        | MapReduce服务 (MRS) 管理员。拥有该服务下的所有权限  |
| DWS Administrator          | 数据管理                                        | 数据仓库服务 (DWS) 管理员。拥有该服务下的所有权限       |
| VPC Administrator          | 训练管理   AI应用管理   部署上线   专属资源池                | 虚拟私有云管理员                           |
| CES ReadOnlyAccess         | AI应用管理   部署上线                               | 云监控服务只读权限                          |
| SMN Administrator          | 训练管理   AI应用管理   部署上线                        | 消息通知服务管理员                          |
| EPS FullAccess             | 训练管理   AI应用管理   部署上线                        | 企业项目管理服务所有权限                       |
| CTS Administrator          | 数据管理   开发环境   训练管理   AI应用管理   部署上线   AI ... | 云审计服务 (CTS) 管理员。拥有该服务下的所有权限        |
| SFS ReadOnlyAccess         | 训练管理                                        | 弹性文件服务只读权限                         |
| LTS FullAccess             | AI应用管理   部署上线                               | 云日志服务所有权限                          |
| ModelArts CommonOperations | 数据管理   开发环境   训练管理   AI应用管理   部署上线   AI ... | ModelArts服务普通用户权限 (不包括创建、更新、删除专... |
| ECS FullAccess             | 开发环境                                        | 弹性云服务器所有权限                         |

4. 勾选“我已经仔细阅读并同意《ModelArts服务声明》”，单击“创建”，完成委托授权配置。

图 7-33 完成委托授权配置



### 7.3.2.5 Step4 测试用户权限

由于4中的权限需要等待15-30分钟生效，建议在配置完成后，等待30分钟，再执行如下验证操作。

1. 使用用户组02中任意一个子用户登录ModelArts管理控制台。在登录页面，请使用“IAM用户登录”方式进行登录。  
首次登录会提示修改密码，请根据界面提示进行修改。
2. 验证ModelArts权限。
  - a. 在左上角选择区域，区域需与授权配置中的区域相同。本示例以“华南-广州”为例。



- b. 在ModelArts左侧菜单栏中，选择“开发环境>Notebook”，界面未提示权限不足，表明ModelArts的使用权限和委托授权配置成功。

如果提示如图所示信息，说明未配置ModelArts委托访问授权，请参考[Step3 为用户配置ModelArts的委托访问授权](#)，使用主用户为子用户配置ModelArts委托访问授权。

图 7-34 提示权限不足



- c. 在ModelArts左侧菜单栏中，选择“开发环境>Notebook”，单击“创建”，如果可以正常打开创建页面，说明具备ModelArts的操作权限。  
您也可以尝试其他功能，例如“训练管理>训练作业”等，如能正常打开创建页面，即可正常使用ModelArts。

3. 验证OBS权限。
  - a. 在左上角的服务列表中，选择OBS服务，进入OBS管理控制台。
  - b. 在OBS管理控制台，单击右上角的“创建桶”，如果能正常打开页面，表示当前用户具备OBS的操作权限。
4. 验证SWR权限。
  - a. 在左上角的服务列表中，选择SWR服务，进入SWR管理控制台。
  - b. 在SWR管理控制台，如果能正常打开页面，表示当前用户具备SWR的操作权限。
5. 依次验证其他可选权限。
6. 验证结束，当前用户同时具备ModelArts部分功能的操作权限，可正常开始使用ModelArts服务。

### 7.3.3 给予用户配置开发环境基本使用权限

#### 场景描述

本文介绍开发环境场景下子用户所需的基本使用权限，您可参考[权限清单](#)新增对应业务场景的权限。示例场景为授权子用户使用Notebook进行调试，数据和代码存放在并行文件系统。以下内容需使用管理账号进行配置。



## 权限清单

- 权限

表 7-23 开发环境所需权限

| 业务场景         | 依赖的服务     | 依赖策略项                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | 支持的功能                    | 配置建议                                      |
|--------------|-----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|-------------------------------------------|
| 开发环境实例生命周期管理 | ModelArts | modelarts:notebook:create<br>modelarts:notebook:list<br>modelarts:notebook:get<br>modelarts:notebook:update<br>modelarts:notebook:delete<br>modelarts:notebook:start<br>modelarts:notebook:stop<br>modelarts:notebook:updateStopPolicy<br>modelarts:image:delete<br>modelarts:image:list<br>modelarts:image:create<br>modelarts:image:get<br>modelarts:pool:list<br>modelarts:tag:list<br>modelarts:network:get<br>aom:metric:get<br>aom:metric:list<br>aom:alarm:list | 实例的启动、停止、创建、删除、更新等依赖的权限。 | 建议配置。<br>仅在 <b>严格授权模式</b> 开启后，需要显式配置左侧权限。 |

| 业务场景     | 依赖的服务     | 依赖策略项                                                                                                                                                 | 支持的功能                                                                                                                      | 配置建议  |
|----------|-----------|-------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------|-------|
| 动态挂载存储配置 | ModelArts | modelarts:notebook:listMountedStorages<br>modelarts:notebook:mountStorage<br>modelarts:notebook:getMountedStorage<br>modelarts:notebook:umountStorage | 动态挂载存储配置。                                                                                                                  | 按需配置。 |
|          | OBS       | obs:bucket:ListAllMyBuckets<br>obs:bucket:ListBucket                                                                                                  |                                                                                                                            |       |
| 镜像管理     | ModelArts | modelarts:image:register<br>modelarts:image:listGroup                                                                                                 | 在镜像管理中注册和查看镜像。                                                                                                             | 按需配置。 |
| 保存镜像     | SWR       | SWR Admin                                                                                                                                             | SWR Admin为SWR最大权限，用于： <ul style="list-style-type: none"> <li>开发环境运行的实例，保存成镜像。</li> <li>使用自定义镜像创建开发环境Notebook实例。</li> </ul> | 按需配置。 |
| 使用SSH功能  | ECS       | ecs:serverKeypairs:list<br>ecs:serverKeypairs:get<br>ecs:serverKeypairs:delete<br>ecs:serverKeypairs:create                                           | 为开发环境Notebook实例配置登录密钥。                                                                                                     | 按需配置。 |
|          | DEW       | kps:domainKeypairs:get<br>kps:domainKeypairs:list                                                                                                     |                                                                                                                            |       |

| 业务场景                              | 依赖的服务     | 依赖策略项                                                                                                                                                                                                                                                                                                | 支持的功能                                                           | 配置建议  |
|-----------------------------------|-----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------|-------|
| 挂载SFS Turbo盘                      | SFS Turbo | SFS Turbo FullAccess                                                                                                                                                                                                                                                                                 | 子用户对SFS目录的读写操作权限。专属池 Notebook实例挂载SFS（公共池不支持），且挂载的SFS不是当前子用户创建的。 | 按需配置。 |
| 查看所有实例                            | ModelArts | modelarts:notebook:listAllNotebooks                                                                                                                                                                                                                                                                  | ModelArts开发环境界面上，查询所有用户的实例列表，适用于给开发环境的实例管理员配置该权限。               | 按需配置。 |
|                                   | IAM       | iam:users:listUsers                                                                                                                                                                                                                                                                                  |                                                                 |       |
| VSCode插件（本地）/ PyCharm Toolkit（本地） | ModelArts | modelarts:notebook:listAllNotebooks<br>modelarts:trainJob:create<br>modelarts:trainJob:list<br>modelarts:trainJob:update<br>modelarts:trainJobVersion:delete<br>modelarts:trainJob:get<br>modelarts:trainJob:logExport<br>modelarts:workspace:getQuotas<br>（如果开通了 <a href="#">工作空间</a> 功能，则需要配置此权限。） | 从本地VSCode连接云上的Notebook实例、提交训练作业等。                               | 按需配置。 |

| 业务场景  | 依赖的服务 | 依赖策略项                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 支持的功能                       | 配置建议  |
|-------|-------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------|-------|
|       | OBS   | obs:bucket:ListAllMybuckets<br>obs:bucket:HeadBucket<br>obs:bucket:ListBucket<br>obs:bucket:GetBucketLocation<br>obs:object:GetObject<br>obs:object:GetObjectVersion<br>obs:object:PutObject<br>obs:object:DeleteObject<br>obs:object:DeleteObjectVersion<br>obs:object:ListMultipartUploadParts<br>obs:object:AbortMultipartUpload<br>obs:object:GetObjectAcl<br>obs:object:GetObjectVersionAcl<br>obs:bucket:PutBucketAcl<br>obs:object:PutObjectAcl<br>obs:object:ModifyObjectMetaData |                             |       |
|       | IAM   | iam:projects:listProjects                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | 从本地PyCharm查询IAM项目列表，完成连接配置。 |       |
| VPC接入 | VPC   | VPC<br>ReadOnlyAccess                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 实例能够挂载在用户的VPC下，实现多网络平面接入。   | 按需配置。 |

 说明

创建自定义策略时，建议将项目级云服务和全局级云服务拆分为两条策略，便于授权时设置最小授权范围。

- 委托

表 7-24 开发环境所需委托

| 业务场景        | 依赖的服务 | 委托授权项                                                                                                                                                                                                                                                                       | 说明                                                    | 配置建议  |
|-------------|-------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------|-------|
| Jupyter Lab | OBS   | obs:object:DeleteObject<br>obs:object:GetObject<br>obs:object:GetObjectVersion<br>obs:bucket>CreateBucket<br>obs:bucket:ListBucket<br>obs:bucket:ListAllMyBuckets<br>obs:object:PutObject<br>obs:bucket:GetBucketAcl<br>obs:bucket:PutBucketAcl<br>obs:bucket:PutBucketCORS | 通过ModelArts的Notebook，在JupyterLab中使用OBS上传下载数据。         | 建议配置。 |
| 开发环境监控功能    | AOM   | aom:alarm:put                                                                                                                                                                                                                                                               | 调用AOM的接口，获取Notebook相关的监控数据和事件，展示在ModelArts的Notebook中。 | 建议配置。 |
| VPC接入       | VPC   | vpc:ports:create<br>vpc:ports:get<br>vpc:ports:delete<br>vpc:subnet:get                                                                                                                                                                                                     | 实例能够挂载在用户的VPC下，实现多网络平面接入。                             | 按需配置。 |

## 操作步骤

本案例场景为**单机单卡场景下使用Notebook进行代码调试**，数据和代码存储在OBS服务的并行文件系统下，调试完成过后可保存镜像。

**步骤1** 使用主用户账号登录管理控制台，单击右上角用户名，在下拉框中选择“统一身份认证”，进入统一身份认证（IAM）服务。

**步骤2** 添加开发环境使用权限和依赖服务SWR权限。在统一身份认证服务页面的左侧导航选择“权限管理 > 权限”，单击右上角的“创建自定义策略”，设置策略。

1. 添加开发环境使用权限。
  - “策略名称”：设置自定义策略名称，例如：notebook。
  - “策略配置方式”：选择JSON视图。

- “策略内容”：填入如下内容。

```
{
 "Version": "1.1",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": [
 "modelarts:notebook:create",
 "modelarts:notebook:list",
 "modelarts:notebook:get",
 "modelarts:notebook:update",
 "modelarts:notebook:delete",
 "modelarts:notebook:start",
 "modelarts:notebook:stop",
 "modelarts:notebook:updateStopPolicy",
 "modelarts:notebook:listMountedStorages",
 "modelarts:notebook:mountStorage",
 "modelarts:notebook:getMountedStorage",
 "modelarts:notebook:umountStorage",
 "modelarts:image:delete",
 "modelarts:image:list",
 "modelarts:image:create",
 "modelarts:image:get",
 "modelarts:pool:list",
 "modelarts:tag:list",
 "modelarts:network:get",
 "aom:metric:get",
 "aom:metric:list",
 "aom:alarm:list"
]
 }
]
}
```

### 步骤3 添加依赖服务OBS权限。

在统一身份认证服务页面的左侧导航选择“权限管理 > 权限”，单击右上角的“创建自定义策略”，设置策略。

- “策略名称”：设置自定义策略名称，例如：notebook-obs。
- “策略配置方式”：JSON视图。
- “策略内容”：填入如下内容。

```
{
 "Version": "1.1",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": [
 "obs:bucket:ListAllMyBuckets",
 "obs:bucket:ListBucket"
]
 }
]
}
```

#### 说明

创建自定义策略时，建议将项目级云服务和全局级云服务拆分为两条策略，便于授权时设置最小授权范围。此处的“trainJob”为项目级云服务、“trainJobobs”为全局级云服务。[了解更多](#)

**步骤4** 创建用户组并加入用户，步骤请参考[Step1 创建用户组并加入用户](#)。

**步骤5** 给用户组授权策略。

在IAM服务的用户组列表页面，单击“授权”，进入到授权页面，为子用户配置权限。勾选“notebook”、“notebook-obs”、“SWR Admin”策略。单击“下一步”和“确定”。

图 7-35 给用户组授权策略



## 步骤6 添加ModelArts委托授权。

### 1. 新建委托授权策略。

在统一身份认证服务页面的左侧导航选择“权限管理 > 权限”，单击右上角的“创建自定义策略”，设置策略。

- “策略名称”：设置自定义策略名称，例如：ma\_agency\_obs。
- “策略配置方式”：JSON视图。
- “策略内容”：填入如下内容。

```
{
 "Version": "1.1",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": [
 "obs:object:GetObject",
 "obs:object:DeleteObject",
 "obs:bucket:PutBucketAcl",
 "obs:object:PutObject",
 "obs:bucket:CreateBucket",
 "obs:bucket:GetBucketAcl",
 "obs:bucket:PutBucketCORS",
 "obs:bucket:ListAllMyBuckets",
 "obs:bucket:ListBucket",
 "obs:object:GetObjectVersion"
]
 }
]
}
```

### 2. 创建委托。

在统一身份认证服务页面的左侧导航选择“权限管理 > 委托”，单击右上角的“创建委托”，设置策略。填写委托信息并单击“下一步”。

- 委托名称：可自定义委托名称，例如：ma\_agency\_notebook。
- 委托类型：选择“云服务”。
- 云服务：选择“ModelArts”。
- 持续时间：选择“永久”。

图 7-36 创建委托

委托 / 创建委托

\* 委托名称

\* 委托类型  普通帐号  
将帐号内资源的操作权限委托给其他华为云帐号。  
 云服务  
将帐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

勾选新建的委托策略，然后单击“下一步”。设置最小授权范围选择“所有资源”，然后单击“确定”。

图 7-37 选择策略

1 选择策略 ———— 2 设置最小授权范围 ———— 3 完成

委托"ma\_agency\_notebook"将拥有所选策略

查看已选(1) 从其他区域项目复制权限

| <input type="checkbox"/>            | 名称            |
|-------------------------------------|---------------|
| <input checked="" type="checkbox"/> | ma_agency_obs |
| <input type="checkbox"/>            | —             |

3. 为子用户配置ModelArts委托权限。



在ModelArts服务页面的左侧导航选择“全局配置”，单击“添加授权”。授权对象选择子用户，在已有委托中选择新建的委托，然后单击“创建”。

图 7-38 配置 ModelArts 委托权限



步骤7 验证权限是否配置成功。

登录子用户账号，如果用户能在控制台上成功[创建Notebook示例](#)、[挂载OBS文件系统](#)（OBS桶需由管理员创建）、[保存镜像](#)，则表示权限配置成功。

----结束

## 7.3.4 给予用户配置训练作业基本使用权限

### 场景描述

本文介绍训练作业场景下子用户所需的基本使用权限，您可参考[权限清单](#)新增对应业务场景的权限。示例场景为授权子用户使用自定义镜像训练，数据和代码存放在OBS桶中。以下内容需使用管理账号进行配置。

### 权限清单

- 权限

表 7-25 训练作业所需权限

| 业务场景 | 依赖的服务     | 依赖策略项                                                                                                                                                  | 支持的功能                                            | 配置建议                                               |
|------|-----------|--------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------|----------------------------------------------------|
| 训练管理 | ModelArts | modelarts:trainJob:*<br>modelarts:trainJobLog:*<br>modelarts:aiAlgorithm:*<br>modelarts:image:list<br>modelarts:network:get<br>modelarts:workspace:get | 创建训练作业和查看训练日志。                                   | 建议配置。<br>仅在 <a href="#">严格授权模式</a> 开启后，需要显式配置左侧权限。 |
|      |           | modelarts:workspace:getQuotas                                                                                                                          | 查询工作空间配额。如果开通了 <a href="#">工作空间</a> 功能，则需要配置此权限。 | 按需配置。                                              |

| 业务场景 | 依赖的服务     | 依赖策略项                                                                                      | 支持的功能              | 配置建议  |
|------|-----------|--------------------------------------------------------------------------------------------|--------------------|-------|
|      |           | modelarts:tag:list                                                                         | 在训练作业中使用标签管理服务TMS。 | 按需配置。 |
|      | IAM       | iam:credentials:listCredentials<br>iam:agencies:listAgencies                               | 使用配置的委托授权项。        | 按需配置。 |
|      | SFS Turbo | sfsturbo:shares:getShare<br>sfsturbo:shares:getAllShares                                   | 在训练作业中使用SFS Turbo。 | 按需配置。 |
|      | SWR       | swr:repository:listTags<br>swr:repository:getRepository<br>swr:repository:listRepositories | 使用自定义镜像运行训练作业。     | 按需配置。 |
|      | SMN       | smn:topic:publish<br>smn:topic:list                                                        | 通过SMN通知训练作业状态变化事件。 | 按需配置。 |

| 业务场景 | 依赖的服务 | 依赖策略项                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 支持的功能             | 配置建议  |
|------|-------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------|-------|
|      | OBS   | obs:bucket:ListAllMybuckets<br>obs:bucket:HeadBucket<br>obs:bucket:ListBucket<br>obs:bucket:GetBucketLocation<br>obs:object:GetObject<br>obs:object:GetObjectVersion<br>obs:object:PutObject<br>obs:object>DeleteObject<br>obs:object>DeleteObjectVersion<br>obs:object:ListMultipartUploadParts<br>obs:object:AbortMultipartUpload<br>obs:object:GetObjectAcl<br>obs:object:GetObjectVersionAcl<br>obs:bucket:PutBucketAcl<br>obs:object:PutObjectAcl<br>obs:object:ModifyObjectMetaData | 使用OBS桶中的数据运行训练作业。 | 按需配置。 |

- 委托

表 7-26 训练作业所需委托

| 业务场景 | 依赖的服务 | 委托授权项                                                                 | 说明                                    | 配置建议  |
|------|-------|-----------------------------------------------------------------------|---------------------------------------|-------|
| 训练作业 | OBS   | obs:bucket:ListBucket<br>obs:object:GetObject<br>obs:object:PutObject | 训练作业启动前下载数据、模型、代码。<br>训练作业运行中上传日志、模型。 | 建议配置。 |

## 操作步骤

本案例场景为[单机单卡场景下创建训练作业](#)，数据和代码存储在OBS服务的并行文件系统下，创建自定义镜像训练作业。

**步骤1** 使用主用户账号登录管理控制台，单击右上角用户名，在下拉框中选择“统一身份认证”，进入统一身份认证（IAM）服务。

**步骤2** 添加训练作业使用权限。在统一身份认证服务页面的左侧导航选择“权限管理 > 权限”，单击右上角的“创建自定义策略”，设置策略。

- “策略名称”：设置自定义策略名称，例如：trainJob。
- “策略配置方式”：选择JSON视图。
- “策略内容”：填入如下内容。

```
{
 "Version": "1.1",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": [
 "modelarts:trainJob:*",
 "modelarts:trainJobLog:*",
 "modelarts:aiAlgorithm:*",
 "modelarts:image:list",
 "modelarts:pool:list",
 "swr:repository:listTags",
 "swr:repository:getRepository",
 "swr:repository:listRepositories"
]
 }
]
}
```

**步骤3** 添加依赖服务OBS权限。

在统一身份认证服务页面的左侧导航选择“权限管理 > 权限”，单击右上角的“创建自定义策略”，设置策略。

- “策略名称”：设置自定义策略名称，例如：trainJob-obs。
- “策略配置方式”：JSON视图。
- “策略内容”：填入如下内容。

```
{
 "Version": "1.1",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": [
 "obs:object:GetObject",
 "obs:object:DeleteObjectVersion",
 "obs:bucket:GetBucketLocation",
 "obs:object:AbortMultipartUpload",
 "obs:object:PutObjectAcl",
 "obs:object:DeleteObject",
 "obs:bucket:HeadBucket",
 "obs:bucket:PutBucketAcl",
 "obs:object:PutObject",
 "obs:object:GetObjectVersionAcl",
 "obs:bucket:ListAllMyBuckets",
 "obs:object:ListMultipartUploadParts",
 "obs:object:ModifyObjectMetaData",
 "obs:bucket:ListBucket",
 "obs:object:GetObjectVersion",
 "obs:object:GetObjectAcl"
]
 }
]
}
```

### 说明

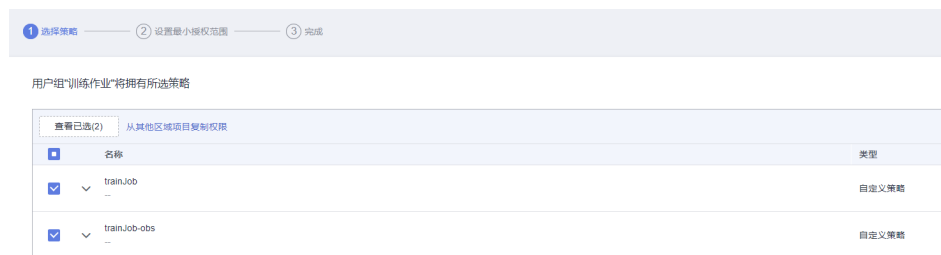
创建自定义策略时，建议将项目级云服务和全局级云服务拆分为两条策略，便于授权时设置最小授权范围。此处的“trainJob”为项目级云服务、“trainJobobs”为全局级云服务。[了解更多](#)

**步骤4** 创建用户组并加入用户，步骤请参考[Step1 创建用户组并加入用户](#)。

**步骤5** 给用户组授权策略。

在IAM服务的用户组列表页面，单击“授权”，进入到授权页面，为子用户配置权限。勾选“trainJob”和“trainJob-obs”策略。单击“下一步”和“确定”。

图 7-39 给用户组授权策略



**步骤6** 为子用户添加镜像组织管理授权。

登录容器镜像服务控制台。在左侧菜单栏选择“组织管理”，单击组织名称。在“用户”页签下单击“添加授权”，在弹出的窗口中为子用户添加“编辑”权限，然后单击“确定”。

图 7-40 组织管理授权



**步骤7** 添加ModelArts委托授权。

1. 新建委托授权策略。

在统一身份认证服务页面的左侧导航选择“权限管理 > 权限”，单击右上角的“创建自定义策略”，设置策略。

- “策略名称”：设置自定义策略名称，例如：ma\_agency\_obs。
- “策略配置方式”：选择可视化视图或者JSON视图均可。
- “策略内容”：填入如下内容。

```
{
 "Version": "1.1",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": [
 "obs:object:GetObject",
 "obs:object:PutObject",
 "obs:bucket:ListBucket"
]
 }
]
}
```

## 2. 创建委托。

在统一身份认证服务页面的左侧导航选择“权限管理 > 委托”，单击右上角的“创建委托”，设置策略。填写委托信息并单击“下一步”。

- 委托名称：可自定义委托名称，例如：ma\_agency\_trainJob。
- 委托类型：选择“云服务”。
- 云服务：选择“ModelArts”。
- 持续时间：选择“永久”。

图 7-41 创建委托

委托 / 创建委托

\* 委托名称

\* 委托类型  普通帐号  
将帐号内资源的操作权限委托给其他华为云帐号。  
 云服务  
将帐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

勾选新建的委托策略，然后单击“下一步”。设置最小授权范围选择“所有资源”，然后单击“确定”。

图 7-42 选择策略



委托"ma\_agency\_trainJob"将拥有所选策略



3. 为子用户配置ModelArts委托权限。  
在ModelArts服务页面的左侧导航选择“全局配置”，单击“添加授权”。授权对象选择子用户，在已有委托中选择新建的委托，然后单击“创建”。

图 7-43 配置 ModelArts 委托权限



**步骤8** 验证权限是否配置成功。

登录子用户账号，如果用户能在控制台上成功创建使用自定义镜像创建训练作业（如[单机单卡场景下创建训练作业](#)），则表示权限配置成功。

----结束

### 7.3.5 给子用户配置部署上线基本使用权限

#### 场景描述

本文介绍部署上线场景下子用户所需的基本使用权限，您可参考[权限清单](#)新增对应业务场景的权限。示例场景为授权子用户权限，使其能够在开发环境Notebook中使用基础镜像构建一个新的推理镜像，并完成AI应用的创建，部署为在线服务。

#### 权限清单

- 权限

表 7-27 管理 AI 应用所需权限

| 业务场景   | 依赖的服务     | 依赖策略项                                                                                                                                                                                                                                                                                                                                                                                                                                                  | 支持的功能                                                                                                          | 配置建议                                      |
|--------|-----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------|-------------------------------------------|
| 管理AI应用 | ModelArts | modelarts:model:*                                                                                                                                                                                                                                                                                                                                                                                                                                      | 创建、删除、查看、导入AI模型。                                                                                               | 建议配置。<br>仅在 <b>严格授权模式</b> 开启后，需要显式配置左侧权限。 |
|        | SWR       | SWR Admin                                                                                                                                                                                                                                                                                                                                                                                                                                              | SWR Admin为SWR最大权限，用于： <ul style="list-style-type: none"> <li>• 从自定义镜像导入。</li> <li>• 从OBS导入时使用自定义引擎。</li> </ul> | 按需配置。                                     |
|        | OBS       | obs:bucket:ListAllMybuckets<br>obs:bucket:HeadBucket<br>obs:bucket:ListBucket<br>obs:bucket:GetBucketLocation<br>obs:object:GetObject<br>obs:object:GetObjectVersion<br>obs:object:PutObject<br>obs:object:DeleteObject<br>obs:object:DeleteObjectVersion<br>obs:object:ListMultipartUploadParts<br>obs:object:AbortMultipartUpload<br>obs:object:GetObjectAcl<br>obs:object:GetObjectVersionAcl<br>obs:bucket:PutBucketAcl<br>obs:object:PutObjectAcl | 从OBS导入模型。<br>模型转换指定OBS路径。                                                                                      | 按需配置。                                     |



表 7-28 部署上线所需权限

| 业务场景 | 依赖的服务     | 依赖策略项                                                                                                                           | 支持的功能            | 配置建议                                      |
|------|-----------|---------------------------------------------------------------------------------------------------------------------------------|------------------|-------------------------------------------|
| 部署服务 | ModelArts | modelarts:service:*                                                                                                             | 部署、启动、查新、更新模型服务。 | 建议配置。<br>仅在 <b>严格授权模式</b> 开启后，需要显式配置左侧权限。 |
|      | LTS       | lts:logs:list                                                                                                                   | 查询和展示LTS日志。      | 按需配置。                                     |
| 批量服务 | OBS       | obs:object:GetObject<br>obs:object:PutObject<br>obs:bucket:CreateBucket<br>obs:bucket:ListBucket<br>obs:bucket:ListAllMyBuckets | 创建批量服务。          | 按需配置。                                     |
| 边缘服务 | CES       | ces:metricData:list                                                                                                             | 查看服务的监控指标。       | 按需配置。                                     |
|      | IEF       | IEF Administrator                                                                                                               | 管理边缘服务。          | 按需配置。                                     |

 说明

创建自定义策略时，建议将项目级云服务和全局级云服务拆分为两条策略，便于授权时设置最小授权范围。

- 委托

表 7-29 部署上线所需委托

| 业务场景 | 依赖的服务 | 委托授权项                                                                                             | 说明             | 配置建议  |
|------|-------|---------------------------------------------------------------------------------------------------|----------------|-------|
| 在线服务 | LTS   | lts:groups:create<br>lts:groups:list<br>lts:topics:create<br>lts:topics:delete<br>lts:topics:list | 在线服务配置LTS日志上报。 | 按需配置。 |

| 业务场景 | 依赖的服务 | 委托授权项                                                                                                                                                              | 说明           | 配置建议  |
|------|-------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------|-------|
| 批量服务 | OBS   | obs:bucket:ListBucket<br>obs:object:GetObject<br>obs:object:PutObject                                                                                              | 运行批量服务。      | 按需配置。 |
| 边缘服务 | IEF   | ief:deployment:list<br>ief:deployment:create<br>ief:deployment:update<br>ief:deployment:delete<br>ief:node:createNodeCert<br>ief:iefInstance:list<br>ief:node:list | 通过IEF部署边缘服务。 | 按需配置。 |

## 操作步骤

本案例场景为在开发环境中构建并调试推理镜像，在Notebook中制作自定义镜像，然后将调试完成的镜像导入ModelArts的AI应用管理中，并部署上线。

- 步骤1** 使用主用户账号登录管理控制台，单击右上角用户名，在下拉框中选择“统一身份认证”，进入统一身份认证（IAM）服务。
- 步骤2** 添加部署上线使用权限。在统一身份认证服务页面的左侧导航选择“权限管理 > 权限”，单击右上角的“创建自定义策略”，设置策略。

添加部署上线使用权限。

- “策略名称”：设置自定义策略名称，例如：service。
- “策略配置方式”：选择JSON视图。
- “策略内容”：填入如下内容。

```
{
 "Version": "1.1",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": [
 "modelarts:service:*",
 "modelarts:model:*",
 "modelarts:notebook:create",
 "modelarts:notebook:list",
 "modelarts:notebook:get",
 "modelarts:notebook:update",
 "modelarts:notebook:delete",
 "modelarts:notebook:start",
 "modelarts:notebook:stop",
 "modelarts:notebook:updateStopPolicy",
 "modelarts:image:delete",
 "modelarts:image:list",
 "modelarts:image:create",
 "modelarts:image:get",
 "modelarts:image:register",
 "modelarts:image:listGroup",
 "modelarts:pool:list",
 "modelarts:tag:list",
]
 }
]
}
```

```

 "aom:metric:get",
 "aom:metric:list",
 "aom:alarm:list"
]
}
]
}

```

**步骤3** 创建用户组并加入用户，步骤请参考[Step1 创建用户组并加入用户](#)。

**步骤4** 给用户组授权策略。

在IAM服务的用户组列表页面，单击“授权”，进入到授权页面，为子用户配置权限。勾选“service”、“SWR Admin”策略。单击“下一步”和“确定”。

**图 7-44** 给用户组授权策略



**步骤5** 添加ModelArts委托授权。

1. 新建委托授权策略。

在统一身份认证服务页面的左侧导航选择“权限管理 > 权限”，单击右上角的“创建自定义策略”，设置策略。

- “策略名称”：设置自定义策略名称，例如：service\_agency。
- “策略配置方式”：JSON视图。
- “策略内容”：填入如下内容。

```

{
 "Version": "1.1",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": [
 "lts:groups:create",
 "lts:groups:list",
 "lts:topics:create",
 "lts:topics:delete",
 "lts:topics:list"
]
 }
]
}

```

2. 创建委托。

在统一身份认证服务页面的左侧导航选择“权限管理 > 委托”，单击右上角的“创建委托”，设置策略。填写委托信息并单击“下一步”。

- 委托名称：可自定义委托名称，例如：ma\_agency\_service。
- 委托类型：选择“云服务”。
- 云服务：选择“ModelArts”。
- 持续时间：选择“永久”。

图 7-45 创建委托

委托 / 创建委托

\* 委托名称

\* 委托类型  普通帐号  
将帐号内资源的操作权限委托给其他华为云帐号。  
 云服务  
将帐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

勾选新建的委托策略，然后单击“下一步”。设置最小授权范围选择“所有资源”，然后单击“确定”。

图 7-46 选择策略

委托"ma\_agency\_service"将拥有所选策略



3. 为子用户配置ModelArts委托权限。

在ModelArts服务页面的左侧导航选择“全局配置”，单击“添加授权”。授权对象选择子用户，在已有委托中选择新建的委托，然后单击“创建”。

图 7-47 配置 ModelArts 委托权限



**步骤6** 验证权限是否配置成功。

登录子用户账号，如果用户能跑通在开发环境中构建并调试推理镜像的案例，在Notebook中制作自定义镜像，然后将调试完成的镜像导入ModelArts的AI应用管理中，并部署上线，则表示权限配置成功。

----结束

## 7.3.6 管理员和开发者权限分离

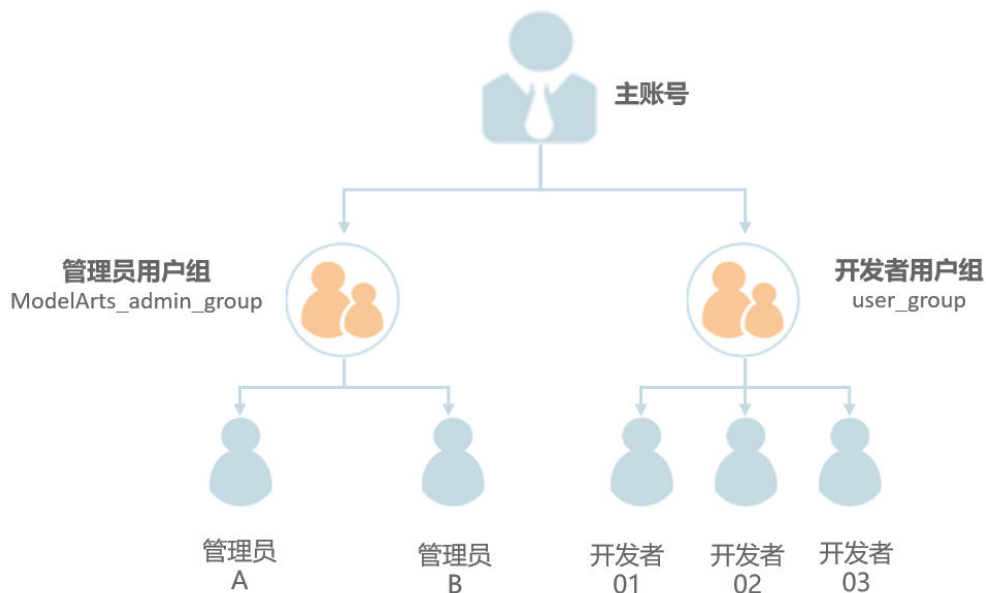
对于中小规模团队，管理员希望对ModelArts资源进行主导分配，全局控制，而对于普通开发者只需关注自己实例的生命周期控制。对于开发者账号，一般不会具有te\_admin的权限，相应的权限也需要主账号进行统一配置。本章节以使用Notebook进行项目开发为例，通过自定义策略配置实现管理员和开发者分离。

### 场景描述

以使用Notebook进行项目开发为例，管理员账号需要拥有ModelArts专属资源池的完全控制权限，以及Notebook所有实例的访问和操作权限。

普通开发者使用开发环境，只需关注对自己Notebook实例的操作权限，包括对自己实例的创建、启动、停止、删除等权限以及周边依赖服务的权限。普通开发者不需要ModelArts专属资源池的操作权限，也不需要查看其他用户的Notebook实例。

图 7-48 账号关系示意图



## 配置管理员权限

管理员账号需要拥有ModelArts专属资源池的完全控制权限，以及Notebook所有实例的访问和操作权限。可以通过以下配置流程实现管理员权限配置。

**步骤1** 使用主账号创建一个管理员用户组ModelArts\_admin\_group，将管理员账号加入用户组ModelArts\_admin\_group中。具体操作请参见[Step1 创建用户组并加入用户](#)。

**步骤2** 创建自定义策略。

1. 使用管理员账号登录控制台，单击右上角用户名，在下拉框中选择“统一身份认证”，进入IAM服务。

图 7-49 登录控制台



2. 创建自定义策略1，赋予用户IAM和OBS服务权限。在统一身份认证服务控制台的左侧菜单栏中，选择“权限管理> 权限”。单击右上角“创建自定义策略”，在“策略名称”中填入“Policy1\_IAM\_OBS”，策略配置方式选择JSON视图，输入策略内容，单击“确定”。

图 7-50 配置自定义策略 1

策略名称: Policy1\_IAM\_OBS

策略配置方式: 可视化视图 | JSON视图

策略内容:

```
1 {
2 "Version": "1.1",
3 "Statement": [
4 {
5 "Action": [
6 "iam:users:listUsers",
7 "iam:projects:listProjects",
8 "obs:object:PutObject",
9 "obs:object:GetObject",
10 "obs:object:GetObjectVersion",
11 "obs:bucket:HeadBucket",
12 "obs:object:DeleteObject",
13 "obs:bucket:CreateBucket",
14 "obs:bucket:ListBucket"
15],
16 "Effect": "Allow"
17 }
18]
19 }
20
```

从已有策略复制

策略描述: 请输入策略描述 (可选)

作用范围: 全局级服务

确定 取消

自定义策略“Policy1\_IAM\_OBS”的具体内容如下，赋予用户IAM和OBS操作权限。可以直接复制粘贴。

```
{
 "Version": "1.1",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": [
 "iam:users:listUsers",
 "iam:projects:listProjects",
 "obs:object:PutObject",
 "obs:object:GetObject",
 "obs:object:GetObjectVersion",
 "obs:bucket:HeadBucket",
 "obs:object:DeleteObject",
 "obs:bucket:CreateBucket",
 "obs:bucket:ListBucket"
]
 }
]
}
```

```
"iam:users:listUsers",
"iam:projects:listProjects",
"obs:object:PutObject",
"obs:object:GetObject",
"obs:object:GetObjectVersion",
"obs:bucket:HeadBucket",
"obs:object:DeleteObject",
"obs:bucket:CreateBucket",
"obs:bucket:ListBucket"
]
}
]
```

3. 重复[步骤2.2](#)创建自定义策略2，赋予用户依赖服务ECS、SWR、MRS和SMN的操作权限，ModelArts的操作权限。“策略名称”为“Policy2\_AllowOperation”，策略配置方式选择JSON视图，输入策略内容，单击“确定”。

自定义策略“Policy2\_AllowOperation”的具体内容如下，赋予用户依赖服务ECS、SWR、MRS和SMN的操作权限，ModelArts的操作权限。可以直接复制粘贴。

```
{
 "Version": "1.1",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": [
 "ecs:serverKeypairs:list",
 "ecs:serverKeypairs:get",
 "ecs:serverKeypairs:delete",
 "ecs:serverKeypairs:create",
 "swr:repository:getNamespace",
 "swr:repository:listNamespaces",
 "swr:repository:deleteTag",
 "swr:repository:getRepository",
 "swr:repository:listTags",
 "swr:instance:createTempCredential",
 "mrs:cluster:get",
 "modelarts:*:*"
]
 }
]
}
```

**步骤3** 将[步骤2](#)创建的自定义策略授权给管理员用户组ModelArts\_admin\_group。

1. 在统一身份认证服务控制台的左侧菜单栏中，选择“用户组”。在用户组页面单击对应用户组名称ModelArts\_admin\_group操作列的“授权”，勾选策略“Policy1\_IAM\_OBS”和“Policy2\_AllowOperation”。单击“下一步”。



图 7-51 给管理员用户组授权



用户组"ModelArts\_admin\_group"将拥有所选策略



2. 选择授权范围方案为所有资源，单击“确定”。

图 7-52 选择用户组授权范围



根据当前您所选择的策略，系统推荐以下授权范围方案，更便于您最小化授权，可进行选择。

选择授权范围方案

所有资源

授权后，IAM用户可以根据权限使用帐号中所有资源，包括企业项目、区域项目和全局服务资源。

指定区域项目资源 ?

全局服务资源 ?

**步骤4** 给管理员用户配置ModelArts委托授权，允许ModelArts服务在运行时访问OBS等依赖服务。

1. 使用主账号登录ModelArts的管理控制台，在左侧导航栏单击“全局配置”，进入“全局配置”页面。
2. 单击“添加授权”。在“访问授权”页面，在“授权对象类型”下面选择“IAM子用户”，“授权对象”选择管理员的账号，选择“新增委托”，“权限配置”选择“普通用户”。管理员不做权限控制，此处默认使用普通用户委托即可。

图 7-53 配置管理员用户委托授权



- 勾选“我已经仔细阅读并同意《 ModelArts服务声明 》”，单击“创建”。

#### 步骤5 测试管理员用户权限。

- 使用管理员用户登录ModelArts管理控制台。在登录页面，请使用“IAM用户登录”方式进行登录。  
首次登录会提示修改密码，请根据界面提示进行修改。
- 在ModelArts控制台的左侧导航栏中，选择“专属资源池”，单击创建，未提示权限不足，表明管理员用户的权限配置成功。

----结束

## 配置开发者权限

开发者权限需要通过IAM的细粒度授权控制实现，可以通过以下配置流程实现开发者权限配置。

**步骤1** 使用主账号创建一个开发者用户组user\_group，将开发者账号加入用户组user\_group中。具体操作请参见[Step1 创建用户组并加入用户](#)。

**步骤2** 创建自定义策略。

- 使用主账号登录控制台，单击右上角用户名，在下拉框中选择“统一身份认证”，进入IAM服务。

图 7-54 登录控制台



2. 创建自定义策略3，拒绝用户操作ModelArts专属资源池并拒用户查看其他用户的Notebook。

在统一身份认证服务控制台的左侧菜单栏中，选择“权限管理> 权限”。单击右上角“创建自定义策略”，“策略名称”为“Policy3\_DenyOperation”，策略配置方式选择JSON视图，输入策略内容，单击“确定”。

自定义策略“Policy3\_DenyOperation”的具体内容如下，可以直接复制粘贴。

```
{
 "Version": "1.1",
 "Statement": [
 {
 "Effect": "deny",
 "Action": [
 "modelarts:pool:create",
 "modelarts:pool:update",
 "modelarts:pool:delete",
 "modelarts:notebook:listAllNotebooks"
]
 }
]
}
```

### 步骤3 将自定义策略授权给开发者用户组user\_group。

1. 在统一身份认证服务控制台的左侧菜单栏中，选择“用户组”。在用户组页面单击对应用户组名称user\_group操作列的“授权”，勾选策略“Policy1\_IAM\_OBS”、“Policy2\_AllowOperation”和“Policy3\_DenyOperation”。单击“下一步”。

图 7-55 给用户组授权



用户组"user\_group"将拥有所选策略



2. 选择授权范围方案为所有资源，单击“确定”。

图 7-56 选择用户组授权范围



**步骤4** 给开发者用户配置ModelArts委托授权，允许ModelArts服务在运行时访问OBS等依赖服务。

1. 使用主账号登录ModelArts的管理控制台，在左侧导航栏单击“全局配置”，进入“全局配置”页面。
2. 单击“添加授权”。在“访问授权”页面，在“授权对象类型”下面选择“IAM子用户”，“授权对象”选择开发者的账号，“委托选择”选择“新增委托”，“委托名称”设置为“ma\_agency\_develop\_user”，“权限配置”选择“自定义”，“权限名称”勾选“OBS Administrator”。开发者用户只需要配置OBS的委托授权即可，允许开发者用户在使用Notebook时，与OBS服务交互。

图 7-57 配置开发者用户的委托授权



3. 勾选“我已经仔细阅读并同意《 ModelArts服务声明 》”，单击“创建”。
4. 在“全局配置”页面，再次单击“添加授权”，进入“访问授权”页面，为其他开发者用户配置委托。  
“授权对象类型”选择“IAM子用户”，“授权对象”选择开发者的账号，“委托选择”选择“已有委托”，“委托名称”勾选上一步创建的“ma\_agency\_develop\_user”，

**步骤5** 测试开发者用户权限。

1. 使用user\_group用户组中任意一个子用户登录ModelArts管理控制台。在登录页面，请使用“IAM用户登录”方式进行登录。  
首次登录会提示修改密码，请根据界面提示进行修改。
2. 在ModelArts左侧菜单栏中，选择“专属资源池”，单击创建，界面未提示权限不足，表明开发者用户的权限配置成功。

图 7-58 提示权限不足



---结束

### 7.3.7 查看所有子账号的 Notebook 实例

当子用户被授予“listAllNotebooks”和“listUsers”权限时，在Notebook页面上，打开“查看所有”，可以看到IAM项目下所有子用户创建的Notebook实例。

#### 📖 说明

配置该权限后，可以查看子用户的Notebook，也可以在Notebook中访问子用户的OBS、SWR等。

### 给子账号配置查看所有 Notebook 实例的权限

1. 使用主用户账号登录管理控制台，单击右上角用户名，在下拉框中选择“统一身份认证”，进入统一身份认证（IAM）服务。
2. 在统一身份认证服务页面的左侧导航选择“权限管理 > 权限”，单击右上角的“创建自定义策略”，需要设置两条策略。

策略1：设置查看Notebook所有实例，如图7-59所示，单击“确定”。

- “策略名称”：设置自定义策略名称，例如：查看Notebook所有实例。
- “策略配置方式”：选择可视化视图。此处以可视化视图配置方式举例。
- “策略内容”：允许，云服务中搜索ModelArts服务并选中，操作列中搜索关键词modelarts:notebook:listAllNotebooks并选中，所有资源选择默认值。

图 7-59 创建自定义策略



策略2：设置查看Notebook实例创建者信息的策略。

- “策略名称”：设置自定义策略名称，例如：查看所有子用户信息。
  - “策略配置方式”：选择可视化视图。
  - “策略内容”：允许，云服务中搜索IAM服务并选中，操作列中搜索关键词 iam:users:listUsers并选中，所有资源选择默认值。
3. 在统一身份认证服务页面的左侧导航选择“用户组”，在用户组页面查找待授权的用户组名称，在右侧的操作列单击“授权”，勾选步骤2创建的两条自定义策略，单击“下一步”，选择授权范围方案，单击“确定”。

此时，该用户组下的所有用户均有权查看该用户组内成员创建的所有Notebook实例。

如果没有用户组，也可以创建一个新的用户组，并通过“用户组管理”功能添加用户，并配置授权。如果指定的子用户没有在用户组中，也可以通过“用户组管理”功能增加用户。

## 子用户启动其他用户的 SSH 实例

子用户可以看到所有用户的Notebook实例后，如果要通过SSH方式远程连接其他用户的Notebook实例，需要将SSH密钥对更新成自己的，否则会报错ModelArts.6786。更新密钥对具体操作请参见[修改Notebook SSH远程连接配置](#)。

具体的错误信息提示：ModelArts.6789: 在ECS密钥对管理中找不到指定的ssh密钥对xxx，请更新密钥对并重试。

## 7.3.8 使用 Cloud Shell 登录训练容器

### 使用场景

允许用户使用ModelArts控制台提供的Cloud Shell登录运行中的训练容器。

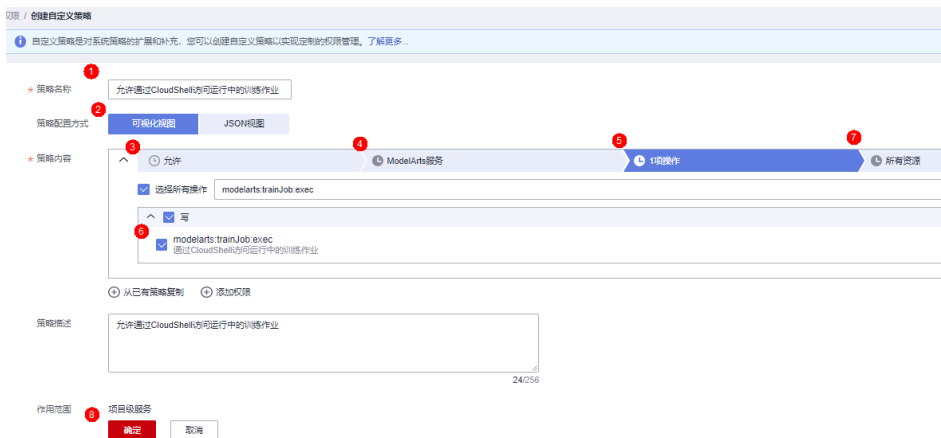
### 约束限制

仅专属资源池均支持使用Cloud Shell，且训练作业必须处于“运行中”状态。

## 前提条件：给予账号配置允许使用 Cloud Shell 的权限

1. 使用主用户账号登录华为云的管理控制台，单击右上角用户名，在下拉框中选择“统一身份认证”，进入统一身份认证（IAM）服务。
2. 在统一身份认证服务页面的左侧导航选择“权限管理 > 权限”，单击右上角的“创建自定义策略”按如下要求设置完成后单击“确定”。
  - “策略名称”：设置自定义策略名称，例如：允许通过Cloud Shell访问运行中的训练作业。
  - “策略配置方式”：选择可视化视图。
  - “策略内容”：允许，云服务中搜索ModelArts服务并选中，操作列中搜索关键词modelarts:trainJob:exec并选中，所有资源选择默认值。

图 7-60 创建自定义策略



3. 在统一身份认证服务页面的左侧导航选择“用户组”，在用户组页面查找待授权的用户组名称，在右侧的操作列单击“授权”，勾选步骤2创建的自定义策略，单击“下一步”，选择授权范围方案，单击“确定”。

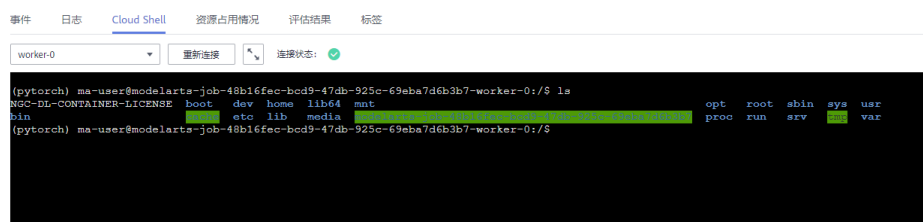
此时，该用户组下的所有用户均有权通过Cloud Shell登录运行中的训练作业容器。

如果没有用户组，也可以创建一个新的用户组，并通过“用户组管理”功能添加用户，并配置授权。如果指定的子用户没有在用户组中，也可以通过“用户组管理”功能增加用户。

## 如何使用 Cloud Shell

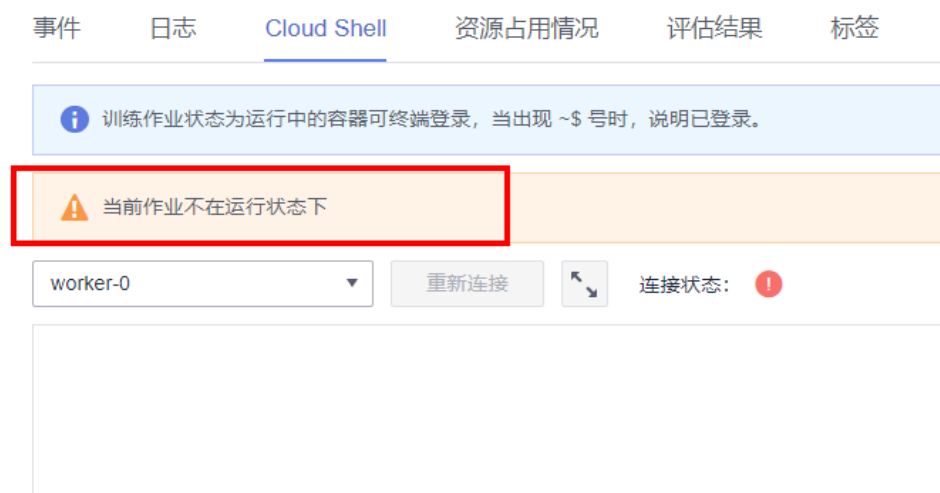
1. 参考前提条件：给予账号配置允许使用Cloud Shell的权限，完成配置。
2. 在ModelArts控制台，选择训练管理>训练作业，在训练作业详情页面，在右侧的Cloud Shell页签，登录训练容器。  
连接成功后，Cloud Shell界面提示如下。

图 7-61 Cloud Shell 界面



作业处于非运行状态、权限不足等原因会导致无法使用Cloud Shell，请根据提示定位原因即可。

图 7-62 报错提示



### 7.3.9 限制用户使用公共资源池

本章节介绍如何控制ModelArts用户权限，限制用户使用ModelArts公共资源池的资源创建训练作业、创建开发环境实例，部署推理服务等。

#### 场景介绍

对于ModelArts专属资源池的用户，不允许使用公共资源池创建训练作业、创建Notebook实例或者部署推理服务时，可以通过权限控制限制用户使用公共资源池。

涉及配置的自定义权限策略项如下；

- modelarts:notebook:create：此策略项表示创建Notebook实例。
- modelarts:trainJob:create：此策略项表示创建训练作业。
- modelarts:service:create：此策略项表示创建推理服务。

#### 给子账号配置权限：限制使用公共资源池

1. 使用主用户账号登录管理控制台，单击右上角用户名，在下拉框中选择“统一身份认证”，进入统一身份认证（IAM）服务。
2. 在统一身份认证服务页面的左侧导航选择“权限管理 > 权限”，单击右上角的“创建自定义策略”，设置策略，单击“确定”。
  - “策略名称”：设置自定义策略名称，例如：不允许用户使用公共资源池创建。
  - “策略配置方式”：选择可视化视图或者JSON视图均可。
  - “策略内容”：拒绝，云服务中搜索“ModelArts”服务并选中，“操作”中查找写操作“modelarts:trainJob:create”、“modelarts:notebook:create”和“modelarts:service:create”并选中。“所有资源”选择“默认值”。“请求条件”中单击“添加条件”，设置“条件键”为“modelarts:poolType”，“运算符”为“StringEquals”，“值”为“public”。



图 7-63 创建自定义策略（可视化视图）

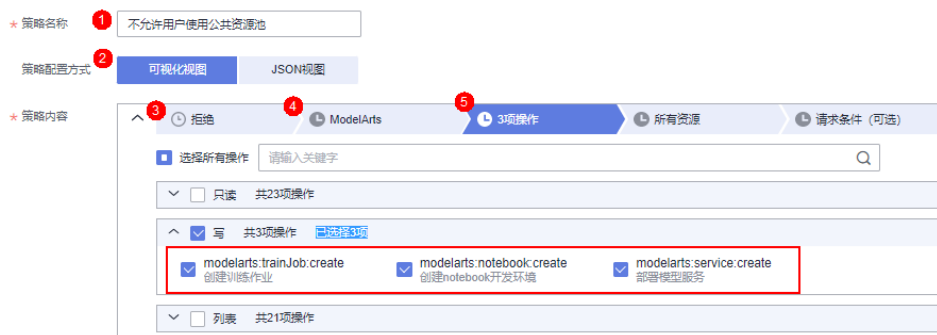
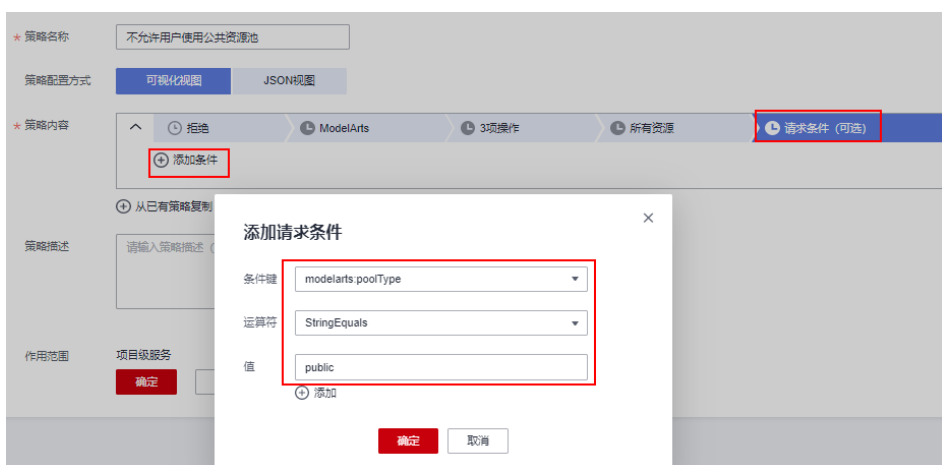


图 7-64 设置请求条件（可视化视图）



JSON视图的策略内容如下：

```
{
 "Version": "1.1",
 "Statement": [
 {
 "Effect": "Deny",
 "Action": [
 "modelarts:trainJob:create",
 "modelarts:notebook:create",
 "modelarts:service:create"
],
 "Condition": {
 "StringEquals": {
 "modelarts:poolType": [
 "public"
]
 }
 }
 }
]
}
```

3. 在统一身份认证服务页面的左侧导航选择“用户组”，在用户组页面查找待授权的用户组名称，在右侧的操作列单击“授权”，勾选步骤2创建的两条自定义策略，单击“下一步”，选择授权范围方案，单击“确定”。

此时，该用户组下的所有用户均有权查看该用户组内成员创建的所有Notebook实例。

如果没有用户组，也可以创建一个新的用户组，并通过“用户组管理”功能添加用户，并配置授权。如果指定的子用户没有在用户组中，也可以通过“用户组管理”功能增加用户。

4. 在用户的委托授权中同步增加此策略，避免在租户面通过委托token突破限制。在统一身份认证服务页面的左侧导航中选择委托，找到该用户组在ModelArts上使用的委托名称，单击右侧的“修改”操作，选择“授权记录”页签，单击“授权”，选中上一步创建的自定义策略“不允许用户使用公共资源池”，单击“下一步”，选择允许使用的资源区域，单击“确定”。

图 7-65 修改授权



## 验证

使用子账号用户登录ModelArts控制台，选择“训练管理 > 训练作业”，单击“创建训练作业”，在创建训练页面，资源池规格只能选择专属资源池。

使用子账号用户登录ModelArts控制台，选择“开发环境 > Notebook”，单击“创建”，在创建Notebook页面，资源池规格只能选择专属资源池。

使用子账号用户登录ModelArts控制台，选择“部署上线 > 在线服务”，单击“部署”，在部署服务页面，资源池规格只能选择专属资源池。

## 7.3.10 给予用户配置文件夹级的 SFS Turbo 访问权限

### 场景描述

本文介绍如何配置文件夹级的SFS Turbo访问权限，实现在ModelArts中访问挂载的SFS Turbo时，只允许子用户访问特定的SFS Turbo文件夹内容。

### 前提条件

- 需要在ModelArts控制台打开严格授权模式，单击“全局配置 > 启用严格模式”。
- 如果打开严格模式前没有为子用户配置过ModelArts权限，开启严格授权模式后可能会导致子用户无法使用ModelArts功能，请参考[快速配置ModelArts访问权限](#)为子用户配置权限。

### 操作步骤

- 步骤1** 使用主用户账号登录管理控制台，鼠标放在右上角用户名，在下拉框中选择“统一身份认证”，进入统一身份认证（IAM）服务。
- 步骤2** 在统一身份认证服务页面的左侧导航选择“权限管理 > 权限”，单击右上角的“创建自定义策略”，设置策略。

- “策略名称”：设置自定义策略名称，例如：ma\_sfs\_turbo。
- “策略配置方式”：JSON视图。
- “策略内容”：填入如下内容。

```

{
 "Version": "1.1",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": [
 "<modelarts_action>"
],
 "Condition": {
 "StringEquals": {
 "modelarts:sfsId": [
 "<your_ssf_id>"
],
 "modelarts:sfsPath": [
 "<sfs_path>"
],
 "modelarts:sfsOption": [
 "<sfs_option>"
]
 }
 }
 }
]
}

```

以上代码中的"<modelarts\_action>"、"<your\_ssf\_id>"、"<sfs\_path>"、"<sfs\_option>"，需要根据您的业务需求替换为实际的参数，各参数含义如下。

表 7-30 参数解释

| 参数              | 参数解释                                                                                                                                                                                                                                                                   |
|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Action          | 表示在何种场景下授予SFS Turbo文件夹访问权限。 <ul style="list-style-type: none"> <li>• 创建开发环境实例：modelarts:trainJob:create</li> <li>• 创建训练作业：modelarts:notebook:create</li> </ul> 支持填写多种Action，例如： <pre>"Action": [   "modelarts:trainJob:create",   "modelarts:notebook:create" ],</pre> |
| modelarts:sfsId | SFS Turbo的ID，在SFS Turbo详情页查看。支持填写多个ID，例如： <pre>"modelarts:sfsId": [   "0e51c7d5-d90e-475a-b5d0-ecf896da3b0d",   "2a70da1e-ea87-4ee4-ae1e-55df846e7f41" ],</pre>                                                                                                        |

| 参数                | 参数解释                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| modelarts:sfsPath | <p>需要进行权限配置的SFS Turbo文件夹路径。支持填写多个路径，例如：</p> <pre data-bbox="603 360 1428 465">"modelarts:sfsPath": [   "/path1",   "/path2/path2-1" ],</pre> <p>如果sfsId中填写了多个ID，则sfsPath会应用于所有sfsId。例如以下代码含义为：为"0e51c7d5-d90e-475a-b5d0-ecf896da3b0d"的"/path1"和"/path2/path2-1"配置访问权限，同时也为"2a70da1e-ea87-4ee4-ae1e-55df846e7f41"的"/path1"和"/path2/path2-1"配置访问权限。</p> <pre data-bbox="603 645 1428 846">"modelarts:sfsId": [   "0e51c7d5-d90e-475a-b5d0-ecf896da3b0d",   "2a70da1e-ea87-4ee4-ae1e-55df846e7f41" ], "modelarts:sfsPath": [   "/path1",   "/path2/path2-1" ],</pre> |

| 参数                  | 参数解释                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|---------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| modelarts:sfsOption | <p>设置用户对于SFS Turbo文件夹的权限类型，支持填写以下参数：</p> <ul style="list-style-type: none"> <li>• 仅读权限：readonly</li> <li>• 读写权限：readwrite</li> </ul> <p>如果需要在自定义策略中添加多个不同的sfsOption，需要在“Statement”中新增JSON结构体，例如：</p> <pre> {   "Version": "1.1",   "Statement": [     {       "Effect": "Allow",       "Action": [         "modelarts:notebook:create"       ],       "Condition": {         "StringEquals": {           "modelarts:sfsId": [             "0e51c7d5-d90e-475a-b5d0-ecf896da3b0d"           ],           "modelarts:sfsPath": [             "/path1"           ],           "modelarts:sfsOption": [             "readonly"           ]         }       }     },     {       "Effect": "Allow",       "Action": [         "modelarts:notebook:create"       ],       "Condition": {         "StringEquals": {           "modelarts:sfsId": [             "0e51c7d5-d90e-475a-b5d0-ecf896da3b0d"           ],           "modelarts:sfsPath": [             "/path2"           ],           "modelarts:sfsOption": [             "readwrite"           ]         }       }     }   ] } </pre> |

**步骤3** 创建用户组并加入用户，步骤请参考[Step1 创建用户组并加入用户](#)。

**步骤4** 给用户组授权策略。在IAM服务的用户组列表页面，单击“授权”，进入到授权页面，为子用户配置权限。勾选[步骤2](#)中创建的“ma\_sfs\_turbo”策略。单击“下一步”和“确定”。

**步骤5** 在已有的ModelArts委托权限中，追加IAM ReadOnlyAccess权限。

1. 在ModelArts管理控制台，单击“全局配置”，在对应委托的操作列，单击“查看权限 > 去IAM修改委托权限”。

图 7-66 去 IAM 修改委托权限



2. 在新页面中，单击“授权记录 > 授权”，搜索“IAM ReadOnlyAccess”，勾选后单击“下一步”并单击“确认”。

图 7-67 IAM ReadOnlyAccess



#### 步骤6 验证权限是否配置成功。

登录子用户账号，在创建训练作业/创建Notebook时，仅能看到配置的SFS Turbo文件夹，则表示权限配置成功。

----结束

## 7.4 FAQ

### 7.4.1 使用 ModelArts 时提示“权限不足”，如何解决？

当您使用ModelArts时如果提示权限不足，请您按照如下指导对相关服务和用户进行授权，并对用户权限进行检查操作。

由于ModelArts的使用权限依赖OBS服务的授权，您需要为用户授予OBS的系统权限。

- 如果您需要授予用户关于OBS的所有权限和ModelArts的基础操作权限，请参见[配置基础操作权限](#)。
- 如果您需要对用户使用OBS和ModelArts的权限进行精细化管理，进行自定义策略配置，请参见[创建ModelArts自定义策略](#)。

### 配置基础操作权限

使用ModelArts的基本功能，您需要为用户配置“作用范围”为“项目级服务”的“ModelArts CommonOperations”权限，由于ModelArts依赖OBS权限，您还需要为用户授予“作用范围”为“全局级服务”的“OBS Administrator”策略。

具体操作步骤如下：

#### 步骤1 创建用户组。

登录IAM管理控制台，单击“用户组>创建用户组”。在“创建用户组”界面，输入“用户组名称”单击“确定”。

#### 步骤2 配置用户组权限。

在用户组列表中，单击步骤1新建的用户组右侧的“授权”，在用户组“授权”页面，您需要配置的权限如下：

1. 配置“作用范围”为“项目级服务”的“ModelArts CommonOperations”权限，如下图所示，然后单击“确定”完成授权。

图 7-68 配置“ModelArts CommonOperations”权限



图 7-69 勾选区域项目



### 说明

区域级项目授权后只在授权区域生效，如果需要所有区域都生效，则所有区域都需要进行授权操作。

2. 配置“作用范围”为“全局级服务”的“OBS Administrator”权限，然后单击“确定”完成授权。

图 7-70 配置“OBS Administrator”权限



图 7-71 选择全局服务资源



### 步骤3 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。

#### 步骤4 用户登录并验证权限。

新创建的用户登录控制台，切换至授权区域，验证权限：

- 在“服务列表”中选择ModelArts，进入ModelArts主界面，选择不同类型的专属资源池，在页面单击“创建”，如果无法进行创建（当前权限仅包含ModelArts CommonOperations），表“ModelArts CommonOperations”已生效。
- 在“服务列表”中选择除ModelArts外（假设当前策略仅包含ModelArts CommonOperations）的任一服务，如果提示权限不足，表示“ModelArts CommonOperations”已生效。
- 在“服务列表”中选择ModelArts，进入ModelArts主界面，单击“数据管理>数据集>创建数据>集”，如果可以成功访问对应的OBS路径，表示全局级服务的“OBS Administrator”已生效。

---结束

## 创建 ModelArts 自定义策略

如果系统预置的ModelArts权限不满足您的授权要求，或者您需要管理用户操作OBS的操作权限，可以创建自定义策略。更多关于创建自定义策略操作和参数说明请参见[创建自定义策略](#)。

目前华为云支持可视化视图创建自定义策略和JSON视图创建自定义策略，本章节将使用JSON视图方式的策略，以为ModelArts用户授予开发环境的使用权限并且配置ModelArts用户OBS相关的最小化权限项为例，指导您进行自定义策略配置。

### 说明

如果一个自定义策略中包含多个服务的授权语句，这些服务必须是同一属性，即都是全局级服务或者项目级服务。

由于OBS为全局服务，ModelArts为项目级服务，所以需要创建两条“作用范围”别为“全局级服务”以及“项目级服务”的自定义策略，然后将两条策略同时授予用户。

1. 创建ModelArts相关OBS的最小化权限的自定义策略，如[图7-72](#)所示。

登录IAM控制台，在“权限管理>权限”页面，单击“创建自定义策略”。参数配置说明如下：

- “策略名称”支持自定义。
- “策略配置方式”为“JSON视图”。
- “策略内容”请参见[ModelArts依赖的OBS权限自定义策略样例](#)，如果您需要了解更多关于OBS的系统权限，请参见[OBS权限管理](#)。



图 7-72 OBS 相关的最小化权限

策略名称: modelarts-obs

策略配置方式: 可视化视图 | **JSON视图**

策略内容:

```
1 {
2 "Version": "1.1",
3 "Statement": [
4 {
5 "Action": [
6 "obs:bucket:ListAllMybuckets",
7 "obs:bucket:HeadBucket",
8 "obs:bucket:ListBucket",
9 "obs:bucket:GetBucketLocation",
10 "obs:object:GetObject",
11 "obs:object:GetObjectVersion",
12 "obs:object:PutObject",
13 "obs:object:DeleteObject",
14 "obs:object:DeleteObjectVersion",
15 "obs:object:ListMultipartUploadParts",
16 "obs:object:AbortMultipartUpload",
17 "obs:object:GetObjectAcl",
18 "obs:object:GetObjectVersionAcl",
19 "obs:bucket:PutBucketAcl",
20 "obs:object:PutObjectAcl"
21],
22 "Effect": "Allow"
23 }
24]
}
```

2. 创建ModelArts开发环境的使用权限的自定义策略，如[图7-73](#)所示。参数配置说明如下：
  - “策略名称”支持自定义。
  - “策略配置方式”为“JSON视图”。
  - “策略内容”请参见[ModelArts开发环境使用权限的自定义策略样例](#)，ModelArts自定义策略中可以添加的授权项（Action）请参见《[ModelArts API参考](#)》>[权限策略和授权项](#)。

图 7-73 开发环境的使用权限



- 如果您需要对除ModelArts和OBS之外的其它服务授权，IAM支持服务的所有策略请参见[权限策略](#)。
- 3. 在IAM控制台[创建用户组并授权](#)。  
在IAM控制台创建用户组之后，将步骤1中创建的自定义策略授权给该用户组。
- 4. [创建用户并加入用户组](#)。  
在IAM控制台创建用户，并将其加入3中创建的用户组。
- 5. [用户登录](#)并验证权限。  
新创建的用户登录控制台，切换至授权区域，验证权限：
  - 在“服务列表”中选择ModelArts，进入ModelArts主界面，单击“数据管理 > 数据集”，如果无法进行创建（当前仅包含开发环境的使用权限），表示仅为ModelArts用户授予开发环境的使用权限已生效。
  - 在“服务列表”中选择除ModelArts，进入ModelArts主界面，单击““开发环境>Notebook>创建””，如果可以成功访问“存储配置”项对应的OBS路径，表示为用户配置的OBS相关权限已生效。

## ModelArts 依赖的 OBS 权限自定义策略样例

如下示例为ModelArts依赖OBS服务的最小化权限项，包含OBS桶和OBS对象的权限。授予示例中的权限您可以通过ModelArts正常访问OBS不受限制。

```

{
 "Version": "1.1",
 "Statement": [
 {
 "Action": [
 "obs:bucket:ListAllMybuckets",
 "obs:bucket:HeadBucket",
 "obs:bucket:ListBucket",
 "obs:bucket:GetBucketLocation",
 "obs:object:GetObject",

```

```
 "obs:object:GetObjectVersion",
 "obs:object:PutObject",
 "obs:object:DeleteObject",
 "obs:object:DeleteObjectVersion",
 "obs:object:ListMultipartUploadParts",
 "obs:object:AbortMultipartUpload",
 "obs:object:GetObjectAcl",
 "obs:object:GetObjectVersionAcl",
 "obs:bucket:PutBucketAcl",
 "obs:object:PutObjectAcl"
],
 "Effect": "Allow"
}
]
```

## ModelArts 开发环境使用权限的自定义策略样例

```
{
 "Version": "1.1",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": [
 "modelarts:notebook:list",
 "modelarts:notebook:create",
 "modelarts:notebook:get",
 "modelarts:notebook:update",
 "modelarts:notebook:delete",
 "modelarts:notebook:action",
 "modelarts:notebook:access"
]
 }
]
}
```

# 8 自动学习

## 8.1 口罩检测（使用新版自动学习实现物体检测应用）

该案例是使用华为云一站式AI开发平台ModelArts的新版“自动学习”功能，基于华为云AI开发者社区AI Gallery中的数据资产，让零AI基础的开发者完成“物体检测”的AI模型的训练和部署。依据开发者提供的标注数据及选择的场景，无需任何代码开发，自动生成满足用户精度要求的模型。可支持图片分类、物体检测、预测分析、声音分类等场景。可根据最终部署环境和开发者需求的推理速度，自动调优并生成满足要求的模型。

开始使用样例前，请仔细阅读**步骤1：准备工作**罗列的要求，提前完成准备工作。使用自动学习功能完成模型构建的步骤如下所示：

- **步骤1：创建训练数据集**
- **步骤3：创建自动学习物体检测项目**
- **步骤4：运行 workflow**
- **步骤5：预测分析**
- **步骤6：清除相应资源**

### 📖 说明

费用说明：本案例使用过程中，从AI Gallery下载数据集免费，在ModelArts上运行训练作业推荐使用免费资源，将模型部署为在线服务推荐使用免费资源。但是数据集存储在OBS桶中会收取少量费用，具体计费请参见[OBS价格详情页](#)，案例使用完成后请参考**步骤6：清除相应资源**及时清除资源和数据。

### 步骤 1：准备工作

- 注册华为账号并开通华为云、实名认证
  - [注册华为账号并开通华为云](#)
  - [进行实名认证](#)
- 配置委托访问授权

ModelArts使用过程中涉及到OBS、SWR、IEF等服务交互，首次使用ModelArts需要用户配置委托授权，允许访问这些依赖服务。

- a. 使用华为云账号登录ModelArts管理控制台，在左侧导航栏单击“全局配置”，进入“全局配置”页面，单击“添加授权”。

- b. 在弹出的“访问授权”窗口中，选择“新增委托”，权限配置选择“普通用户”，并勾选“我已经仔细阅读并同意《ModelArts服务声明》”，然后单击“创建”。

图 8-1 配置委托访问授权



- c. 完成配置后，在ModelArts控制台的全局配置列表，可查看到此账号的委托配置信息。

图 8-2 查看委托配置信息

| 授权对象      | 授权对象类型 | 授权类型 | 授权内容             | 授权方式 | 创建时间                          | 操作                                      |
|-----------|--------|------|------------------|------|-------------------------------|-----------------------------------------|
| all-users | 所有用户   | 委托   | modelarts_agency | 角色授权 | 2023/11/21 09:57:47 GMT+08:00 | <a href="#">查看详情</a> <a href="#">删除</a> |

## 步骤 2：创建训练数据集

1. 单击[口罩检测小数据集](#)进入数据集详情页，单击右侧“下载”。
2. 在弹出的窗口中选择云服务区域，例如该案例选择云服务区域为“华北-北京四”，单击“确定”进入下载详情页。
3. 在“下载详情”页面，填写参数。
  - 下载方式：ModelArts数据集。
  - 目标区域：华北-北京四，目标区域须与[步骤1中的2](#)选择的云服务区域保持一致。
  - 数据类型：图片。
  - 数据集输入位置：用来存放源数据集信息，例如本案例中从Gallery下载的数据集。单击图标选择您的OBS桶下的任意一处目录，但不能与输出位置为同一目录。
  - 数据集输出位置：用来存放输出的数据标注的相关信息，或版本发布生成的Manifest文件等。单击图标选择OBS桶下的空目录，且此目录不能与输入位置一致，也不能为输入位置的子目录。
  - 名称：创建数据集名称，为方便后续创建物体检测项目选择对应的数据集，建议您的数据集名称具有可识别性。
  - 描述：描述数据集详细信息。

图 8-3 下载详情

下载方式 对象存储服务 (OBS) ModelArts数据集

目标区域 华北-北京四

\* 数据类型 图片 音频 文本 视频 自由格式  
支持格式: .jpg、.png、.jpeg、.bmp

\* 数据集输入位置 请选择对象存储服务 (OBS) 路径  
注意: 用来存放源数据集信息, 数据集输入位置不能和输出位置相同。

\* 数据集输出位置 请选择对象存储服务 (OBS) 路径  
注意: 用来存放输出的数据标注的相关信息, 或版本发布生成的Manifest文件等, 此位置不能与输入位置一致, 也不能为输入位置的子目录。

\* 名称 dataset-2ce0

描述



4. 确认无误后单击右下角“确定”。
5. 系统会跳转到我的下载页面，单击  按钮，查看下载进度，等待数据集下载完成（下载完成大约需要5分钟，请耐心等待）。单击  展开下载详情，可以查看该数据集的“目标位置”。

图 8-4 查看数据集

口罩检测小数据集

下载时间 2023-02-08 16:22 发布者 ModelArts.AI开发文件大小 10MB 文件数量 582

---

数据集ID fc0e89d89

下载作业ID 236c368

目标区域 华北-北京四

目标位置

### 步骤 3：创建自动学习物体检测项目

1. 确保数据集创建完成且可正常使用后，在ModelArts控制台，左侧导航栏选择“自动学习”默认进入新版自动学习页面，选择物体检测项目，单击“创建项目”。
2. 进入“创建物体检测”页面后，填写相关参数。
  - 计费模式：默认按需计费。
  - 名称：自行创建项目名称。
  - 描述：自行描述项目详情，例如口罩检测。
  - 数据集：下拉选择已下载的数据集（**步骤1**中已成功导入的数据集，默认为下拉数据集列表中的第一个数据集）。
  - 输出路径：选择**步骤1的3**中的数据集输出位置。
  - 训练规格：根据您的实际需要选择对应的训练规格。根据您的选择的资源规格不同，收费标准不同，价格详情请参见**价格详情**。

图 8-5 创建物体检测

\* 计费模式 按需计费

\* 名称

描述   
0/500

\* 数据集  创建数据集

\* 输出路径  选择

\* 训练规格

3. 确认无误后单击右下角“创建项目”可自动跳转至新版自动学习的运行总览页面。
4. 工作流会依次运行数据标注、数据集版本发布、数据校验、物体检测、模型注册、服务部署等节点，直至工作流全部运行完成。

### 步骤 4：运行工作流

项目完成创建之后，会自动跳转到新版自动学习的运行总览页面。同时您的工作流会自动从数据标注节点开始运行。您需要做的是：

1. 在数据标注节点，待数据标注节点变为橘色即为“等待操作”状态，双击数据标注节点，打开数据标注节点的运行详情页面，单击“继续运行”。
2. 在弹窗中，单击“确定”，工作流会继续从数据标注节点依次运行到服务部署节点。该段时间不需要用户做任何操作。

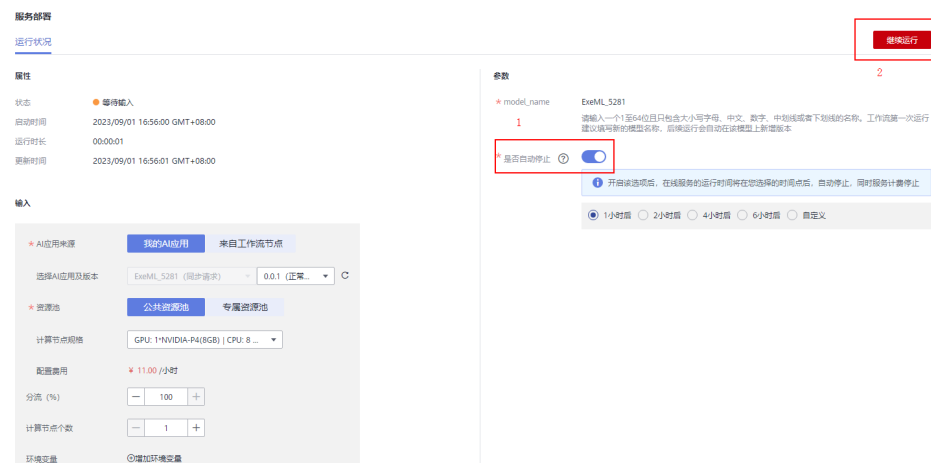
图 8-6 确认继续运行



3. 当工作流运行到“服务部署”节点，状态会变为“等待输入”，需要选择填写以下两个参数，其他参数均为默认值，保持不变：

- 计算节点规格：根据您的实际需求选择相应的规格，不同规格的配置费用不同，价格详情请参见[价格详情](#)。
- 是否自动停止：为避免资源浪费，建议打开自动停止开关，根据您的实际需要，选择自动停止时间，也可以自定义自动停止的时间。

图 8-7 用户输入



4. 参数填写完毕之后，单击运行状况右边的“继续运行”，单击确认弹窗中的“确定”即可继续完成工作流的运行。

图 8-8 继续运行



## 步骤 5：预测分析

运行完成的工作流会自动部署为相应的在线服务，您只需要在相应的服务详情页面进行预测即可。

1. 在服务部署节点单击“实例详情”直接跳转进入在线服务详情页，或者在 ModelArts 管理控制台，选择“部署上线>在线服务”，单击生成的在线服务名称，即可进入在线服务详情页。
2. 在服务详情页，单击选择“预测”页签。



图 8-9 上传预测图片



3. 单击“上传”选择上传一张需要预测的图片，单击“预测”，即可在右边的预测结果显示区查看您的预测结果。

图 8-10 查看预测结果（1）--没戴口罩

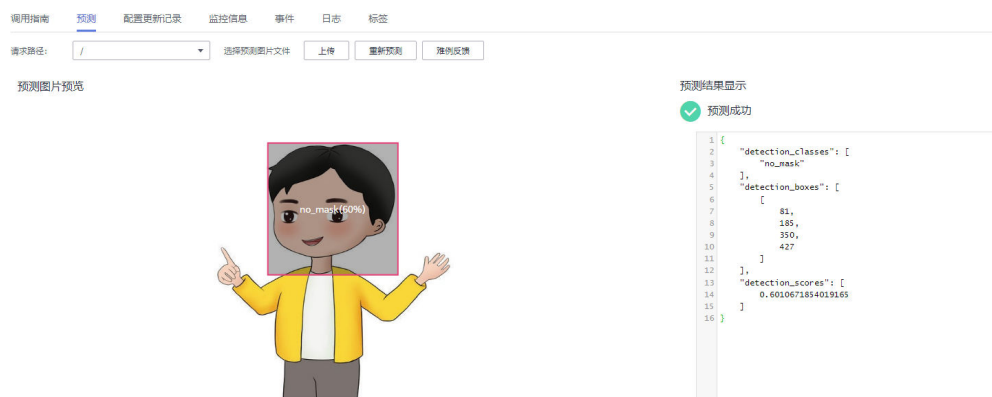


图 8-11 查看预测结果（2）--戴口罩



## 步骤 6: 清除相应资源

在完成预测之后，建议关闭服务，以免产生不必要的计费。

### 1. 停止运行服务


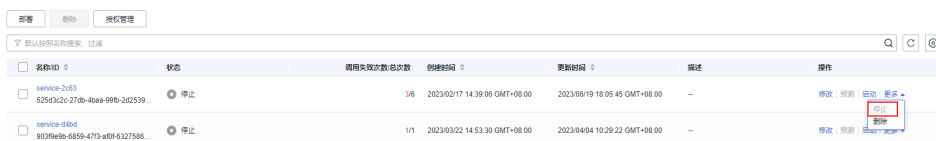

- 预测完成后，单击页面右上角的“停止”，即可停止该服务。
- 单击左上角  返回在线服务，在对应的服务名称所在行，单击选择操作列的“更多>停止”，停止该服务。

图 8-12 停止服务



2. 清除OBS中的数据。

- a. 在控制台左侧导航栏的服务列表 ，选择“对象存储服务OBS”，进入OBS服务详情页面。
- b. 在左侧导航栏选择“桶列表”，在列表详情，找到自己创建的OBS桶，单击桶名称，进入OBS桶详情。
- c. 在桶的详情页，左侧导航栏选择“对象”，在右侧“名称”列选中不需要的存储对象，在操作列单击“更多”，选择“删除”，即可删除相应的存储对象。

常见问题

- 创建数据集时找不到创建的OBS桶，请[查看OBS桶与ModelArts是否在同一个区域](#)。
- 数据校验节点失败。  
请查看您的数据集是否符合规范，数据集规范请参考[数据集要求与上传规范](#)。

## 8.2 垃圾分类（使用新版自动学习实现图像分类）

随着科技发展与人们生活质量的快速提升，生活垃圾分类成为当下越来越热门的话题，常见的生活垃圾分为厨余垃圾蛋壳、厨余垃圾水果果皮、可回收物塑料玩具、可回收物纸板箱、其他垃圾烟蒂、其他垃圾一次性餐盒、有害垃圾干电池、有害垃圾过期药物等。人工识别效率低下、费时费力，AI技术显然可以为此贡献一份力量。

该案例介绍了华为云一站式开发平台ModelArts的自动学习功能实现的常见生活垃圾分类，让您不用编写代码也可以实现生活垃圾分类。

 说明

本案例只适用于新版自动学习功能。

### 步骤 1：准备工作

注册华为账号并开通华为云、实名认证

- [注册华为账号并开通华为云](#)
- [进行实名认证](#)

### 步骤 2：创建 OBS 桶

1. 登录[OBS管理控制台](#)，在桶列表页面右上角单击“创建桶”，创建OBS桶。例如，创建名称为“dataset-exeml”的OBS桶。

图 8-13 创建桶



**说明**

- 创建桶的区域需要与ModelArts所在的区域一致。例如：当前ModelArts在华北-北京四区域，在对象存储服务创建桶时，请选择华北-北京四。请参考[查看OBS桶与ModelArts是否在同一区域](#)检查您的OBS桶区域与ModelArts区域是否一致。
  - 请勿开启桶加密，ModelArts不支持加密的OBS桶，会导致ModelArts读取OBS中的数据失败。
2. 在桶列表页面，单击桶名称，进入该桶的概览页面。

图 8-14 桶列表



3. 单击左侧导航的“对象”，在对象页面单击“新建文件夹”，创建OBS文件夹。具体请参见[新建文件夹](#)章节。

图 8-15 新建文件夹



### 步骤 3: 准备训练数据集



1. 单击**8类常见生活垃圾图片数据集**，进入AI Gallery数据集详情页，单击右侧“下载”。
2. 选择对应的云服务区域例如：华北-北京四，需要确保您选择的区域与您的管理控制台所在的区域一致。
3. 进入“下载详情”页面，填写以下参数。
  - 下载方式：ModelArts数据集。
  - 目标区域：华北-北京四。
  - 数据类型：系统会根据您的数据集，匹配到相应的数据类型。例如本案例使用的数据集，系统匹配为“图片”类型。
  - 数据集输入位置：用来存放源数据集信息，例如本案例中从Gallery下载的数据集。单击图标选择您的OBS桶下的任意一处目录，但不能与输出位置为同一目录。
  - 数据集输出位置：用来存放输出的数据标注的相关信息，或版本发布生成的Manifest文件等。单击图标选择OBS桶下的空目录，且此目录不能与输入位置一致，也不能为输入位置的子目录。

图 8-16 下载详情



下载方式 对象存储服务 (OBS) ModelArts数据集

目标区域 华北-北京四

\* 数据类型 图片 音频 文本 视频 自由格式  
支持格式: .jpg、.png、.jpeg、.bmp

\* 数据集输入位置 请选择对象存储服务 (OBS) 路径   
注意: 用来存放源数据集信息, 数据集输入位置不能和输出位置相同。

\* 数据集输出位置 请选择对象存储服务 (OBS) 路径   
注意: 用来存放输出的数据标注的相关信息, 或版本发布生成的Manifest文件等。此位置不能与输入位置一致, 也不能为输入位置的子目录。

\* 名称 dataset-2ce0

描述

4. 完成参数填写，单击“确定”，自动跳转至AI Gallery个人中心“我的下载”页



签，单击按钮，查看下载进度，等待5分钟左右下载完成，单击展开下载详情，可以查看该数据集的“目标位置”。

图 8-17 等待下载完成

| 8类常见生活垃圾图片数据集 |                  |
|---------------|------------------|
| 下载时间          | 2023-07-12 14:18 |
| 发布者           | WAYNE            |
| 文件大小          | 20MB             |
| 文件数量          | 1600             |
| 数据集ID         | 8af...74af3a     |
| 下载作业ID        | 002...3301       |
| 目标区域          | 华北-北京四           |
| 目标位置          | /sw...12/        |

## 步骤 4：配置委托访问授权

ModelArts使用过程中涉及到OBS、SWR、IEF等服务交互，首次使用ModelArts需要用户配置委托授权，允许访问这些依赖服务。

1. 使用华为云账号登录**ModelArts管理控制台**，在左侧导航栏单击“全局配置”，进入“全局配置”页面，单击“添加授权”。
2. 在弹出的“访问授权”窗口中，参数选择如下：
  - 授权对象类型：所有用户
  - 委托选择：新增委托
  - 权限配置：普通用户

选择完成后勾选“我已经仔细阅读并同意《ModelArts服务声明》”，然后单击“创建”。

图 8-18 配置委托访问授权



3. 完成配置后，在ModelArts控制台的全局配置列表，可查看到此账号的委托配置信息。

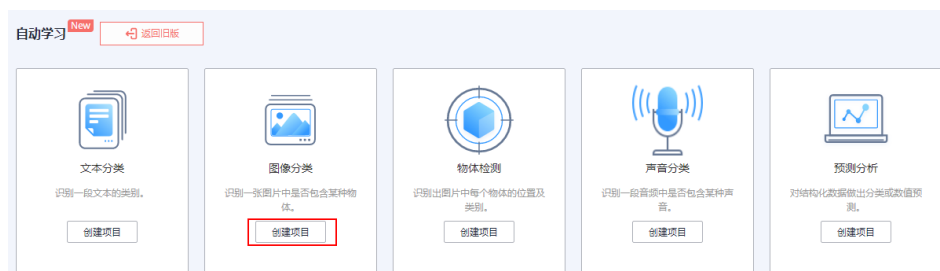
图 8-19 查看委托配置信息



## 步骤 5：创建新版自动学习图像分类项目

1. 确保数据集创建完成且可正常使用后，在ModelArts控制台，左侧导航栏选择“自动学习”，进入自动学习总览页面。

图 8-20 创建项目



- 单击选择“图像分类”创建项目。完成参数填写：
  - 计费模式：按需计费。
  - 名称：自定义您的项目名称。
  - 描述：自定义描述您的项目详情，例如垃圾分类。
  - 数据集：下拉选择已下载的数据集（[步骤2](#)中已成功导入的数据集，默认为下拉数据集列表中的第一个数据集）。
  - 输出路径：选择您[步骤1](#)创建好的OBS文件夹下的路径，用来存储训练模型等相关文件。
  - 训练规格：根据您的实际需要选择对应的训练规格。根据您的选择的资源规格不同，收费标准不同，价格详情请参见[价格详情](#)。

图 8-21 创建图像分类

The screenshot shows a form for creating an image classification project. The fields are as follows:

- 计费模式**: 按需计费 (Selected)
- 名称**: ExeML\_dd2f
- 描述**: (Empty text area, 0/500 characters)
- 数据集**: 请选择数据集 (Dropdown menu, with a '创建数据集' button)
- 输出路径**: (Empty text field, with a '选择' button)
- 训练规格**: 请选择规格 (Dropdown menu)

- 参数填写完成，单击“创建项目”。

## 步骤 6: 运行 workflow

项目完成创建之后，会自动跳转到新版自动学习的运行总览页面。同时您的 workflow 会自动从数据标注节点开始运行。您需要做的是：

- 观察数据标注节点，待数据标注节点变为橘色即为“等待操作”状态。双击数据标注节点，打开数据标注节点的运行详情页面，单击“继续运行”。
- 在弹出的窗口中，单击“确定”，workflow 会开始继续运行。
- 当 workflow 运行到“服务部署”节点，状态会变为“等待输入”，您需要填写以下两个输入参数，其他参数保持默认。
  - 计算节点规格：根据您的实际需求选择相应的规格，不同规格的配置费用不同，选择好规格后，配置费用处会显示相应的费用。
  - 是否自动停止：为了避免资源浪费，建议您打开该开关，根据您的需求，选择自动停止时间，也可以自定义自动停止的时间。

图 8-22 用户输入



### 说明

- 只有华北-北京四支持限时免费规格，且每个用户只限创建一个基于免费规格的实例。
- 参数填写完毕之后，单击运行状况右边的“继续运行”，单击确认弹窗中的“确定”即可继续完成工作流的运行。

图 8-23 继续运行



## 步骤 7：预测分析

运行完成的工作流会自动部署相应的在线服务，您只需要在相应的服务详情页面进行预测即可。

- 在服务部署节点单击“实例详情”或者在ModelArts管理控制台，选择“部署上线>在线服务”，单击生成的在线服务名称，即可进入在线服务详情页。
- 在服务详情页，单击选择“预测”页签。

图 8-24 上传预测图片





3. 单击“上传”选择一张需要预测的图片，单击“预测”，即可在右边的预测结果显示区查看您的预测结果。

图 8-25 预测样例图



图 8-26 查看预测结果



### 说明

本案例中数据和算法生成的模型仅适用于教学模式，并不能应对复杂的预测场景。即生成的模型对预测图片有一定范围和要求，预测图片必须和训练数据集中的图片相似才可能预测准确。

ModelArts的AI Gallery中提供了常见的精度较高的算法和相应的训练数据集，用户可以在 [AI Gallery的资产集市](#) 中获取。

## 步骤 8：清除相应资源

在完成预测之后，建议关闭服务，以免产生不必要的计费。

### 1. 停止运行服务

- 预测完成后，单击页面右上角的“停止”，即可停止该服务。




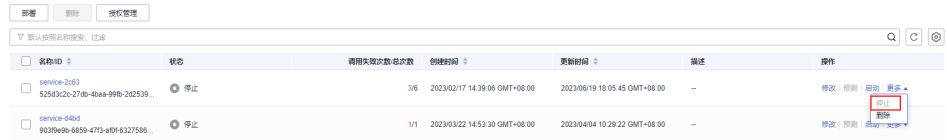

- 单击左上角  返回在线服务，在对应的服务名称所在行，单击选择操作列的“更多>停止”，停止该服务。

图 8-27 停止服务



| 名称ID                                            | 状态 | 调用失败次数 | 启动次数 | 创建时间                          | 更新时间                          | 描述 | 操作       |
|-------------------------------------------------|----|--------|------|-------------------------------|-------------------------------|----|----------|
| service-2d83<br>42565c2c-279b-4baa-999b-2d2539  | 停止 | 3/6    |      | 2023/02/17 14:39:06 GMT+08:00 | 2023/06/19 18:05:45 GMT+08:00 | -- | 修改 删除 更多 |
| service-d4d4<br>91399e9e-6859-47f3-af0f-6327586 | 停止 | 1/1    |      | 2023/03/02 14:53:30 GMT+08:00 | 2023/04/04 10:29:22 GMT+08:00 | -- | 修改 删除 更多 |

2. 清除OBS中的数据。

- 在控制台左侧导航栏的服务列表 ，选择“对象存储服务OBS”，进入OBS服务详情页面。
- 在左侧导航栏选择“桶列表”，在列表详情，找到自己创建的OBS桶，单击桶名称，进入OBS桶详情。
- 在桶的详情页，左侧导航栏选择“对象”，在右侧“名称”列选中不需要的存储对象，在操作列单击“更多”，选择“删除”，即可删除相应的存储对象。

常见问题

- 创建数据集时找不到创建的OBS桶，请[查看OBS桶与ModelArts是否在同一个区域](#)。
- 数据校验节点失败。  
请查看您的数据集是否符合规范，数据集规范请参考[数据集要求与上传规范](#)。

# 9 开发环境

## 9.1 使用算法套件快速完成水表读数识别

本示例围绕真实AI需求场景，介绍算法开发套件在水表表盘读数识别算法开发任务上的使用流程。

算法开发套件中目前提供自研(ivg系列)和开源(mm系列)共两套算法资产，可应用于分类、检测、分割和OCR等任务中。本示例中将组合使用自研分割算法(ivgSegmentation)和开源OCR算法(mmOCR)完成水表读数识别项目，并使用算法开发套件将其部署为华为云在线服务。

### 📖 说明

本案例教程仅适用于“华北-北京四”区域，新版Notebook。

### 准备数据

1. 登录OBS控制台，创建OBS对象桶，区域选择“华北-北京四”。
2. 登录ModelArts控制台，选择控制台区域为“华北-北京四”。
3. 在“全局配置”页面查看是否已经配置授权，允许ModelArts访问OBS。如果没有配置授权，请参考[配置访问授权（全局配置）](#)添加授权。
4. 分别下载本案例的数据集，[水表表盘分割数据集](#)和[水表表盘读数OCR识别数据集](#)到OBS桶中，单击数据集右侧的“下载”，弹出“选择云服务区域”，选择区域后单击“确定”进入下载详情页面。下载方式选择“对象存储服务（OBS）”，填写OBS路径信息等，详细步骤请参考[下载数据集](#)。

OBS路径示例如下：

obs://{OBS桶名称}/water\_meter\_segmentation 水表表盘分割数据集

obs://{OBS桶名称}/water\_meter\_crop 水表表盘读数OCR识别数据集

### 📖 说明

从AI Gallery下载数据集免费，但是数据集存储在OBS桶中会收取少量费用，具体计费请参见[OBS价格详情页](#)，案例使用完成后请及时清除资源和数据。

## 准备开发环境

1. 在ModelArts控制台的“开发环境 > Notebook”页面中，创建基于pytorch1.8-cuda10.2-cudnn7-ubuntu18.04镜像，类型为GPU，具体操作请参见[创建 Notebook实例](#)章节。

如果需要使用本地IDE（PyCharm或VS Code）远程连接Notebook，需要开启SSH远程开发。本案例以在线的JupyterLab为例介绍整个过程。

图 9-1 创建 Notebook 实例



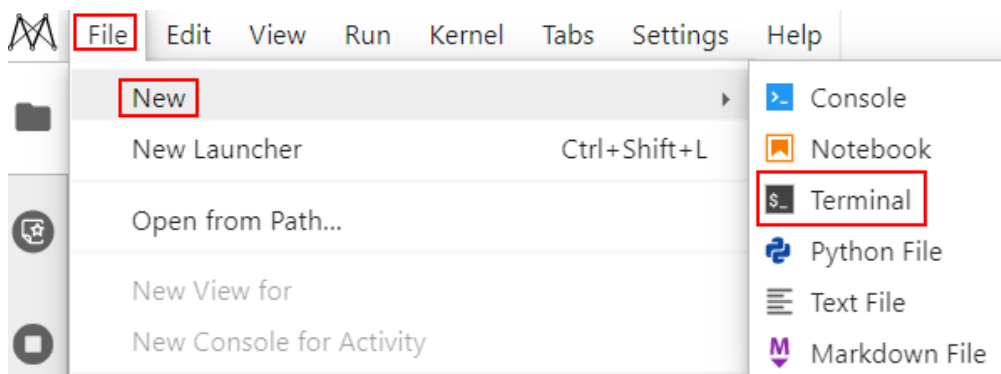
2. Notebook创建完成后，状态为“运行中”。单击“操作”栏的“打开”，进入JupyterLab页面。

图 9-2 使用 JupyterLab 打开

| 名称       | 状态             | 镜像                                  | 规格          | 描述  | 创建时间                          | 创建者 | 操作          |
|----------|----------------|-------------------------------------|-------------|-----|-------------------------------|-----|-------------|
| notebook | 运行中 (59分种后...) | pytorch1.8-cuda10.2-cudnn7-ubunt... | CPU: 2核 8GB | ... | 2023/09/04 15:50:45 GMT+08:00 |     | 打开 自动 停止 更多 |

3. 打开JupyterLab的Terminal。此处以Terminal为例介绍整个过程。JupyterLab更多操作请参见[JupyterLab简介及常用操作](#)。

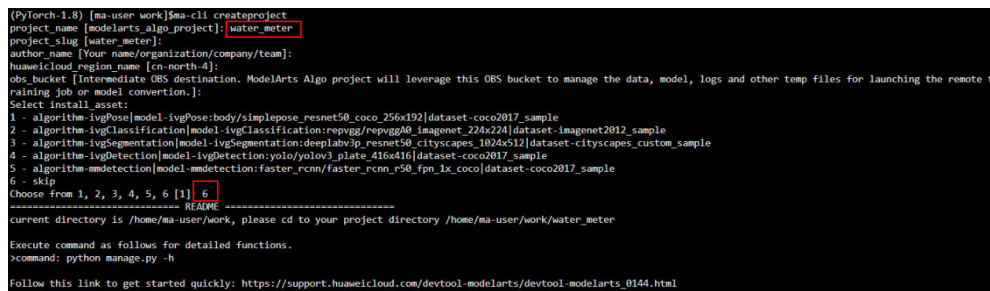
图 9-3 打开 Terminal



## Step1 创建算法工程

1. 在JupyterLab的Terminal中，在work目录下执行**ma-cli createproject**命令创建工程，根据提示输入工程名称，例如：`water_meter`。然后按回车键选择默认参数（连续按五次回车），并选择跳过资产安装步骤（选择6）。

图 9-4 创建工程



2. 执行以下命令进入工程目录。  
`cd water_meter`
3. 执行以下命令复制项目数据到Notebook中。  
`python manage.py copy --source {obs_dataset_path} --dest ./data/raw/water_meter_crop`  
`python manage.py copy --source {obs_dataset_path} --dest ./data/raw/water_meter_segmentation`

### 说明

{obs\_dataset\_path}路径为**Step1 准备数据**中下载到OBS中的数据路径，比如“obs://{OBS桶名称}/water\_meter\_segmentation”和“obs://{OBS桶名称}/water\_meter\_crop”

图 9-5 复制数据集到 Notebook 中



## Step2 使用 deeplabv3 完成水表区域分割任务

1. 执行如下命令安装ivgSegmentation套件。  
`python manage.py install algorithm ivgSegmentation==1.0.2`

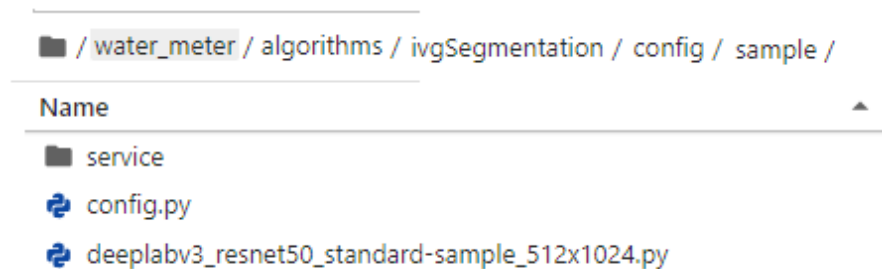
图 9-6 ivgSegmentation 套件安装成功

```
INFO:ma_cau:Successfully installed ivgSegmentation_1.0.2 to /home/ma-user/work/water_meter/algorithms/ivgSegmentation
```

如果提示ivgSegmentation版本不正确，可以通过命令**python manage.py list algorithm**查询版本。

2. 安装ivgSegmentation套件后，在JupyterLab界面左侧的工程目录中进入“./algorithms/ivgSegmentation/config/sample”文件夹中查看目前支持的分割模型，以sample为例（sample默认的算法就是deeplabv3），文件夹中包括config.py（算法外壳配置）和deeplabv3\_resnet50\_standard-sample\_512x1024.py（模型结构）。

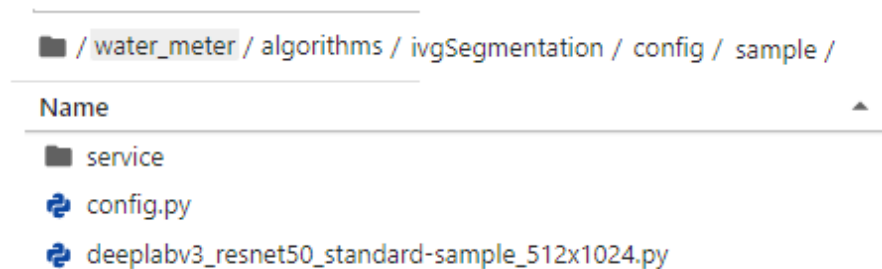
图 9-7 进入 sample 文件夹



3. 表盘分割只需要区分背景和读数区域，因此属于二分类，需要根据项目所需数据集对配置文件进行修改，如下所示：

修改“config.py”文件。

图 9-8 修改 sample 文件夹下的 config.py 文件



```
config.py
```

```
...
alg_cfg = dict(
...
 data_root='data/raw/water_meter_segmentation', # 修改为真实路径本地分割数据集路
径
...
)
```

修改完后按Ctrl+S保存。

4. 修改“deeplabv3\_resnet50\_standard-sample\_512x1024.py”文件。

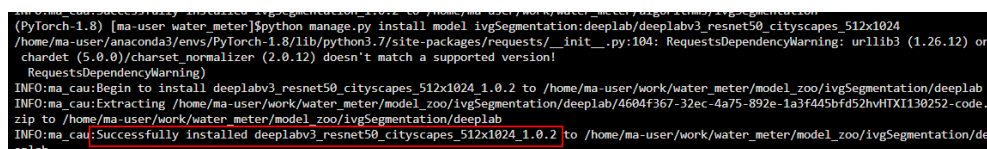
图 9-9 修改 deeplabv3\_resnet50\_standard-sample\_512x1024.py 文件



修改完按Ctrl+S保存。

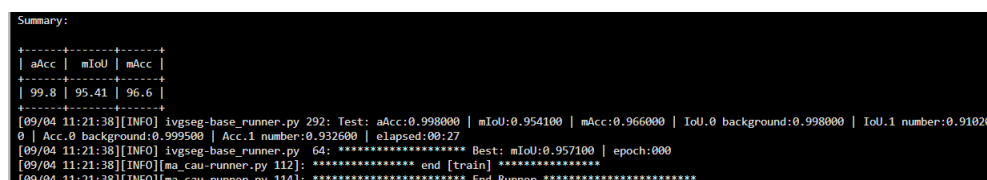
5. 在water\_meter工程目录下，执行如下命令安装deeplabv3预训练模型。  
python manage.py install model ivgSegmentation:deeplab/  
deeplabv3\_resnet50\_cityscapes\_512x1024

图 9-10 安装 deeplabv3 预训练模型



6. 执行如下命令训练分割模型。（推荐使用GPU进行训练）  
python manage.py run --cfg algorithms/ivgSegmentation/config/sample/config.py --gpus 0

图 9-11 分割模型训练结果



训练好的模型会保存在指定位置中，默认为“./output/deeplabv3\_resnet50\_standard-sample\_512x1024/checkpoints/”中。

7. 验证模型效果。  
模型训练完成后，可以在验证集上计算模型的指标，首先修改配置文件的模型位置。  
修改“config.py”文件，修改完按Ctrl+S保存。

```
config.py
...
alg_cfg = dict(
...
 load_from='./output/deeplabv3_resnet50_standard-sample_512x1024/checkpoints/
checkpoint_best.pth.tar', # 修改训练模型的路径
...
)
```

执行如下命令计算模型指标。

```
python manage.py run --cfg algorithms/ivgSegmentation/config/sample/config.py --
pipeline evaluate
```

图 9-12 模型指标计算结果

```
[09/04 11:37:07][INFO] ivgseg-base_runner.py 292: Test: aAcc:0.998100 | mIoU:0.957100 | mAcc:0.972400 | IoU.0 background:0.998100 | IoU.1 number:0.91610
0 | Acc.0 background:0.999300 | Acc.1 number:0.945500 | elapsed:11:40
[09/04 11:37:07][INFO][ma_cau-runner.py 112]: ***** end [evaluate] *****
[09/04 11:37:07][INFO][ma_cau-runner.py 114]: ***** End Runner *****
```

## 8. 模型推理。

模型推理能够指定某一张图片，并且推理出图片的分割区域，并进行可视化，首先需要指定需要推理的图片路径。

修改“config.py”文件，修改完按Ctrl+S保存。

```
alg_cfg = dict(
...
 img_file='./data/raw/water_meter_segmentation/image/train_10.jpg' # 指定需要推理的图
 片路径
...
)
```

执行如下命令推理模型。

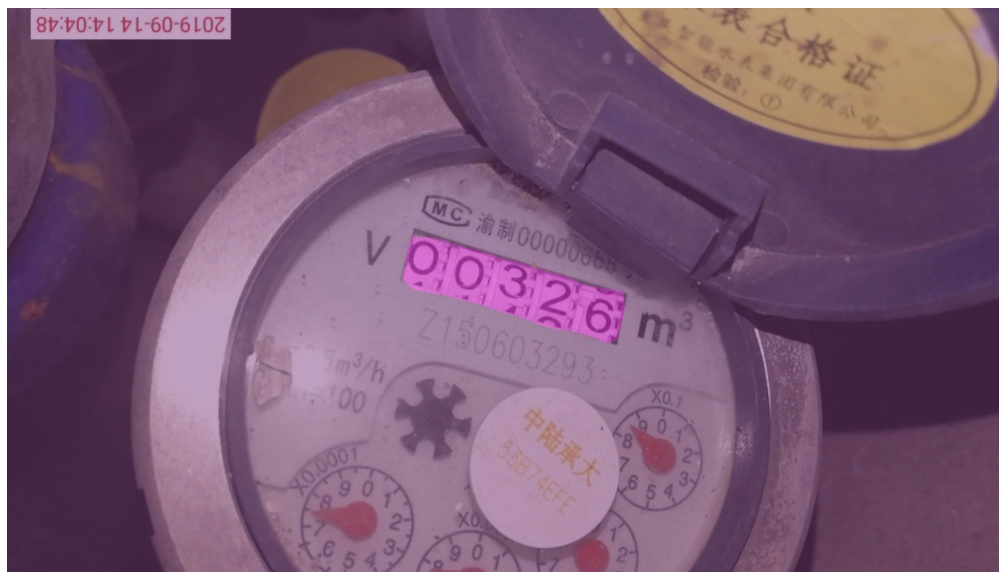
```
python manage.py run --cfg algorithms/ivgSegmentation/config/sample/config.py --
pipeline infer
```

图 9-13 表盘分割模型推理结果

```
--> results-[segmentation result is ignored because it is too large]
100% | 1/1 [00:03<00:00, 3.94s/it]
[09/04 11:38:54][INFO][ma_cau-runner.py 112]: ***** end [infer] *****
[09/04 11:38:54][INFO][ma_cau-runner.py 114]: ***** End Runner *****
```

推理输出的图片路径在“./output/deeplabv3\_resnet50\_standard-sample\_512x1024”下。

图 9-14 水表表盘分割结果可视化



9. 执行如下命令导出算法SDK。  
`python manage.py export --cfg algorithms/ivgSegmentation/config/sample/config.py --is_deploy`  
算法开发套件支持将模型导出成一个模型SDK，方便进行模型部署等下游任务。SDK导出的路径为“./export/deeplabv3\_resnet50\_standard-sample\_512x1024/Linux\_x86\_64\_GPU\_PyTorch\_Common\_py”

图 9-15 SDK 导出路径

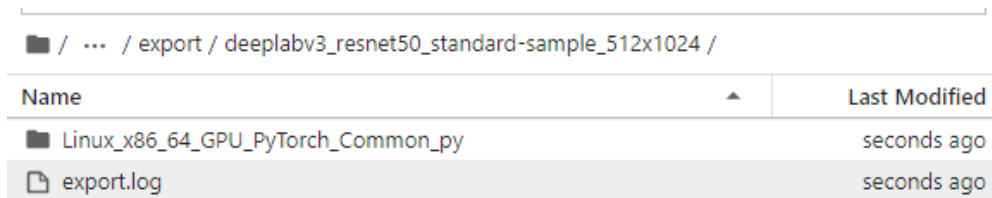
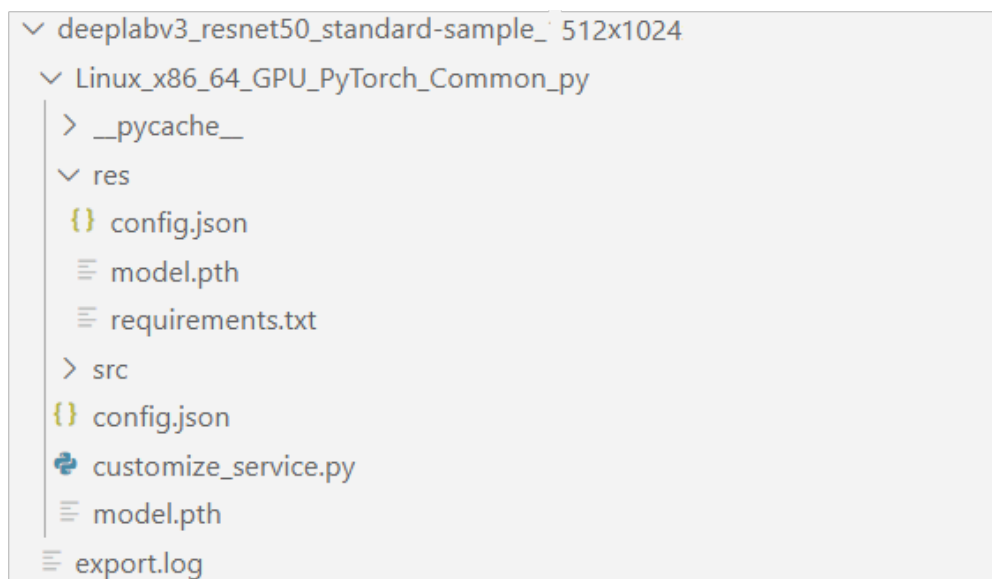


图 9-16 SDK 导出示意图

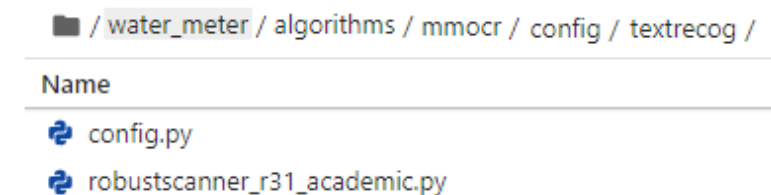




## Step3 水表读数识别

1. 执行如下命令安装mmocr套件。  
python manage.py install algorithm mmocr==0.2.1
2. 安装mmocr套件后，“./algorithms/mmocr/config/textrecog”文件夹中包括config.py（算法外壳配置）和robustscanner\_r31\_academic.py（模型结构），需要根据所需算法和数据集路径修改配置文件。以下以robust\_scanner算法为例。

图 9-17 进入 textrecog 文件夹



修改“robustscanner\_r31\_academic.py”，如下所示：

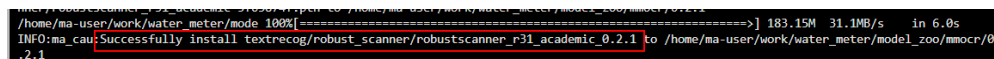
```

...
train_prefix = 'data/raw/water_meter_crop/' # 修改数据集路径改为水表ocr识别数据集路径
train_img_prefix1 = train_prefix + 'train'
train_ann_file1 = train_prefix + 'train.txt'
...
test_prefix = 'data/raw/water_meter_crop/'
test_img_prefix1 = test_prefix + 'val/'
test_ann_file1 = test_prefix + 'val.txt'

```

3. 执行如下命令安装robust\_scanner预训练模型。  
python manage.py install model mmocr:textrecog/robust\_scanner/  
robustscanner\_r31\_academic

图 9-18 安装 robust\_scanner 模型



4. 训练OCR模型。  
初次使用mmcv时需要编译mmcv-full，该过程较慢，可以直接使用官方预编译的依赖包。

预编译包URL：<https://download.openmmlab.com/mmcv/dist/cu102/torch1.6.0/index.html>

```

pip uninstall mmcv -y
pip install https://download.openmmlab.com/mmcv/dist/cu102/torch1.6.0/mmcv_full-1.3.9-cp37-cp37m-manylinux1_x86_64.whl
pip install rapidfuzz==2.15.1
pip install numpy -U

```

修改“./algorithms/mmocr/config/textrecog/config.py”，将EPOCHS（迭代数量）改为2。

图 9-19 修改 textrecog 文件夹下的 config.py 文件

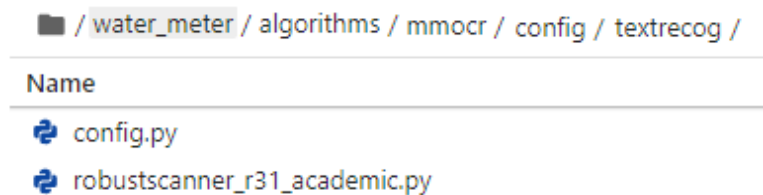


图 9-20 迭代数量修改为 2

```
BATCH_SIZE = 128
EPOCHS = 2
LR = 1e-3

/cache is recommended for data root
```

执行如下命令训练OCR模型。（仅使用GPU进行训练，大概需要几分钟）

```
python manage.py run --cfg algorithms/mmocr/config/textrecog/config.py
```

图 9-21 OCR 模型训练结果

```
2023-09-04 11:00:39,876 - mmocr - INFO - Exp name: robustscanner_r31_academic.py
2023-09-04 11:00:39,876 - mmocr - INFO - Epoch(val) [2][2] 0_word_acc: 0.8300, 0_word_acc_ignore_case: 0.8300, 0_word_acc_ignore_case_symbol: 0.8300, 0_char_recall: 0.9650, 0_char_precision: 0.9650, 0_1-N.E.D: 0.9650
[09/04 11:00:41][INFO][ma_cau-runner.py 112]: ***** end [train] *****
[09/04 11:00:41][INFO][ma_cau-runner.py 114]: ***** End Runner *****
```

训练好的模型会保存在指定位置中，默认为output/robustscanner\_r31\_academic/文件夹中。

5. 验证模型效果。

模型训练完成后，可以在验证集上计算模型的指标，首先修改配置文件的模型位置。

修改“./algorithms/mmocr/config/textrecog/config.py”

```
#config.py
```

```
...
model_path = './output/robustscanner_r31_academic/latest.pth'
...
```

执行如下命令验证模型。

```
python manage.py run --cfg algorithms/mmocr/config/textrecog/config.py --pipeline evaluate
```

图 9-22 计算模型的指标

```
Evaluating data/raw/water_meter_crop/val.txt with 200 images now
{'0_word_acc': 0.83, '0_word_acc_ignore_case': 0.83, '0_word_acc_ignore_case_symbol': 0.83, '0_char_recall': 0.965, '0_char_precision': 0.965, '0_1-N.E.D': 0.965}
[09/04 11:03:39][INFO][ma_cau-runner.py 112]: ***** end [evaluate] *****
[09/04 11:03:39][INFO][ma_cau-runner.py 114]: ***** End Runner *****
```

6. 可选: 模型推理。

模型推理能够指定某一张图片，并且推理出图片的分割区域，并进行可视化。首先需要指定待推理的图片路径，修改“./algorithms/mmocr/config/textrecog/config.py”，具体如下。

```
...
infer_img_file='./data/raw/water_meter_crop/val/train_10.jpg' # 指定需要推理的图片路径
...
```

执行如下命令推理。

```
python manage.py run --cfg algorithms/mmocr/config/textrecog/config.py --pipeline infer
```

图 9-23 模型推理结果

```
[09/04 11:06:27][INFO][ma_cau-runner.py 186]: Command: python algorithms/mmocr/algorithm/tools_adapter/infer.py --config algorithms/mmocr/config/textrecog/robustscanner_r31_academic.py --img ./data/raw/water_meter_crop/val/train_10.jpg --checkpoint ./output/robustscanner_r31_academic/latest.pth --out_file output/robustscanner_r31_academic/vis/vis_train_10.jpg
Use load_from_local_loader
result: {'text': '00326', 'score': 0.9999996185302734}
[09/04 11:06:38][INFO][ma_cau-runner.py 112]: ***** and [infer] *****
[09/04 11:06:38][INFO][ma_cau-runner.py 114]: ***** End Runner *****
```

推理输出的图片路径在“output/robustscanner\_r31\_academic/vis”文件夹下。

图 9-24 表盘读数识别结果图



7. 执行如下命令导出算法SDK。

```
python manage.py export --cfg algorithms/mmocr/config/textrecog/config.py
```

## Step4 部署为在线服务

本次展示仅部署OCR服务，包括本地部署和线上部署，部署上线后调用部署服务进行本地图片的推理，获取水表的预测读数。部署在线服务，需要指定OBS桶以便保存部署所需要的文件。

1. 修改“./algorithms/mmocr/config/textrecog/config.py”文件，配置为用户的OBS桶。

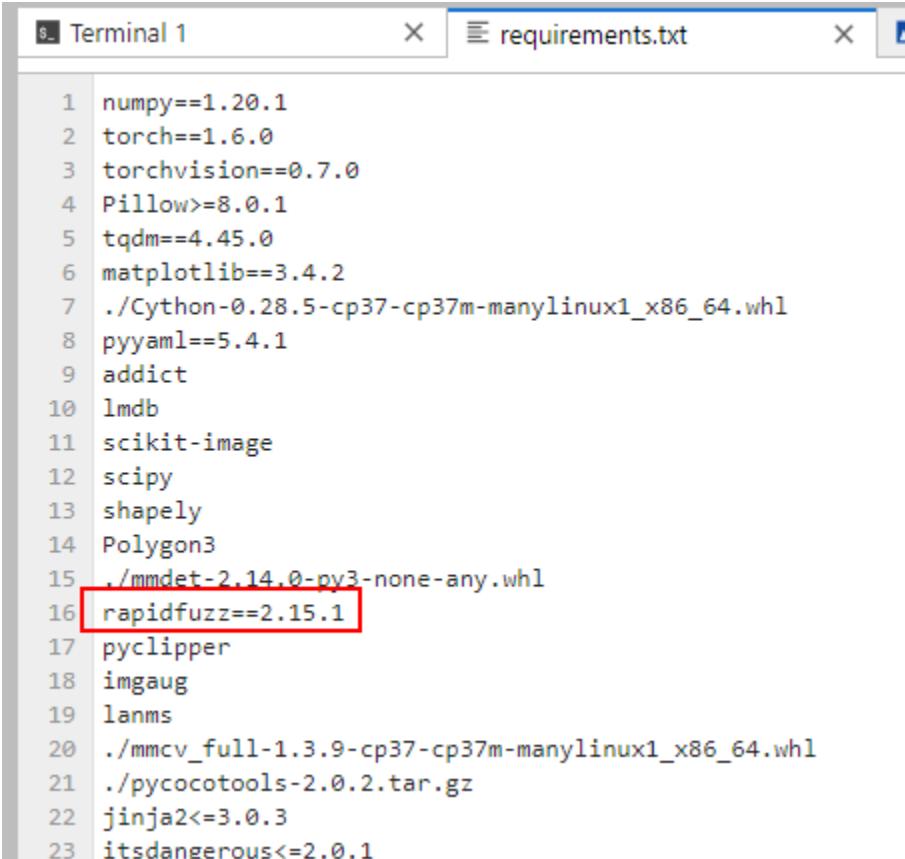
```
替换为用户自己的OBS桶信息
obs_bucket = 'obs://{your_obs_bucket_path}'
```

2. 导出模型文件并修改rapidfuzz版本，然后本地部署。

```
python manage.py export --cfg algorithms/mmocr/config/textrecog/config.py --is_deploy
导出部署模型所需文件
```

修改“./export/robustscanner\_r31\_academic/Linux\_x86\_64\_GPU\_PyTorch\_Common\_py/res/requirements.txt”，将rapidfuzz版本修改为2.15.1

图 9-25 修改 rapidfuzz 版本为 2.15.1



```
Terminal 1 requirements.txt
1 numpy==1.20.1
2 torch==1.6.0
3 torchvision==0.7.0
4 Pillow>=8.0.1
5 tqdm==4.45.0
6 matplotlib==3.4.2
7 ./Cython-0.28.5-cp37-cp37m-manylinux1_x86_64.whl
8 pyyaml==5.4.1
9 addict
10 lmbd
11 scikit-image
12 scipy
13 shapely
14 Polygon3
15 ./mmdet-2.14.0-py3-none-any.whl
16 rapidfuzz==2.15.1
17 pyclicker
18 imgaug
19 lanms
20 ./mmdcv_full-1.3.9-cp37-cp37m-manylinux1_x86_64.whl
21 ./pycocotools-2.0.2.tar.gz
22 jinja2<=3.0.3
23 itsdangerous<=2.0.1
```

```
python manage.py deploy --cfg algorithms/mmdcr/config/textrecog/config.py # 本地部署调试
```

### 本地部署成功后的输出结果

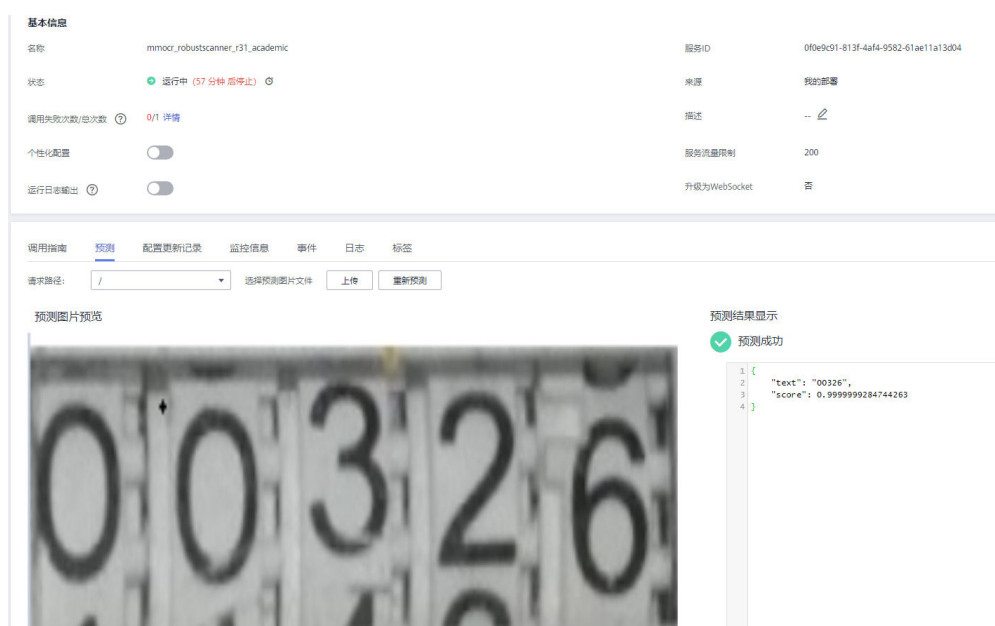
```
#
...
[Conda environment created successfully.]
local_service_port is 127.0.0.1:42153
Deploying the local service ...
Successfully deployed the local service. You can check the log in /home/ma-user/work/water_meter/export/robustscanner_r31_academic/Linux_x86_64_GPU_PyTorch_Common_py/log.txt
[07/05 09:40:14][INFO][ma_cau-deployer.py 49]: {
 "text": "00326",
 "score": 0.9999999046325684
}
[07/05 09:40:14][INFO][ma_cau-deployer.py 59]: ***** End Deployer *****
```

### 3. 本地部署成功后执行如下命令进行在线部署，大约需要十几分钟。

```
python manage.py deploy --cfg algorithms/mmdcr/config/textrecog/config.py --
launch_remote
```

部署成功后，任务会提交至ModelArts控制台的默认工作空间，在“部署上线 > 在线服务”页面会看到此任务。

图 9-26 部署为在线服务



## Step5 清除资源和数据

通过此示例学习完成创建算法套件流程后，如果不再使用，建议您清除相关资源，避免造成资源浪费和不必要的费用。

- 删除Notebook：在ModelArts“开发环境 > Notebook”界面，单击对应实例“操作”列的“更多 > 删除”。
- 删除数据：前往OBS，删除上传的数据，然后删除文件夹及OBS桶。
- 停止在线服务：在ModelArts“部署上线 > 在线服务”界面，单击对应在线服务“操作”列的“更多 > 停止”。

## 9.2 基于 SFS 创建、迁移和管理 Conda 虚拟环境

本文介绍了如何将Notebook的Conda环境迁移到SFS磁盘上。这样重启Notebook实例后，Conda环境不会丢失。

步骤如下：

1. [创建新的虚拟环境并保存到SFS目录](#)
2. [克隆原有的虚拟环境到SFS盘](#)
3. [重新启动镜像激活SFS盘中的虚拟环境](#)
4. [保存并共享虚拟环境](#)

### 前提条件

创建一个Notebook，“资源类型”选择“专属资源池”，“存储配置”选择“SFS弹性文件服务器”，打开terminal。

### 创建新的虚拟环境并保存到 SFS 目录

创建新的conda虚拟环境。

```
shell
conda create --prefix /home/ma-user/work/envs/user_conda/sfs-new-env python=3.7.10 -y
```

查看现有的conda虚拟环境，此时可能出现新创建的虚拟环境的名称为空的情况。

```
shell
conda env list
conda environments:
#
base /home/ma-user/anaconda3
PyTorch-1.8 /home/ma-user/anaconda3/envs/PyTorch-1.8
python-3.7.10 * /home/ma-user/anaconda3/envs/python-3.7.10
 /home/ma-user/work/envs/user_conda/sfs-new-env
```

添加新创建的虚拟环境到conda env。

```
shell
conda config --append envs_dirs /home/ma-user/work/envs/user_conda/
```

查看现有的conda虚拟环境，此时新的虚拟环境已经能够正常显示，可以直接通过名称进行虚拟环境的切换。

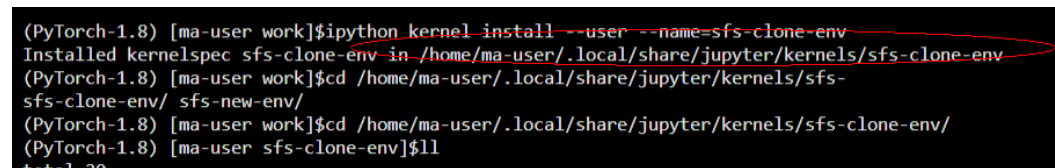
```
shell
conda env list
conda activate sfs-new-env
conda environments:
#
base /home/ma-user/anaconda3
PyTorch-1.8 /home/ma-user/anaconda3/envs/PyTorch-1.8
python-3.7.10 * /home/ma-user/anaconda3/envs/python-3.7.10
sfs-new-env /home/ma-user/work/envs/user_conda/sfs-new-env
```

（可选）将新建的虚拟环境注册到JupyterLab kernel（可以在JupyterLab中直接使用虚拟环境）。

```
shell
pip install ipykernel
ipython kernel install --user --name=sfs-new-env
rm -rf /home/ma-user/.local/share/jupyter/kernels/sfs-new-env/logo-*
```

说明：此处“.local/share/jupyter/kernels/sfs-new-env”为举例，请以用户实际的安装路径为准。

图 9-27 安装路径回显



```
(PyTorch-1.8) [ma-user work]$ipython kernel install --user --name=sfs-clone-env
Installed kernelspec sfs-clone-env in /home/ma-user/.local/share/jupyter/kernels/sfs-clone-env
(PyTorch-1.8) [ma-user work]$cd /home/ma-user/.local/share/jupyter/kernels/sfs-clone-env/
(PyTorch-1.8) [ma-user work]$cd /home/ma-user/.local/share/jupyter/kernels/sfs-clone-env/
(PyTorch-1.8) [ma-user sfs-clone-env]$ll
total 20
```

刷新JupyterLab页面，可以看到新的kernel。

### 📖 说明

重启Notebook后kernel需要重新注册。

## 克隆原有的虚拟环境到 SFS 盘

```
shell
conda create --prefix /home/ma-user/work/envs/user_conda/sfs-clone-env --clone PyTorch-1.8 -y
```

```
Source: /home/ma-user/anaconda3/envs/PyTorch-1.8
Destination: /home/ma-user/work/envs/user_conda/sfs-clone-env
Packages: 20
Files: 39687
Preparing transaction: done
Verifying transaction: done
Executing transaction: done
#
To activate this environment, use
#
$ conda activate /home/ma-user/work/envs/user_conda/sfs-clone-env
#
To deactivate an active environment, use
#
$ conda deactivate
```

查看新创建的clone虚拟环境，如果出现新创建的虚拟环境的名称为空的情况，可以参考[添加新创建到虚拟环境到conda env](#)。

```
shell
conda env list
conda environments:
#
base /home/ma-user/anaconda3
PyTorch-1.8 /home/ma-user/anaconda3/envs/PyTorch-1.8
python-3.7.10 /home/ma-user/anaconda3/envs/python-3.7.10
sfs-clone-env /home/ma-user/work/envs/user_conda/sfs-clone-env
sfs-new-env * /home/ma-user/work/envs/user_conda/sfs-new-env
```

（可选）将新建的虚拟环境注册到JupyterLab kernel（可以在JupyterLab中直接使用虚拟环境）

```
shell
pip install ipykernel
python kernel install --user --name=sfs-clone-env
rm -rf /home/ma-user/.local/share/jupyter/kernels/sfs-clone-env/logo-*
```

说明：此处“.local/share/jupyter/kernels/sfs-clone-env”为举例，请以用户实际的安装路径为准。

刷新JupyterLab页面，可以看到新的kernel。

## 重新启动镜像激活 SFS 盘中的虚拟环境

方法一，直接使用完整conda env路径。

```
shell
conda activate /home/ma-user/work/envs/user_conda/sfs-new-env
```

方法二，先添加虚拟环境到conda env，然后使用名称激活。

```
shell
conda config --append envs_dirs /home/ma-user/work/envs/user_conda/
conda activate sfs-new-env
```

方法三，直接使用完成虚拟环境中的python或者pip。

```
shell
/home/ma-user/work/envs/user_conda/sfs-new-env/bin/pip list
/home/ma-user/work/envs/user_conda/sfs-new-env/bin/python -V
```

## 保存并共享虚拟环境

将要迁移的虚拟环境打包。

```
shell
pip install conda-pack
conda pack -n sfs-clone-env -o sfs-clone-env.tar.gz --ignore-editable-packages
Collecting packages...
Packing environment at '/home/ma-user/work/envs/user_conda/sfs-clone-env' to 'sfs-clone-env.tar.gz'
[#####] | 100% Completed | 3min 33.9s
```

解压到SFS目录。

```
shell

mkdir /home/ma-user/work/envs/user_conda/sfs-tar-env
tar -zxvf sfs-clone-env.tar.gz -C /home/ma-user/work/envs/user_conda/sfs-tar-env
```

查看现有的conda虚拟环境。

```
shell
conda env list
conda environments:
#
base /home/ma-user/anaconda3
PyTorch-1.8 * /home/ma-user/anaconda3/envs/PyTorch-1.8
python-3.7.10 /home/ma-user/anaconda3/envs/python-3.7.10
sfs-clone-env /home/ma-user/work/envs/user_conda/sfs-clone-env
sfs-new-env /home/ma-user/work/envs/user_conda/sfs-new-env
sfs-tar-env /home/ma-user/work/envs/user_conda/sfs-tar-env
test-env /home/ma-user/work/envs/user_conda/test-env
```

## 9.3 本地开发的 MindSpore 模型迁移至云上训练

本案例介绍如何将本地开发好的MindSpore模型代码，通过PyCharm ToolKit连接到ModelArts进行云上调试和训练。

开始使用样例前，请仔细阅读[准备工作](#)罗列的要求，提前完成准备工作。本案例的步骤如下所示：

**步骤1：安装和登录PyCharm ToolKit**

**步骤2：使用PyCharm进行本地开发调试**

**步骤3：使用ModelArts Notebook进行开发调试**

**步骤4：使用PyCharm提交训练作业至ModelArts**

**步骤5：清除相应资源**

### 准备工作

- 本地已安装PyCharm 2019.2或以上版本，推荐Windows版本，社区版或专业版均可，请单击[PyCharm工具下载地址](#)获取工具并在本地完成安装。
  - 使用PyCharm ToolKit远程连接Notebook开发环境，仅限PyCharm专业版。
  - 使用PyCharm ToolKit提交训练作业，社区版和专业版都支持。
- 已注册华为账号并开通华为云，且在使用ModelArts前检查账号状态，账号不能处于欠费或冻结状态。
- 已创建当前使用账号的访问密钥，并获得对应的AK和SK。如果未创建，请参见[创建访问密钥（AK和SK）](#)。



- 当前账号已完成访问授权的配置。如未完成，请参考[使用委托授权](#)。

## 环境说明

- Python 3.7.6
- PyCharm 2023.1.3 (Professional Edition)

### 📖 说明

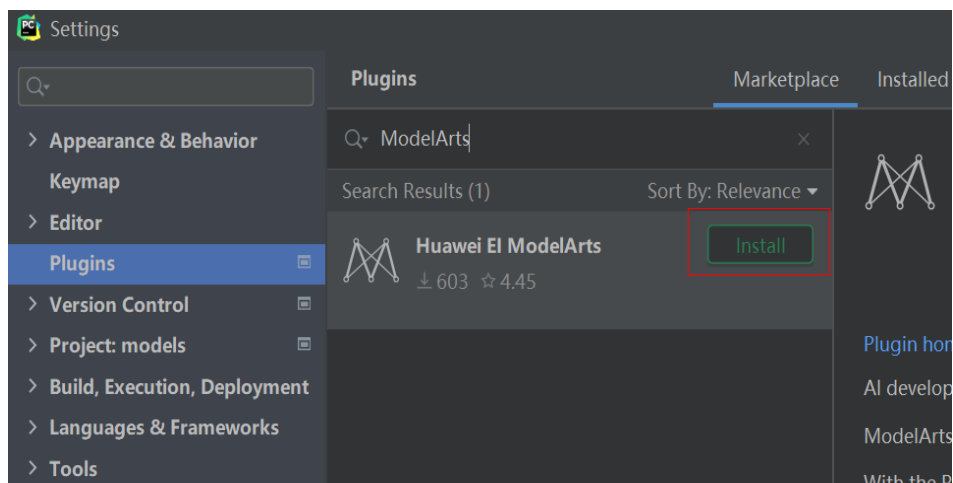
本案例使用PyCharm版本为PyCharm 2023.1.3 (Professional Edition)，不同版本PyCharm之间部分界面可能不同，仅供参考。

## 步骤 1：安装和登录 PyCharm ToolKit

### 1. 安装PyCharm ToolKit

在PyCharm中选择“File>Settings>Plugins”，在Marketplace里搜索“ModelArts”，单击“Install”即可完成安装。

图 9-28 通过 Marketplace 安装



### 2. 登录PyCharm ToolKit

#### a. 打开“Edit Credential”界面。

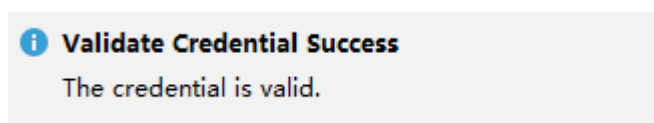
安装完插件后，会在IDE菜单栏出现“ModelArts”，单击后选择“Edit Credential”。

#### b. 验证登录信息

将创建访问密钥（AK和SK）输入到ToolKit对应位置，单击OK按钮进行登录，出现下图提示即为登录成功。

如果未创建，请参见[创建访问密钥（AK和SK）](#)

图 9-29 成功登录提示



## 步骤 2：使用 PyCharm 进行本地开发调试

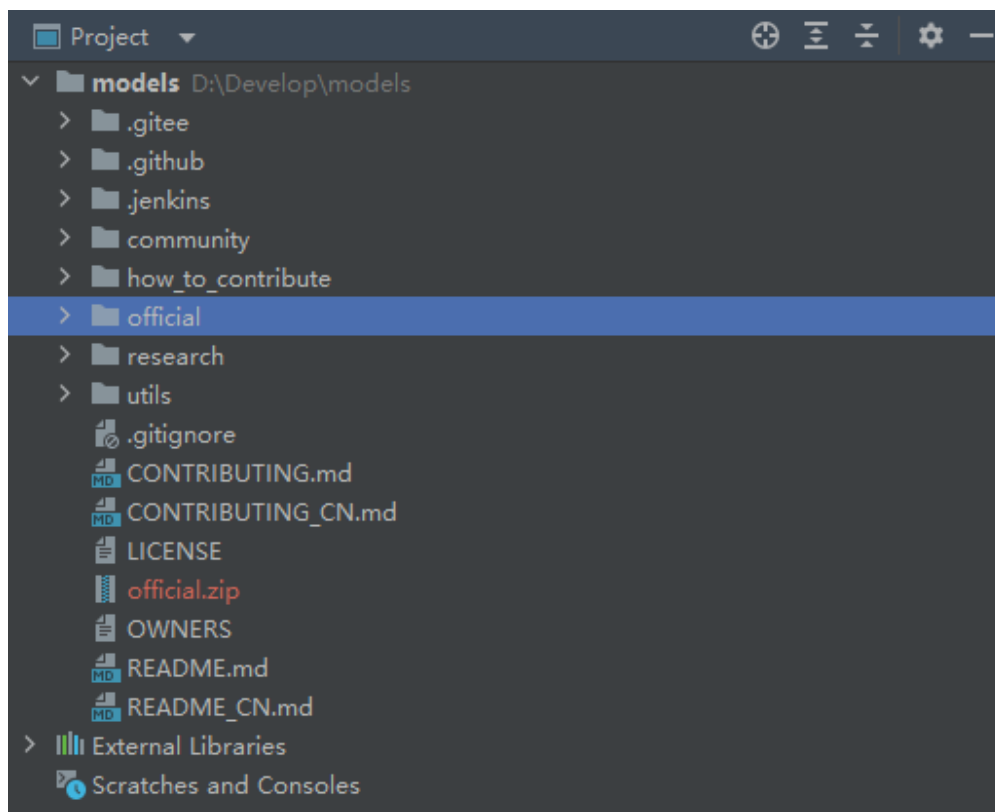
### 1. 下载代码至本地

本案例中，以图像分类模型resnet50模型为例，路径为“./models/official/cv/resnet/”

# 在本地电脑Terminal下载代码至本地

```
git clone https://gitee.com/mindspore/models.git -b v1.5.0
```

图 9-30 下载代码至本地



### 2. 配置本地PC开发环境

修改“models/official/cv/resnet/requirements.txt”文件，改为：

```
numpy==1.17.5
```

```
scipy==1.5.4
```

```
easydict==1.9
```

执行pip命令安装：

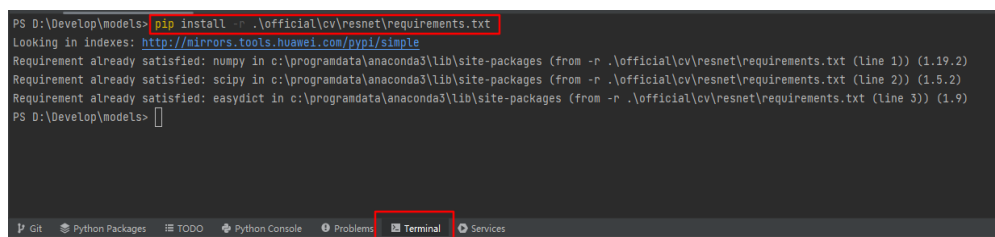
# 在PyCharm的Terminal安装mindspore

```
pip install mindspore==1.7.0 --trusted-host https://repo.huaweicloud.com -i https://repo.huaweicloud.com/repository/pypi/simple
```

# 在PyCharm的Terminal安装resnet依赖

```
pip install -r .\official\cv\resnet\requirements.txt --trusted-host https://repo.huaweicloud.com -i https://repo.huaweicloud.com/repository/pypi/simple
```

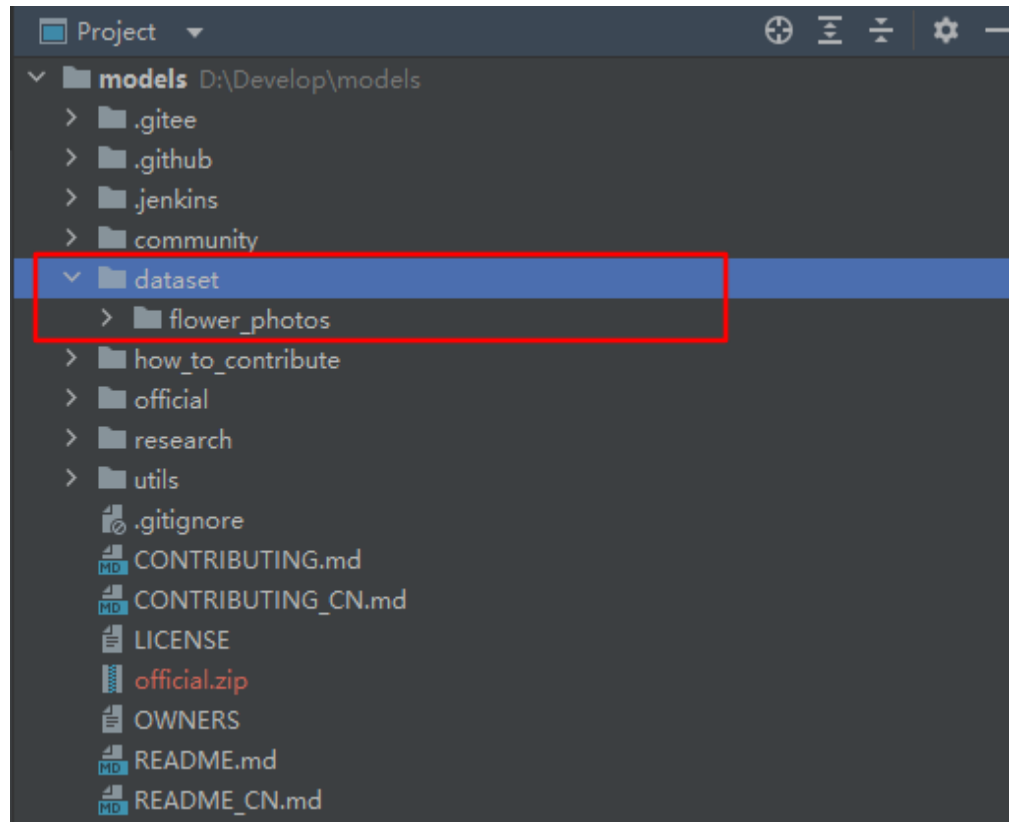
图 9-31 安装 resnet 依赖



### 3. 准备数据集

本样例使用的数据集为类别数为五类的花卉识别数据集，[下载数据集](#)并解压数据到工程目录。新建dataset文件夹，将解压后数据集保存在dataset文件夹下。

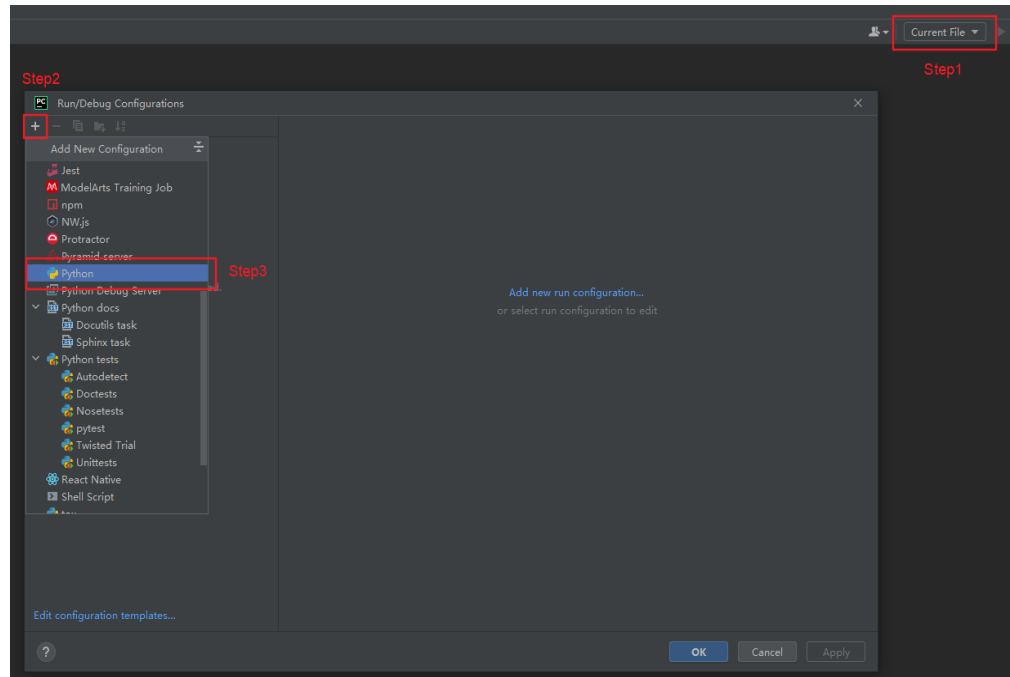
图 9-32 准备数据集



### 4. 配置PyCharm解释器和入参

单击右上角“Current File”，选择“Edit Configuration”，打开“Run/Debug Configuration”对话框。在对话框中单击“+”，选择“Python”。

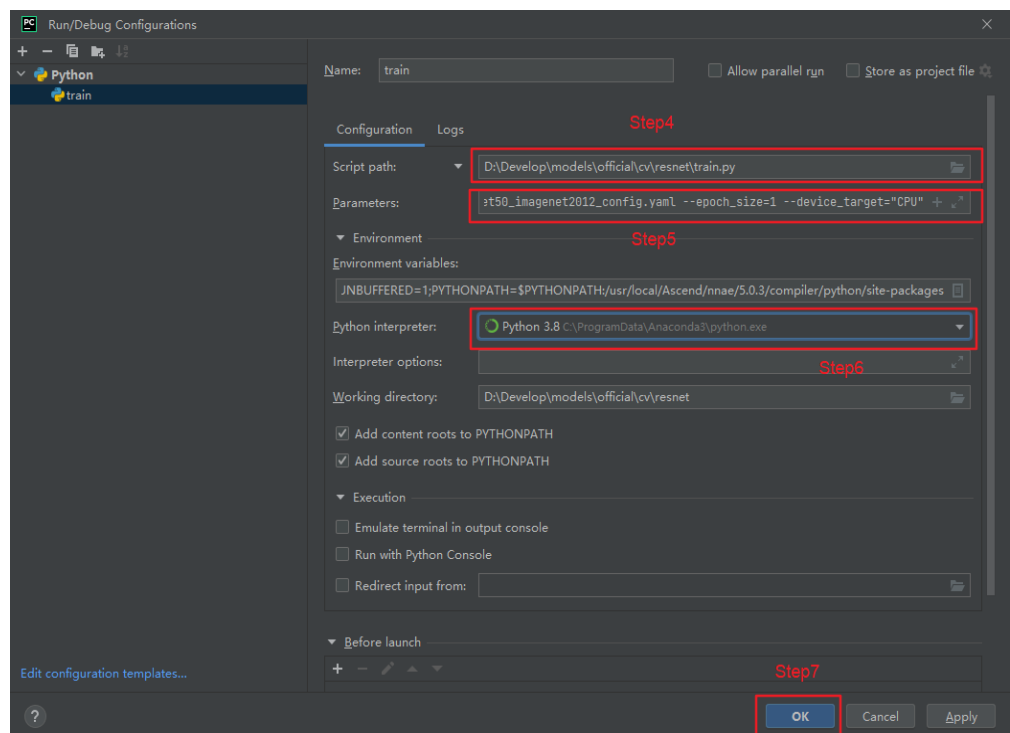
图 9-33 前往 PyCharm 解释器



“Script path”选择train.py文件，“Parameters”命令如下所示，并选择Python解释器，然后单击“OK”：

```
--net_name=resnet50 --dataset=imagenet2012 --data_path=../../dataset/flower_photos/ --
class_num=5 --config_path=./config/resnet50_imagenet2012_config.yaml --epoch_size=1 --
device_target="CPU"
```

图 9-34 配置 PyCharm 解释器



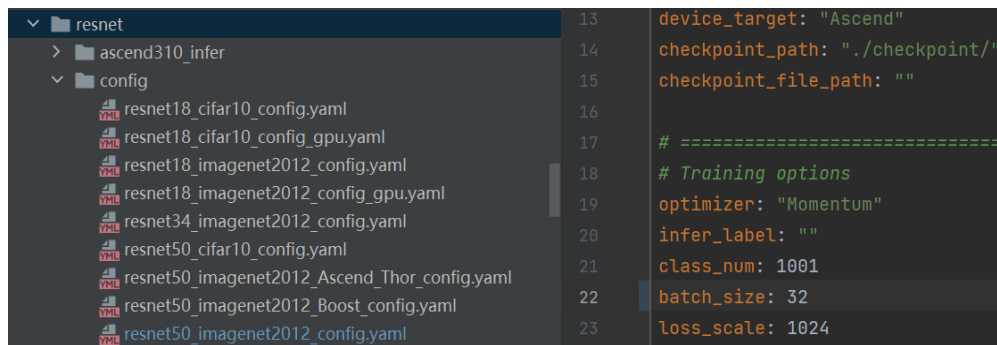
### 📖 说明

根据README说明文档，配置Parameter参数device\_target="CPU"表示CPU环境运行，device\_target="Ascend"表示在Ascend环境运行。

#### 5. 本地代码开发调测

一般本地CPU算力较低并且内存较小，可能出现内存溢出的报错，因此可以把“models/official/cv/resnet/config/resnet50\_imagenet2012\_config.yaml”的“batch\_size”由“256”改为“32”，使得训练作业可以快速运行。

图 9-35 修改 batch\_size



AI开发过程中的数据集开发及模型开发是和硬件规格无关的，而且这一部分的开发耗时是最长的，因此可以先在本地PC的CPU环境进行数据集和模型开发调试。

### 📖 说明

本例中，因为样例代码已经支持在CPU上进行训练，因此用户能够在CPU上完成整个训练流程。如果代码只支持在GPU或者Ascend上训练，那么可能会报错，需要使用Notebook进行云端调试。

设置断点后单击“调试”，可实现代码逐步调试，查看中间变量值。

图 9-36 “调试”按钮

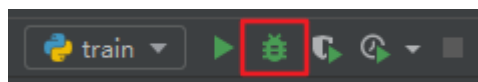
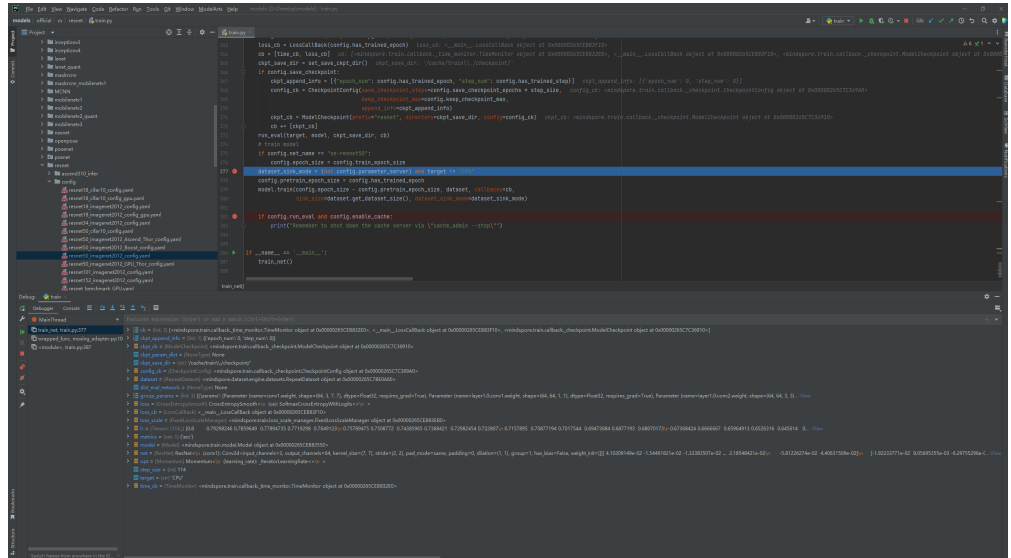


图 9-37 通过设置断点实现代码调试



可单击“运行”按钮，通过日志观察是否能正常训练。

图 9-38 “运行”按钮

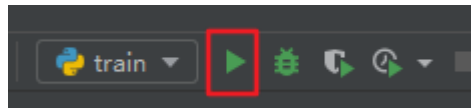
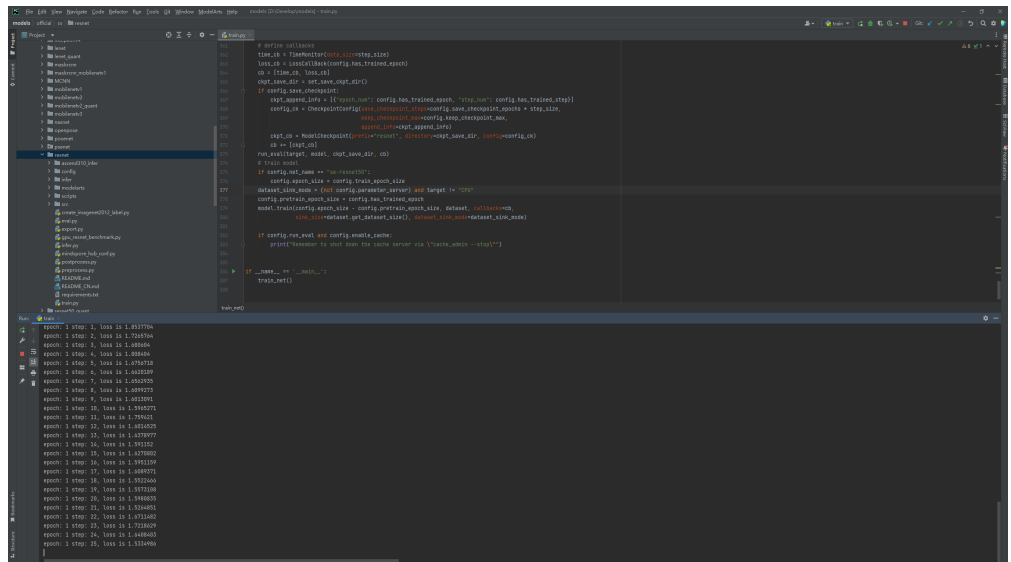


图 9-39 训练日志



### 步骤 3: 使用 ModelArts Notebook 进行开发调试

使用 ModelArts Notebook 进行开发调试具有如下优势:

- 环境保持一致
- 配置一键完成

- 代码远程Debug
- 资源按需使用

**说明**

只有PyCharm专业版支持本章节，社区版可以直接跳转至[步骤4: 使用PyCharm提交训练作业至ModelArts](#)完成创建训练作业。

1. 连接Notebook开发环境

- a. 创建或打开云端Ascend规格的Notebook。创建Notebook详细操作请参见[创建Notebook实例](#)，Notebook规格相关信息如下所示：

“镜像”：tensorflow1.15-mindspore1.7.0-cann5.1.0-euler2.8-aarch64。

“资源选择”：公共资源池。

“类型”：ASCEND。

“规格”：选Ascend类型的，以界面实际可选值为准。

“存储配置”：EVS存储。

“SSH远程开发”：开启。

“密钥对”：选择已有密钥对，或单击密钥对右侧的“立即创建”创建密钥对。

2. 通过ToolKit连接云端Notebook

- a. 在IDE菜单栏中选择“ModelArts>Notebook>Remote Config”，在打开的界面中选择要连接的Notebook实例。

**说明**

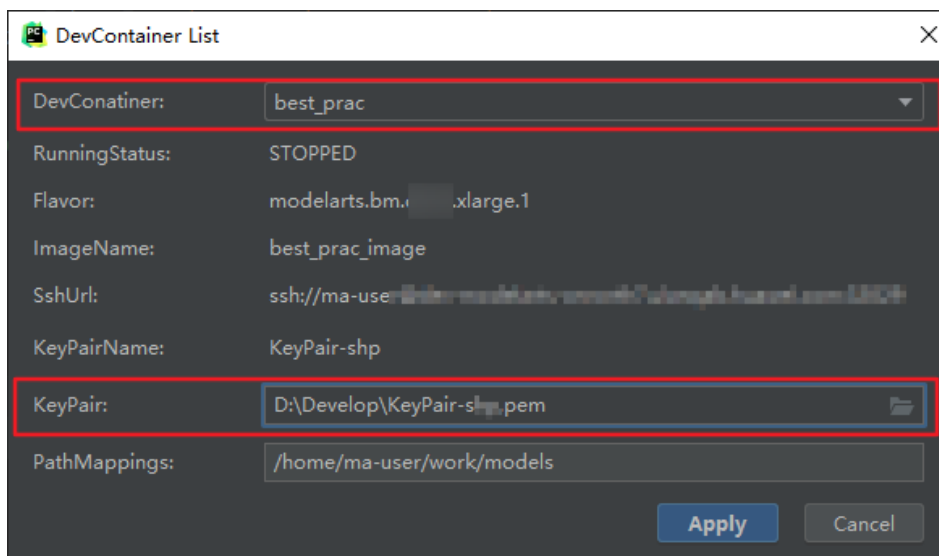
此处如果看不到Connect to Remote选项，请先参考[创建Notebook实例](#)章节，创建Notebook实例，并开启该实例的SSH远程开发功能。

也可能是PyCharm ToolKit的版本不正确，请按照文档要求下载新版本的PyCharm ToolKit。

下载前请先清除浏览器缓存，如果之前下载过老版本的PyCharm ToolKit，浏览器会有缓存，可能会导致新版本下载失败。

- b. 在KeyPair中选择该Notebook实例对应的密钥，选择完成后，单击Apply进行远程Notebook一键配置，等待一段时间后，会出现重启IDE的确认框，单击确认重启，重启后即可生效。

图 9-40 Toolkit 连接 Notebook 配置界面



**说明**

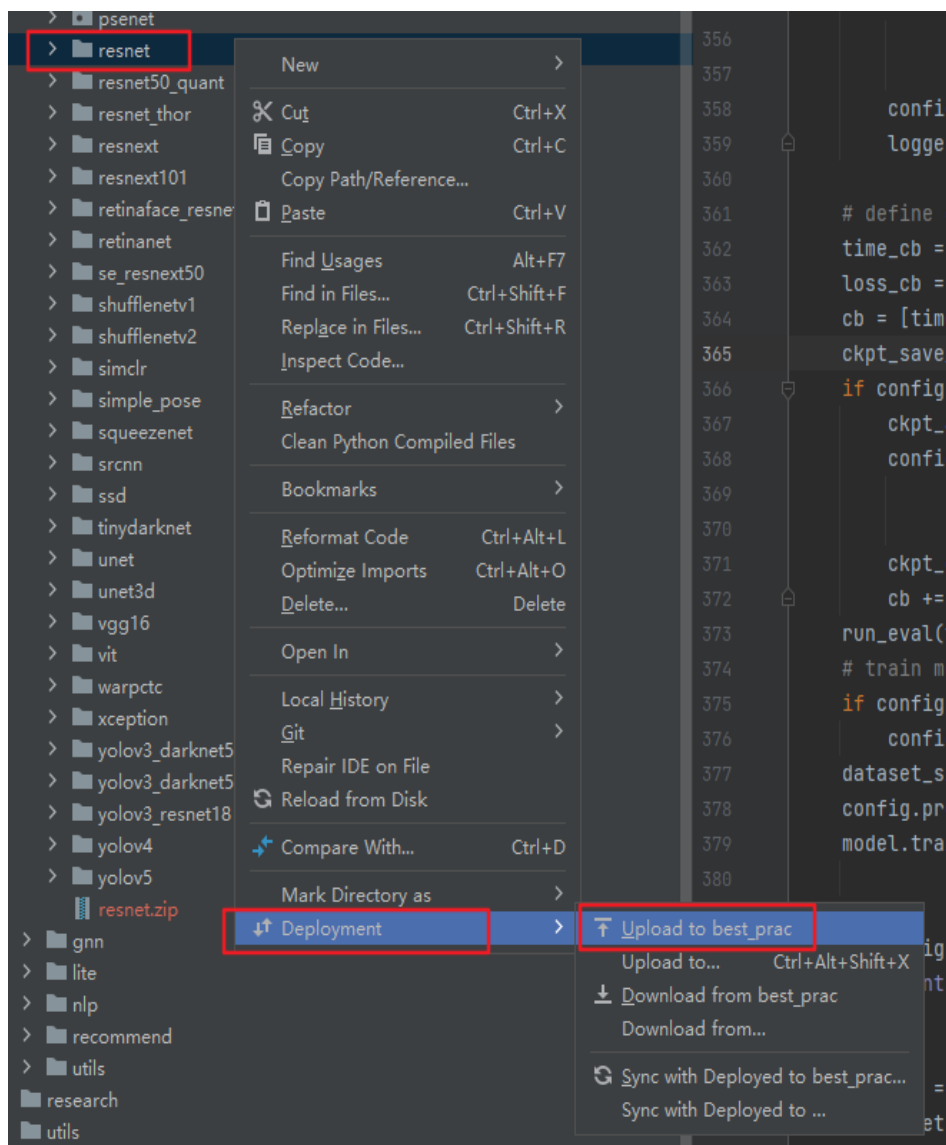
- KeyPair: 需要选择保存在本地的Notebook对应的keypair认证。即创建Notebook时创建的密钥对文件，创建时会直接保存到浏览器默认的下载文件夹中。
- PathMappings: 该参数为本地IDE项目和Notebook对应的同步目录，默认为“/home/ma-user/work/project”，可根据自己实际情况更改。

3. 同步代码和数据至云端Notebook

a. 将代码同步至Notebook

选择resnet文件夹，右键选择“Deployment>Upload to”上传代码至Notebook。

图 9-41 同步代码至 Notebook

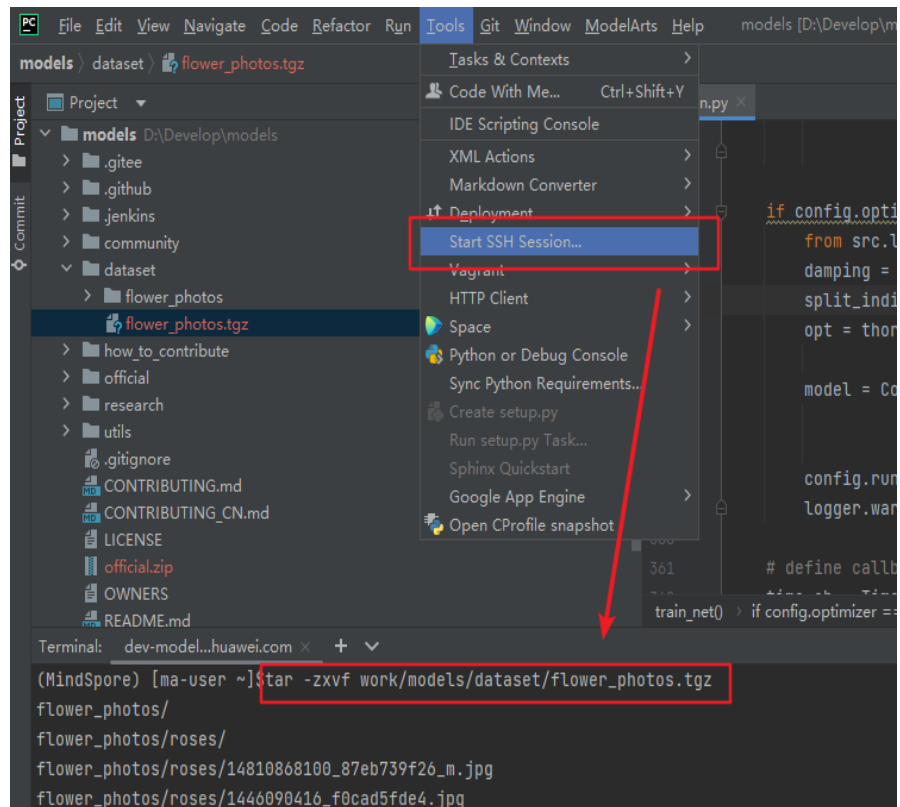


b. 将数据同步至Notebook

- (推荐) 方法1: 数据集压缩包上传至Notebook后解压  
把数据集压缩包右键选择“Deployment>Upload to”的方式上传至Notebook后，在Notebook中对数据集进行解压操作，解压命令如下：  
tar -zxvf work/models/dataset/flower\_photos.tgz



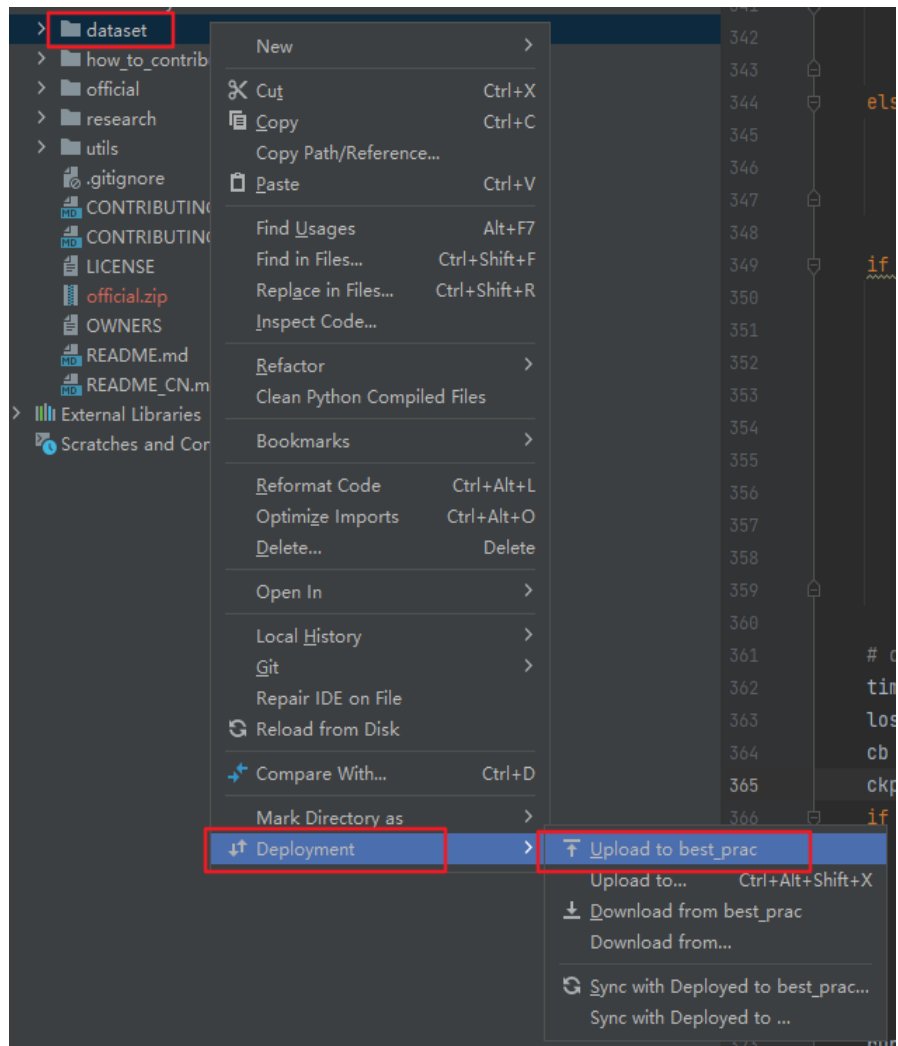
图 9-42 数据集压缩包上传至 Notebook 后解压



- 方法2: 文件夹直接上传至Notebook

类似上传代码至Notebook，直接上传数据文件夹。（由于本案例数据集中图片数量较多，通过IDE进行上传比较耗时，推荐使用方法1进行上传）

图 9-43 文件夹直接上传至 Notebook



**注意**

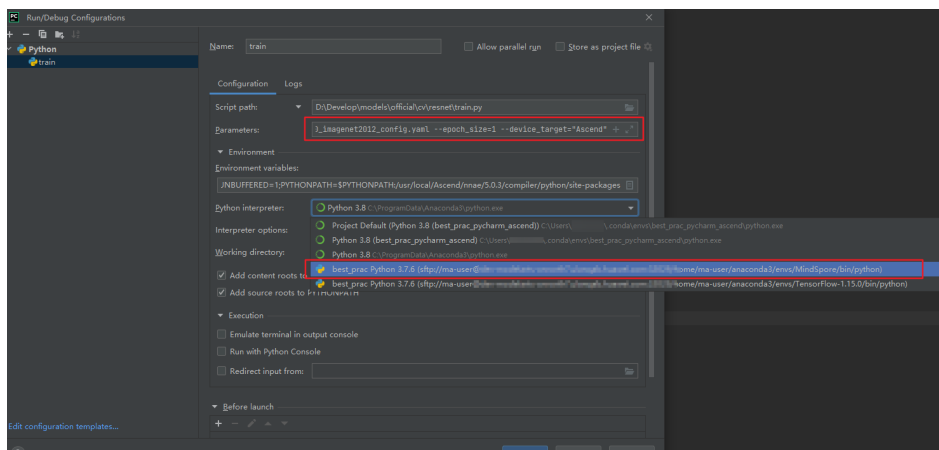
- 当数据集比较大达到数GB时，建议先将数据集先上传至OBS再通过OBS上传至 Notebook，PyCharm只适合做小文件的同步上传。
- 调试时建议使用较小的数据集子集，方便数据同步与数据加载。

4. 配置云端Python解释器

修改Parameters参数，并选择云端Python解释器。

```
--net_name=resnet50 --dataset=imagenet2012 --data_path=../../dataset/flower_photos/ --
class_num=5 --config_path=./config/resnet50_imagenet2012_config.yaml --epoch_size=1 --
device_target="Ascend"
```

图 9-44 配置云端 python 解释器

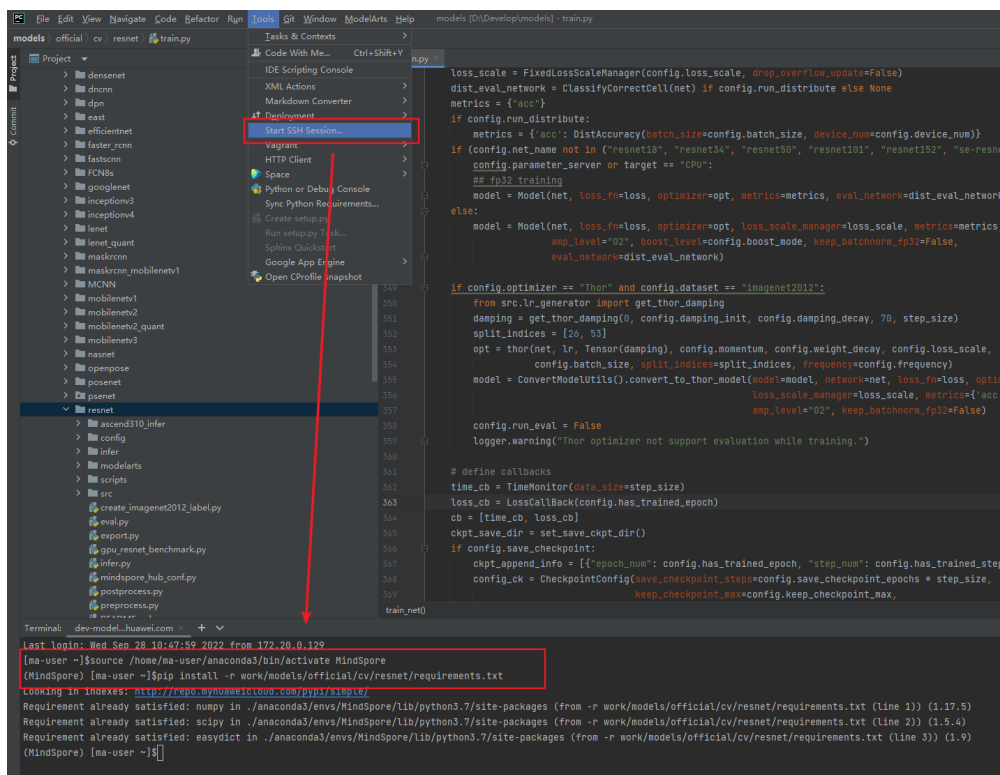


5. 云端Notebook安装依赖

打开“Tool>Start SSH Section”，安装依赖软件。

```
进入MindSpore环境
source /home/ma-user/anaconda3/bin/activate MindSpore
安装resnet依赖
pip install -r work/models/official/cv/resnet/requirements.txt
```

图 9-45 云端 Notebook 安装依赖



6. 云端调试与运行

配置完云端的解释器后，PyCharm可以直接使用远端Notebook中的python解释器和硬件规格，满足用户在本本地体验到真实的硬件环境并进行全流程的调试和验证。

**注意**

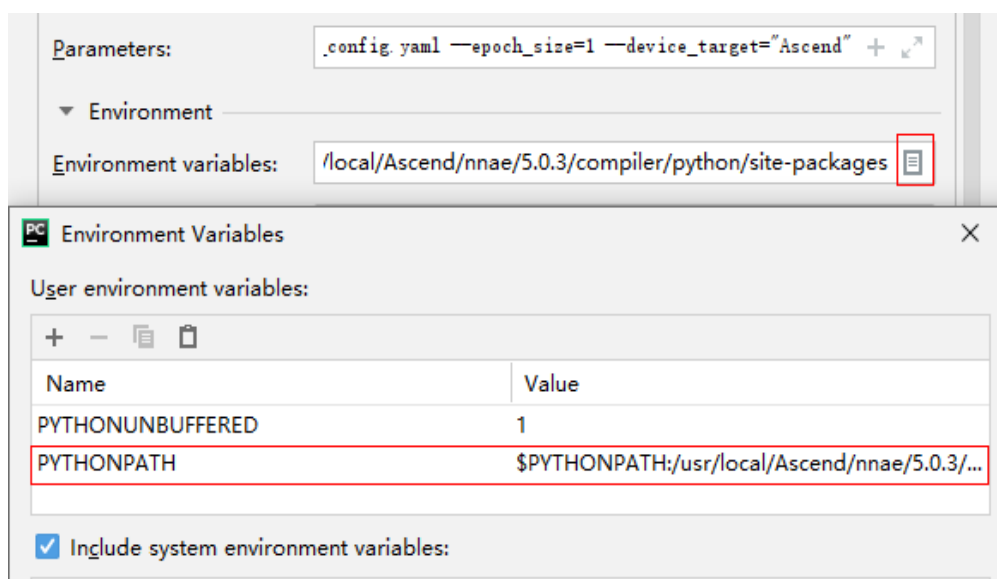
基于Ascend的样例中，可能会抛出异常。

```
ModuleNotFoundError: No module named 'te'
```

原因是：PyCharm的PYTHONPATH会将Notebook中的环境变量中指定的“PYTHONPATH”进行覆盖，因此，还需要将te包所在的路径添加到PyCharm的“PYTHONPATH”中。

te包的路径通过“pip show te”查看，例如te包返回对应的路径为：“/usr/local/Ascend/nnae/5.0.3/compiler/python/site-package”，则“PYTHONPATH”对应的“Value”为“\$PYTHONPATH:/usr/local/Ascend/nnae/5.0.3/compiler/python/site-package”

图 9-46 将 te 包所在的路径添加到 PyCharm 的 PYTHONPATH 中



7. 保存开发环境镜像

成功完成Notebook调测后，此时的Notebook已经包含了模型训练所有的依赖环境，因此可以将已经调测完成的开发环境保存成一个镜像，选择“Notebook>更多>保存镜像”。此时Notebook会冻结，需要等待几分钟（只需要保存一次）。保存后的镜像可以在“ModelArts>镜像管理”中进行查看，对应完整的镜像名称为“详情->SWR地址”。

图 9-47 查看保存后的镜像



**说明**

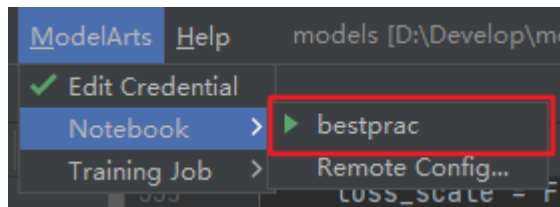
Notebook在代码调试完成及保存镜像后就可以关闭了，减少资源浪费。

8. 连接、停止、启动和断开Notebook实例

- 连接Notebook实例

当Notebook实例为绿色三角形状态时，表示该实例运行中（但未与PyCharm连接）。此时单击该实例名称，实例会变为绿色勾状态，表示PyCharm已与实例连接成功。

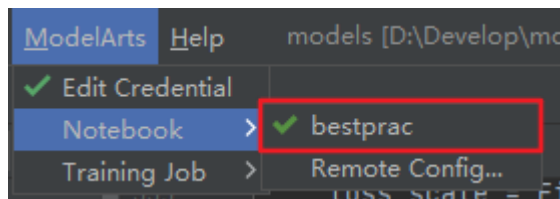
图 9-48 实例运行中状态



- 停止Notebook实例

当Notebook实例为绿色勾状态时，表示该实例运行中且与PyCharm连接成功。此时单击该实例名称，实例会变为黄色感叹号状态，表示停止Notebook实例。

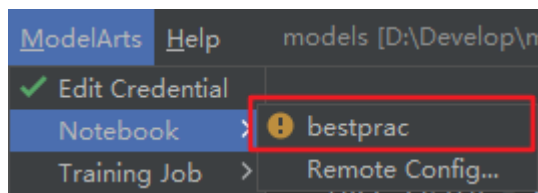
图 9-49 实例运行中且与 PyCharm 连接成功状态



- 启动Notebook实例

当Notebook实例为黄色感叹号状态时，表示该实例已停止。此时单击该实例名称，实例会变为绿色勾状态，表示启动Notebook实例且与PyCharm连接成功。（默认启动时间为4小时）

图 9-50 实例已停止状态



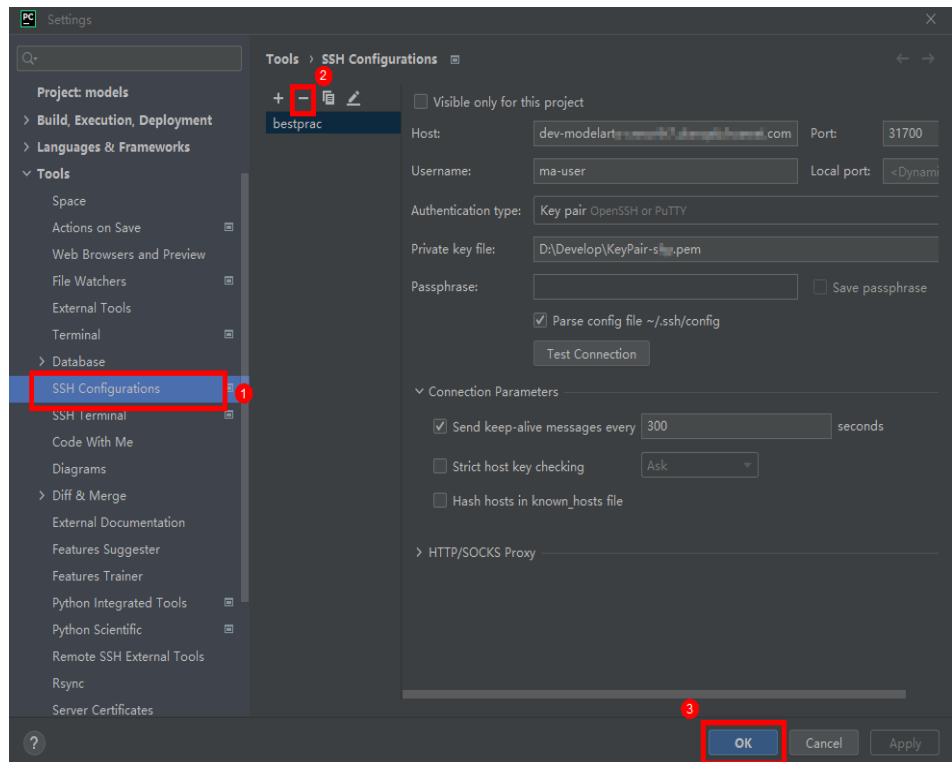
- 断开PyCharm ToolKit中的Notebook实例SSH连接

选择“File>Settings>Tool>SSH Configurations”，单击需要断开的实例，选择“-”，单击“OK”，则IDE菜单栏“ModelArts>Notebook”中的Notebook实例连接断开。

**注意**

该步骤会使Notebook实例不在PyCharm ToolKit中呈现，但Notebook实例仍然存在于控制台。如果想删除Notebook实例以释放资源，请登录ModelArts管理控制台，在Notebook管理页面进行删除。

图 9-51 断开 PyCharm ToolKit 中的 Notebook 实例 SSH 连接



#### 步骤 4：使用 PyCharm 提交训练作业至 ModelArts

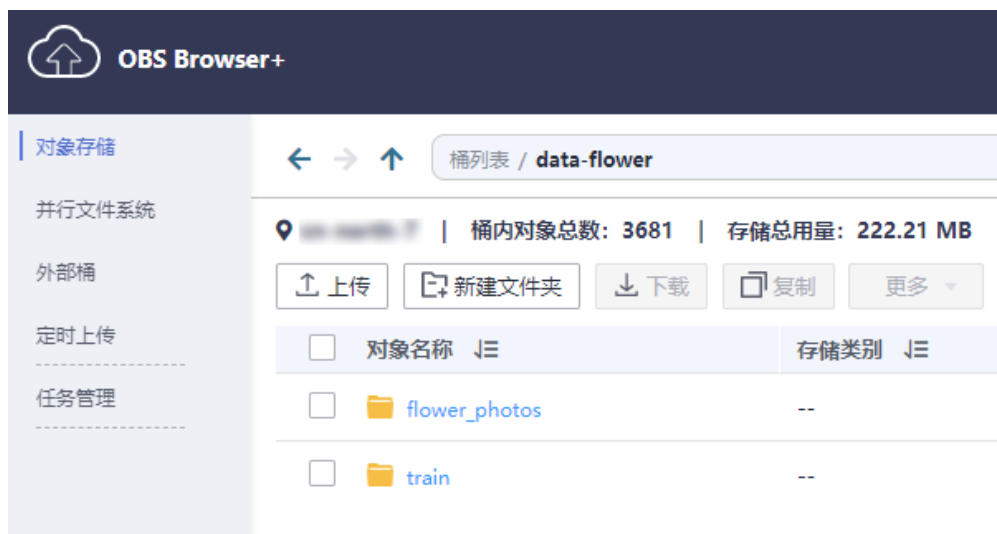
ModelArts训练平台提供了海量的算力规格和训练优化，支持将本地调试好的代码以及之前保存的开发环境镜像直接在PyCharm中提交训练作业。

##### 1. 创建OBS桶并上传数据

由于训练作业是在ModelArts端运行，因此需要把训练数据和训练代码上传至云端 Notebook。可借助OBS Browser+把下载好的训练数据上传至OBS，具体安装步骤请见[安装OBS Browser+](#)。

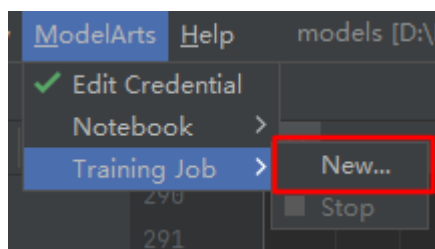
新建data-flower桶，把训练数据flower\_photos文件夹通过OBS Browser+上传至对应的OBS，并新建train文件夹用来存放训练作业相关数据。

图 9-52 上传数据至 OBS



2. 创建训练作业  
在IDE菜单栏选择“ModelArts>Training Job>New...”创建训练作业。

图 9-53 创建训练作业



创建训练作业界面各参数名称及含义如下表所示。

表 9-1 参数名称及含义

| 参数名称                 | 含义                                                               |
|----------------------|------------------------------------------------------------------|
| JobName              | 训练作业的名称，默认为当前的时间。                                                |
| AI Engine            | 训练引擎，这里选择“mindspore_1.7.0-cann_5.1.0-py_3.7-euler_2.8.3-aarch64” |
| Boot File Path       | 本地训练启动代码。                                                        |
| Code Directory       | 本地代码目录                                                           |
| Image Path(optional) | 可选项，输入自定义镜像swr路径地址（使用的自定义镜像和预置的训练镜像引擎一致）                         |
| Data OBS Path        | OBS上的数据集路径（需要提前把数据上传到OBS中）                                       |
| Training OBS Path    | OBS路径（该路径必须是存在的），用于保存代码和训练模型及日志的输出                               |

| 参数名称               | 含义                             |
|--------------------|--------------------------------|
| Running Parameters | 训练脚本接收的参数。                     |
| Specifications     | 计算规格，这里选择Ascend类型的，以界面实际可选值为准。 |
| Compute Node       | 节点数（单机训练默认为1）                  |

PyCharm中支持两种方式创建训练作业：使用预置镜像训练作业、自定义镜像创建训练作业。

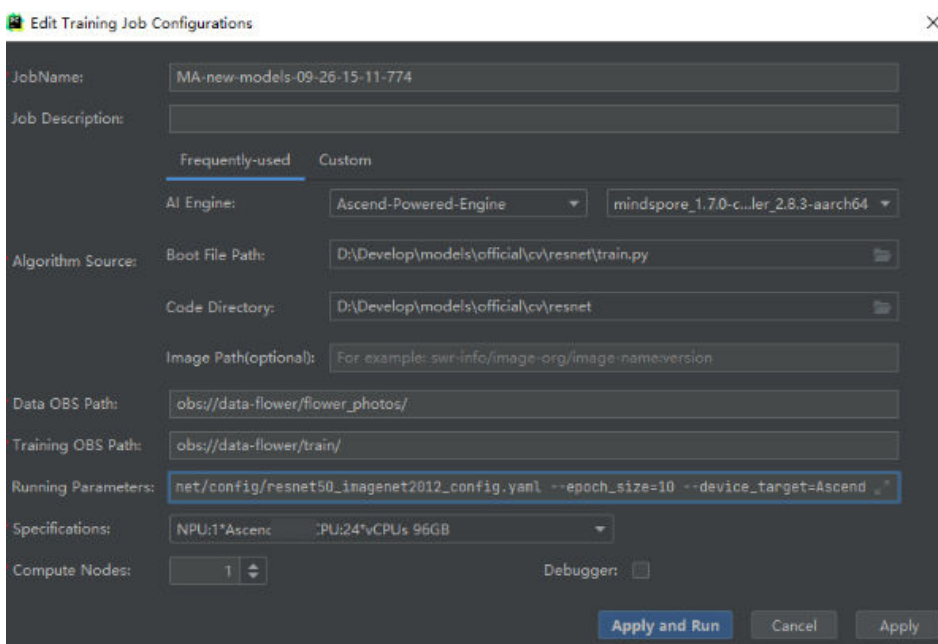
– 使用预置镜像创建训练作业

在RunningParameters中填入如下训练参数，其余参数按实际路径填写。

```
--net_name=resnet50 --dataset=imagenet2012 --enable_modelarts=True --class_num=5 --
config_path=/home/ma-user/modelarts/user-job-dir/resnet/config/
resnet50_imagenet2012_config.yaml --epoch_size=10 --device_target=Ascend
```

填写完训练作业参数后，单击“Apply and Run”即完成训练作业创建。

图 9-54 使用预置镜像创建训练作业



– 使用自定义镜像创建训练作业

使用自定义镜像创建训练作业和使用预置镜像创建训练作业的差别，在于Image Path处填入了自定义镜像的地址。填写完训练作业参数后，单击“Apply and Run”即完成训练作业创建。

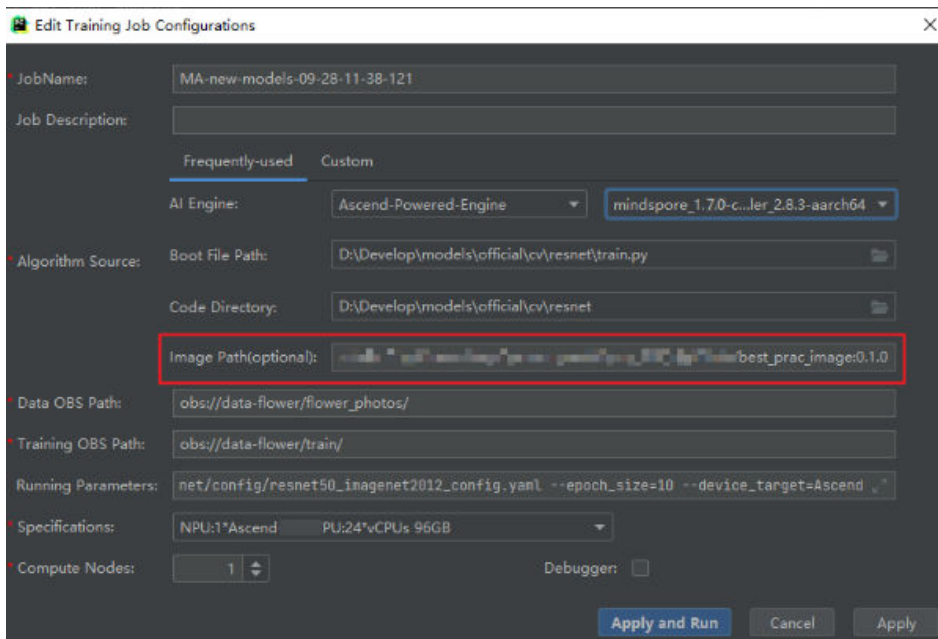
**说明**

在选择AI Engine预置镜像时，需要和自定义镜像保持一致，该设置的作用为通过预置镜像的启动命令启动自定义镜像。

例如自定义镜像中用到Mindspore，则预置镜像中可选择包含Mindspore的镜像。



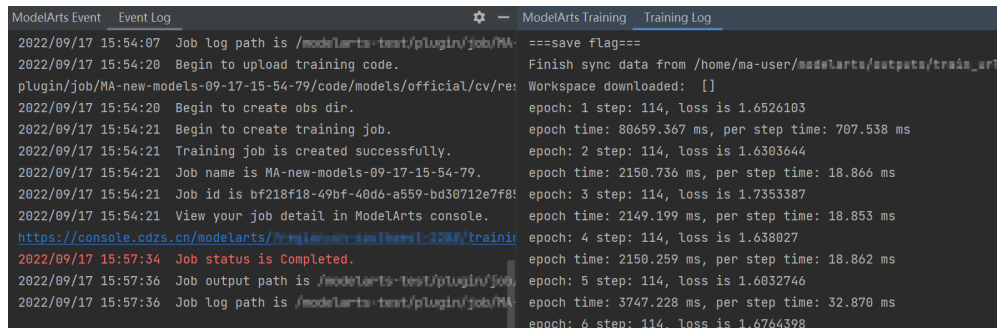
图 9-55 使用自定义镜像创建训练作业



3. 查看训练日志

在单击“Apply and Run”按钮后，训练的日志可以在PyCharm窗口中实时展示。也可以单击Event Log中的控制台链接，转调到网页端中查看训练日志。

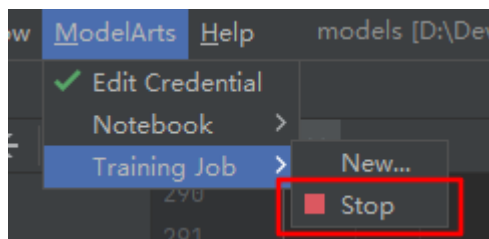
图 9-56 在 PyCharm 中查看训练日志



4. 终止训练作业

如果想要在中途终止训练，可以在PyCharm中单击“ModelArts>Training Job>Stop”，或者直接在网页端单击终止。

图 9-57 终止训练作业



## 步骤 5：清除相应资源

为避免产生不必要的费用，在完成试用后，建议您删除相关资源，如在线服务、训练作业及其OBS目录。

- 停止Notebook：在“Notebook”页面，单击对应实例操作列的“停止”。
- 在PyCharm菜单栏中，选择“ModelArts > Stop Training Job”停止此训练作业。
- 进入OBS管理控制台，删除创建的OBS桶。先逐个删除桶内文件夹和文件，再执行删除桶的操作。

## 9.4 使用 ModelArts VS Code 插件进行模型开发 (Ascend)

### 9.4.1 方案概述

#### 应用场景

Notebook等线上开发工具工程化开发体验不如IDE，但是本地开发服务器等资源有限，运行和调试环境大多使用团队公共搭建的CPU或GPU服务器，并且是多人共用，这带来一定环境搭建和维护成本。因此使用本地IDE+远程Notebook结合的方式，可以同时享受IDE工程化开发和云上资源的即开即用，优势互补，满足开发者需求。

VS Code在Python项目开发中提供了优秀的代码编辑、调试、远程连接和同步能力，在开发者中广受欢迎。本文以Ascend Model Zoo为例，介绍如何通过VS Code插件及ModelArts Notebook进行云端数据调试及模型开发。

#### 方案优势

云端开发调试优势：

- 环境保持一致
- 配置一键完成
- 代码远程调试
- 资源按需使用

### 9.4.2 资源规划

表 9-2 资源和成本规划内容说明

| 资源               | 资源说明                                            | 成本规划              |
|------------------|-------------------------------------------------|-------------------|
| Snt9(32GB显存)单卡规格 | 此处的规格为举例，选择ASCEND类型的资源规格即可。                     | 按需计费，19.5元/小时     |
| EVS存储            | 磁盘规格默认为5GB，从Notebook实例创建成功起，直至删除成功，每GB按照规定费用收费。 | 按需计费，0.007元/小时/GB |

**须知**

本文提供的成本预估费用仅供参考，资源的实际费用以华为云管理控制台显示为准。

**表 9-3 环境准备说明**

| 维度                                                       | 说明                                                                                                                                                                                                                                                                                                                                                                                                                          |
|----------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 下载VS Code IDE，下载路径： <a href="#">开源Visual Studio Code</a> | 根据不同的操作系统选择不同的安装包。                                                                                                                                                                                                                                                                                                                                                                                                          |
| 创建Notebook并打开Terminal                                    | <ol style="list-style-type: none"> <li>1. <a href="#">登录ModelArts控制台</a>，单击左侧导航“开发环境 &gt; Notebook”，然后单击“创建”。镜像选择“mindspore1.7.0-cann5.1.0-py3.7-euler2.8.3”，类型选择“ASCEND”，并打开“SSH远程开发”开关，密钥对选择已有的或单击“立即创建”。</li> <li>2. Notebook创建后，“状态”为“运行中”。单击“操作”列的“打开”，进入JupyterLab，然后参考下图打开Terminal。</li> </ol> <p><b>图 9-58 打开 Terminal</b></p>  |

表 9-4 数据和代码下载说明

| 维度               | 说明                                                                                                                                                                                                                                                                                                        |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>下载项目代码</p>    | <p>在Terminal执行如下命令下载项目代码。本例中，以图像分类模型resnet50模型为例。下载后的文件如图9-59所示，代码所在路径为“./models/official/cv/resnet/”。</p> <pre># 下载代码 git clone https://gitee.com/mindspore/models.git -b v1.5.0</pre> <p><b>图 9-59 下载后的模型包文件</b></p>  |
| <p>下载花卉识别数据集</p> | <p>本样例使用的数据集为类别数为五类的花卉识别数据集。</p> <p>在Terminal里执行如下命令下载并解压数据集，将数据集保存在“./models/dataset/flower_photos”文件夹。</p> <pre>cd models mkdir dataset cd dataset wget http://download.tensorflow.org/example_images/flower_photos.tgz tar xzvf flower_photos.tgz</pre>                                                |

### 9.4.3 操作步骤

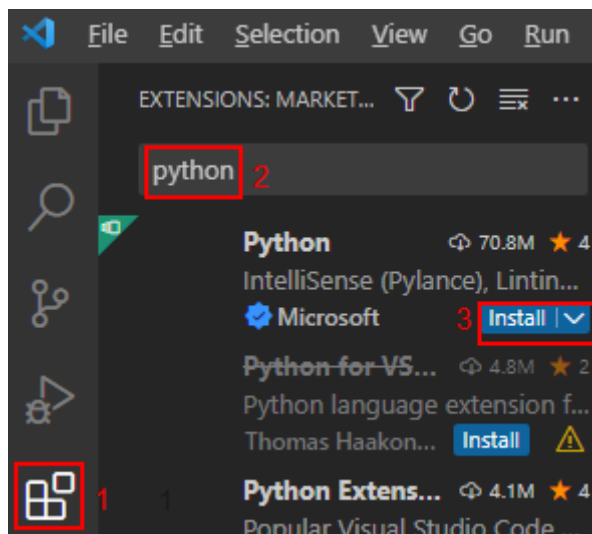
#### 步骤 1: 通过 VS Code 插件连接云端 Notebook

通过VS Code插件连接云端Notebook，详细操作请参考[VS Code—一键连接 Notebook](#)。

#### 步骤 2: 安装 Python 插件以及配置入参

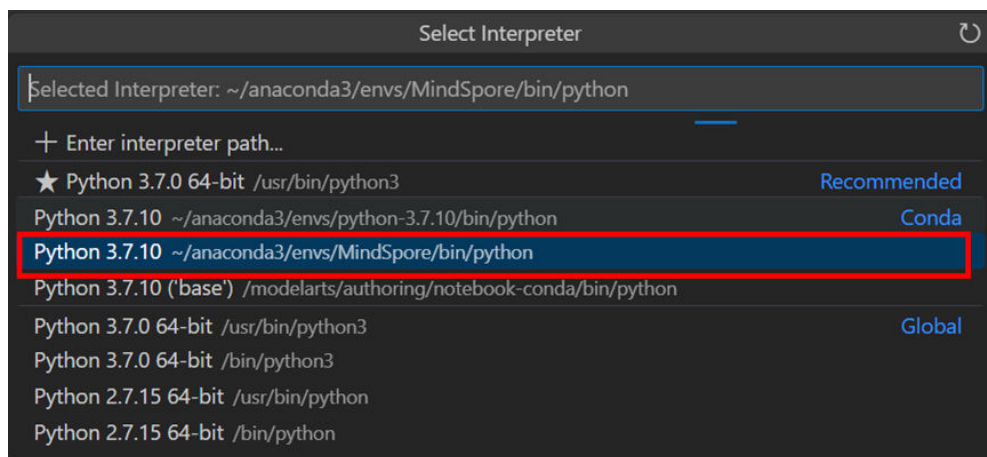
1. 打开VS Code工具，单击“Extensions”，搜索python，然后单击“Install”。

图 9-60 安装 Python



2. 输入Ctrl+Shift+P，搜索“python:select interpreter”，选择Python解释器。

图 9-61 选择 python 解释器



3. 单击“RUN > Add Configuration...”选择Python > Python File，填入如下代码。

如果文件已创建，单击“RUN > Open Configurations”，填入如下代码。

# 根据README说明文档，配置的Parameter入参如下，其中 device\_target="CPU"表示CPU环境运行，device\_target="Ascend"表示在Ascend环境运行

```
"configurations": [
 {
 "name": "Python: Django Debug Single Test",
 "type": "python",
 "request": "launch",
 "program": "${file}",
 "args": [
 "--net_name", "resnet50",
 "--dataset", "imagenet2012",
 "--data_path", "/home/ma-user/work/models/dataset/flower_photos/",
 "--class_num", "5",
 "--config_path", "/home/ma-user/work/models/official/cv/resnet/config/
```

```
resnet50_imagenet2012_config.yaml",
 "--epoch_size", "1",
 "--device_target", "Ascend"
]
}
]
```

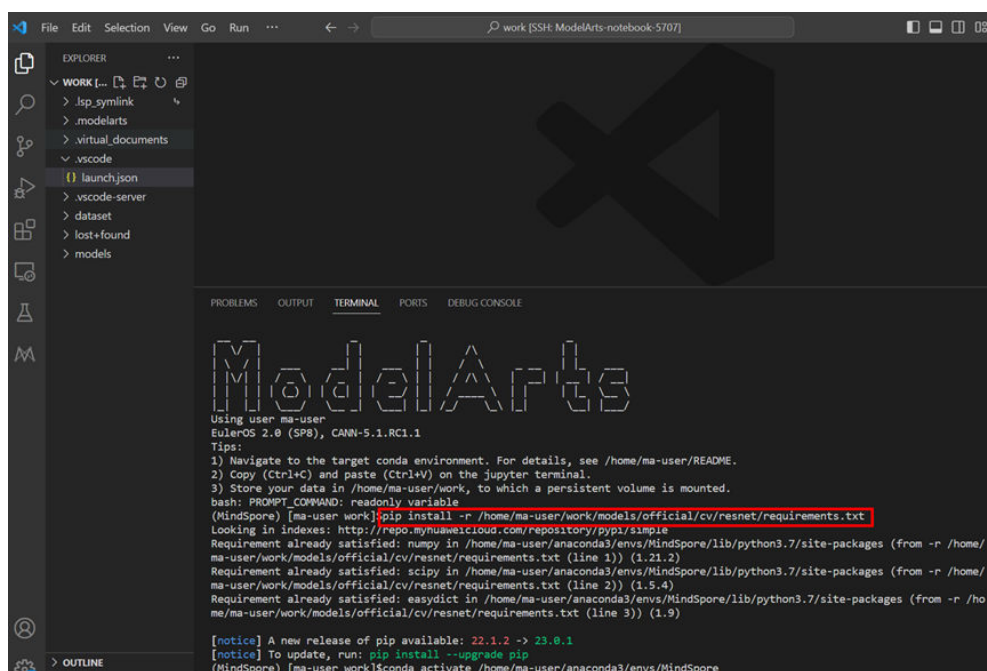
### 步骤 3: 在 VS Code 中远程调试代码

1. 参考表9-4上传本地代码和数据至云端Notebook。
2. 云端Notebook安装依赖。

在本地IDE中打开“Terminal > New Terminal”，执行如下命令。

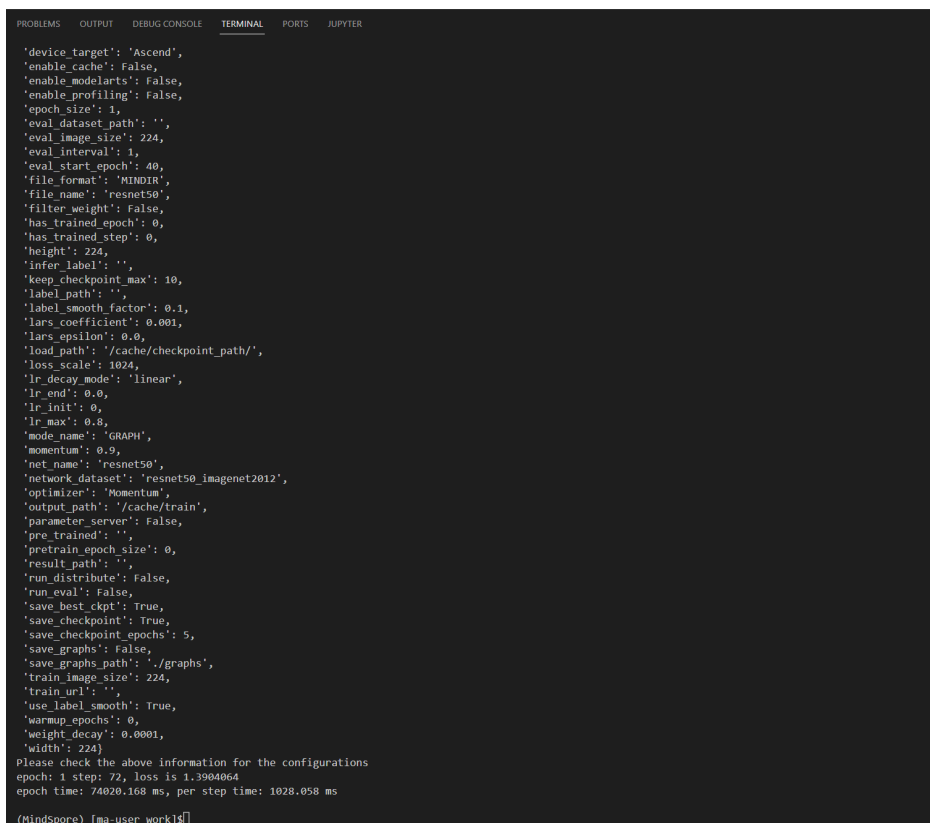
```
pip install -r /home/ma-user/work/models/official/cv/resnet/requirements.txt
```

图 9-62 执行命令



3. 云端调试与运行。
  - a. 打开训练文件。文件所在路径为“/home/ma-user/work/models/official/cv/resnet/train.py”
  - b. 代码调测：在需要调测点打断点，然后单击“RUN > Start Debugging”。
  - c. 代码运行：单击“RUN > Run Without Debugging”，运行结果如下：

图 9-63 代码运行结果



```
PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL PORTS JUPYTER
'device_target': 'Ascend',
'enable_cache': False,
'enable_modelarts': False,
'enable_profiling': False,
'epoch_size': 1,
'eval_dataset_path': '',
'eval_image_size': 224,
'eval_interval': 1,
'eval_start_epoch': 40,
'file_format': 'MINDIR',
'file_name': 'resnet50',
'filter_weight': False,
'has_trained_epoch': 0,
'has_trained_step': 0,
'height': 224,
'infer_label': '',
'keep_checkpoint_max': 10,
'label_path': '',
'label_smooth_factor': 0.1,
'lars_coefficient': 0.001,
'lars_epsilon': 0.0,
'load_path': '/cache/checkpoint_path/',
'loss_scale': 1024,
'lr_decay_mode': 'linear',
'lr_end': 0.0,
'lr_init': 0,
'lr_max': 0.8,
'mode_name': 'GRAPH',
'momentum': 0.9,
'net_name': 'resnet50',
'network_dataset': 'resnet50_imagenet2012',
'optimizer': 'Momentum',
'output_path': '/cache/train',
'parameter_server': False,
'pre_trained': '',
'pretrain_epoch_size': 0,
'result_path': '',
'run_distribute': False,
'run_eval': False,
'save_bestckpt': True,
'save_checkpoint': True,
'save_checkpoint_epochs': 5,
'save_graphs': False,
'save_graphs_path': './graphs',
'train_image_size': 224,
'train_url': '',
'use_label_smooth': True,
'warmup_epochs': 0,
'weight_decay': 0.0001,
'width': 224
Please check the above information for the configurations
epoch: 1 step: 72, loss is 1.3994064
epoch time: 74020.168 ms, per step time: 1028.058 ms
(MindSpore) [ma-user work]$
```

## 步骤 4：保存开发环境镜像

完成Notebook调测后，此时的Notebook已经包含了模型训练所有的依赖环境，因此可以将已经调测完成的开发环境保存成一个镜像。

- 方式一：保存镜像需要指定镜像名称、镜像标签、SWR服务的组织等信息，保存镜像需要等待几分钟时间，期间不能对Notebook有额外操作。  
SWR服务的组织可以在SWR服务中进行创建，也可以使用SDK创建默认的SWR组织，默认最多只能创建5个组织。
  - a. 在“/home/ma-user/work/models/official/cv/resnet/”下创建save\_image.py,
  - b. 复制代码至save\_image.py,
  - c. 运行save\_image.py，进行保存镜像。

save\_image.py代码如下：

```
save_image.py
导入ModelArts SDK的依赖，并初始化Session，此处的ak、sk、project_id、region_name请
替换成用户自己的信息
from modelarts.session import Session
认证用的ak和sk硬编码到代码中或者明文存储都有很大的安全风险，建议在配置文件或者环
境变量中密文存放，使用时解密，确保安全；
本示例以ak和sk保存在环境变量中来实现身份验证为例，运行本示例前请先在本地环境中设
置环境变量HUAWEICLOUD_SDK_AK和HUAWEICLOUD_SDK_SK。
__AK = os.environ["HUAWEICLOUD_SDK_AK"]
__SK = os.environ["HUAWEICLOUD_SDK_SK"]
如果进行了加密还需要进行解密操作
session = Session(access_key=__AK,secret_key=__SK, project_id='****', region_name='****')
```

```
保存notebook镜像
from modelarts.image_mgmt import ImageSave
from modelarts.service import SWRManagement
创建一个镜像组织。如果组织数量已超过阈值，则会报错“namespace is invalid”，需要删除一个组织或手动指定一个已有的组织信息（使用image_organization = “your-swr-namespace-name”指定）
image_organization = SWRManagement(session).get_default_namespace()
image_organization = “your-swr-namespace-name”
print("Default image_organization:", image_organization)
image_name = "mindspore-image-models-image" #@param {type:"string"}
image_tag = "1.0.0" #@param {type:"string"}
image_save = ImageSave(session=session, name=image_name, tag=image_tag,
organization=image_organization)
image_save.save()
```

- 方式二：在ModelArts控制台单击“保存镜像”。

在Notebook列表中，对于要保存的Notebook实例，单击右侧“操作”列的“更多 > 保存镜像”，进入“保存镜像”页面，设置组织、镜像名称、镜像版本和描述信息后单击“确认”保存镜像。此时Notebook会冻结，需要等待几分钟。详细操作请参考[保存Notebook镜像环境](#)。

图 9-64 保存镜像



#### 查看所保存的镜像

保存后的镜像可以在ModelArts控制台“镜像管理”页面查看到该镜像详情。单击镜像的名称，进入镜像详情页，可以查看镜像版本/ID，状态，资源类型，镜像大小，SWR地址等。

## 步骤 5：使用 SDK 提交训练作业

本地调测完成后可以提交训练作业。因为数据在Notebook中，设置InputData中“is\_local\_source”的参数为“True”，会自动将本地数据同步上传到OBS中。

步骤如下：

1. 在“/home/ma-user/work/models/official/cv/resnet/”下创建train\_notebook.py，
2. 复制代码至train\_notebook.py，
3. 运行train\_notebook.py，进行训练作业提交。

```
train_notebook.py
导入ModelArts SDK的依赖，并初始化Session，此处的ak、sk、project_id、region_name请替换
```



```
成用户自己的信息
from modelarts.train_params import TrainingFiles
from modelarts.train_params import OutputData
from modelarts.train_params import InputData
from modelarts.estimatorV2 import Estimator
from modelarts.session import Session

认证用的ak和sk硬编码到代码中或者明文存储都有很大的安全风险，建议在配置文件或者环境变量
中密文存放，使用时解密，确保安全；
本示例以ak和sk保存在环境变量中来实现身份验证为例，运行本示例前请先在本地环境中设置环境
变量HUAWEICLOUD_SDK_AK和HUAWEICLOUD_SDK_SK。
__AK = os.environ["HUAWEICLOUD_SDK_AK"]
__SK = os.environ["HUAWEICLOUD_SDK_SK"]
如果进行了加密还需要进行解密操作
session = Session(access_key=__AK,secret_key=__SK, project_id='****', region_name='****')

样例中为了方便默认创建一个OBS桶，推荐将调测所需要传输的文件统一放到`${default_bucket}/
intermediate`目录下，也可以按照注释代码自行指定

obs_bucket = session.obs.get_default_bucket()
print("Default bucket name: ", obs_bucket)
default_obs_dir = f"{obs_bucket}/intermediate"
#default_obs_dir = "obs://your-bucket-name/folder-name"

本地的工程代码文件夹路径
code_dir_local = "/home/ma-user/work/models/official/cv/resnet/" #@param {type:"string"}

代码的启动文件名称
boot_file = "train.py" #@param {type:"string"}
train_file = TrainingFiles(code_dir=code_dir_local, boot_file=boot_file)

本地数据集路径
local_data_path = "/home/ma-user/work/models/dataset/flower_photos" #@param
{type:"string"}

模型输出保存路径
output_local = "/home/ma-user/work/models/official/cv/resnet/output" #@param
{type:"string"}
模拟训练过程中模型输出回传至指定OBS的路径，需要以"/"结尾
obs_output_path = f"{default_obs_dir}/mindspore_model/output/"

指定一个obs路径用于存储输出结果
output = [OutputData(local_path=output_local, obs_path=obs_output_path, name="output")]

模拟训练过程中模训练日志回传至指定OBS的路径，需要以"/"结尾
log_obs_path = f"{default_obs_dir}/mindspore_model/logs/"

训练所需的代码路径，代码会自动从本地上传至OBS
code_obs_path = f"{default_obs_dir}/mindspore_model/"
data_obs_path = f"{default_obs_dir}/dataset/flower_photos/"

sdk会将代码自动上传至OBS，并同步到训练环境
train_file = TrainingFiles(code_dir=code_dir_local, boot_file=boot_file, obs_path=code_obs_path)

指定OBS中的数据集路径，会自动将local_path数据上传至obs_path，用户可以在代码中通过 --
data_url接收这个数据集路径
input_data = InputData(local_path=local_data_path, obs_path=data_obs_path,
is_local_source=True, name="data_url")

from modelarts.service import SWRManagement
image_organization = SWRManagement(session).get_default_namespace()
```

```

image_organization = "your-swr-namespace-name"
print("Default image_organization:", image_organization)

image_name = "mindspore-image-models-image" #@param {type:"string"}
image_tag = "1.0.0" #@param {type:"string"}

import os
ENV_NAME=os.getenv('ENV_NAME')

启动训练任务：使用user_command (shell命令) 方式启动训练任务
注意：训练启动默认的工作路径为"/home/ma-user/modelarts/user-job-dir"，而代码上传路径为
"./resnet/${code_dir}"下
--enable_modelarts=True 该代码仓已适配ModelArts
estimator = Estimator(session=session,
 training_files=train_file,
 outputs=output,
 user_image_url=f"{image_organization}/{image_name}:{image_tag}", # 自定义镜像swr地址，由镜像仓库组织/镜像名称:镜像tag组成
 user_command=f'cd /home/ma-user/modelarts/user-job-dir/ && /home/ma-user/anaconda3/envs/MindSpore/bin/python ./resnet/train.py --net_name=resnet50 --dataset=imagenet2012 --enable_modelarts=True --class_num=5 --config_path=./resnet/config/resnet50_imagenet2012_config.yaml --epoch_size=10 --device_target="Ascend" --enable_modelarts=True', # 执行训练命令
 train_instance_type="modelarts.p3.large.public", # 虚拟资源规格，不同region的资源规格可能不同，请参考“Estimator参数说明”表下的说明查询修改
 train_instance_count=1, # 节点数，适用于多机分布式训练，默认是1
 #pool_id='若指定专属池，替换为页面上查到的poolId'，同时修改资源规格为专属池专用的虚拟子规格
 log_url=log_obs_path
)
job_name是可选参数，可不填随机生成工作名
job_instance = estimator.fit(inputs=[input_data],
 job_name="modelarts_training_job_with_sdk_by_command_v01")

```

表 9-5 Estimator 参数说明

| 参数名称                 | 参数说明                                                        |
|----------------------|-------------------------------------------------------------|
| session              | modelarts session                                           |
| training_files       | 训练代码的路径和启动文件                                                |
| user_image_url       | 自定义镜像swr地址，由镜像仓库组织/镜像名称:镜像tag组成                             |
| user_command         | 执行训练命令                                                      |
| train_instance_type  | 本地调测'local'或云端资源规格。每个region的资源规格可能是不同的，可以通过下述说明查询对应的资源规格信息。 |
| train_instance_count | 节点数                                                         |
| log_url              | 日志输出路径                                                      |
| job_name             | 作业名称，不可以重复                                                  |

## 📖 说明

train\_instance\_type表示训练的资源规格，每个region的资源规格可能是不同的。通过如下方法查询资源规格：

- 公共资源池执行如下命令查询

```
from modelarts.session import Session
from modelarts.estimatorV2 import Estimator
from pprint import pprint

认证用的ak和sk硬编码到代码中或者明文存储都有很大的安全风险，建议在配置文件或者环境变量中密文存放，使用时解密，确保安全；
本示例以ak和sk保存在环境变量中来实现身份验证为例，运行本示例前请先在本地环境中设置环境变量HUAWEICLOUD_SDK_AK和HUAWEICLOUD_SDK_SK。
__AK = os.environ["HUAWEICLOUD_SDK_AK"]
__SK = os.environ["HUAWEICLOUD_SDK_SK"]
如果进行了加密还需要进行解密操作
session = Session(access_key=__AK,secret_key=__SK, project_id='***', region_name='***')

info = Estimator.get_train_instance_types(session=session)
pprint(info)
```

- 专属池规格

ModelArts专属资源池统一使用虚拟子规格，不区分GPU和Ascend。资源规格参考[表9-6](#)查询。

**表 9-6** 专属资源池虚拟规格的说明

| train_instance_type           | 说明 |
|-------------------------------|----|
| modelarts.pool.visual.xlarge  | 1卡 |
| modelarts.pool.visual.2xlarge | 2卡 |
| modelarts.pool.visual.4xlarge | 4卡 |
| modelarts.pool.visual.8xlarge | 8卡 |

## 步骤 6：清除资源

Notebook在代码调试完成及提交训练作业后就可以关闭了，减少资源扣费。

当调测完成且实例处于运行状态时，单击停止；

当下次调测且实例处于停止状态时，单击启动实例，随开随用。

## 训练输出保存结构说明

ModelArts训练作业的输出和日志信息会定时同步到指定的OBS中，本示例中模型输出路径和日志输出路径分别为f"{default\_obs\_dir}/mindspore\_model/output/"和f"{default\_obs\_dir}/mindspore\_model/logs/"，用户可以在OBS中查看训练输出信息。

本示例中训练输出保存在OBS的目录结构如下所示：

```

${your_bucket}
├── intermediate
└── dataset
```

```
├── flower_photos
│ ├── flower_photos.zip
│ └── mindspore_model
├── logs
│ └── xxx-xxx-xxx--0.log
├── output
│ └── 20220627-105226-resnet50-224
└── mindspore-image-models.zip
```

## 提交训练作业常见问题

- **报错信息: Exception: You have attempted to create more buckets than allowed**  
原因分析: 由于桶的数量多于限额, 无法自动创建。  
解决方法: 用户可以删除一个桶, 或者直接指定一个已存在的桶 (修改变量 obs\_bucket 的值)。
- **报错信息: "errorMessage": "The number of namespaces exceeds the upper limit" 或 "namespace is invalid"**  
原因分析: SWR组织数限额, SWR组织默认最多只能创建5个组织。  
解决方法: 用户可以删除一个SWR组织, 或者直接指定一个已存在的SWR组织 (修改变量 image\_organization 的值)。
- **报错信息: standard\_init\_linux.go:224: exec user process caused "exet format error"**  
原因分析: 可能由于训练规格错误导致训练作业卡死。  
解决方法: 请参考[说明](#)查询资源规格。
- **报错信息: 报错镜像失败, 报错: 401, 'Unauthorized', b{'errors': [{"errorCode": "SVCSTG.SWR.4010000", errorMessage": "Authenticate Error", ...}]}**  
原因分析: 远程连接Notebook时需要输入鉴权信息。  
解决方法: 传入AK, SK信息。  

```
认证用的ak和sk硬编码到代码中或者明文存储都有很大的安全风险, 建议在配置文件或者环境变量中密文存放, 使用时解密, 确保安全;
本示例以ak和sk保存在环境变量中来实现身份验证为例, 运行本示例前请先在本地环境中设置环境变量HUAWEICLOUD_SDK_AK和HUAWEICLOUD_SDK_SK。
__AK = os.environ["HUAWEICLOUD_SDK_AK"]
__SK = os.environ["HUAWEICLOUD_SDK_SK"]
如果进行了加密还需要进行解密操作
session = Session(access_key=__AK, secret_key=__SK, project_id='***', region_name='***')
```

# 10 模型训练

## 10.1 使用 AI Gallery 的订阅算法实现花卉识别

本案例以“ResNet\_v1\_50”算法、花卉识别数据集为例，指导如何从AI Gallery下载数据集和订阅算法，然后使用算法创建训练模型，将所得的模型部署为在线服务。其他算法操作步骤类似，可参考“ResNet\_v1\_50”算法操作。

### 📖 说明

费用说明：本案例使用过程中，从AI Gallery下载数据集和订阅算法免费，在ModelArts上运行训练作业推荐使用免费资源，将模型部署为在线服务推荐使用免费资源。但是数据集存储在OBS桶中会收取少量费用，具体计费请参见[OBS价格详情页](#)，案例使用完成后请及时清除资源和数据。

### 步骤 1：准备工作

- 注册华为账号并开通华为云、实名认证
  - [注册华为账号并开通华为云](#)
  - [进行实名认证](#)

- 配置委托访问授权

ModelArts使用过程中涉及到OBS、SWR、IEF等服务交互，首次使用ModelArts需要用户配置委托授权，允许访问这些依赖服务。

- a. 使用华为云账号登录[ModelArts管理控制台](#)，在左侧导航栏单击“全局配置”，进入“全局配置”页面，单击“添加授权”。
- b. 在弹出的“访问授权”窗口中，

**授权对象类型：所有用户**

**委托选择：新增委托**

**权限配置：普通用户**

选择完成后勾选“我已经仔细阅读并同意《ModelArts服务声明》”，然后单击“创建”。

图 10-1 配置委托访问授权



- c. 完成配置后，在ModelArts控制台的全局配置列表，可查看到此账号的委托配置信息。

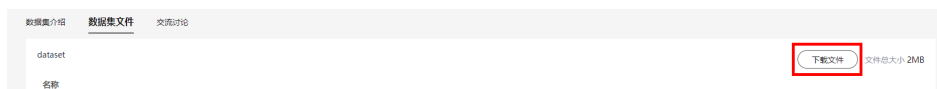
图 10-2 查看委托配置信息

| 授权对象     | 授权对象类型 | 授权类型 | 授权内容             | 授权方式 | 创建时间                          | 操作                   |
|----------|--------|------|------------------|------|-------------------------------|----------------------|
| ak-users | 所有用户   | 委托   | modelarts_agency | 角色授权 | 2023/11/21 09:57:47 GMT+08:00 | <a href="#">查看详情</a> |

## 步骤 2：准备训练数据

1. 单击案例链接[四类花卉图像分类小数据集](#)，进入案例详情页。
2. 单击“数据集文件”页签后，单击“下载文件”按钮后，跳转至下载页面详情页。

图 10-3 下载数据集



3. 在下载详情页，填写参数。
  - 下载方式：选择“对象存储服务（OBS）”
  - 目标区域：选择“华北-北京四”（即上一步中选择的云服务区）
  - 目标位置：请选择一个空的OBS目录，本示例为“/test-modelartzs/dataset-flower/”

图 10-4 下载至 OBS



### 说明

此处从AI Gallery下载并使用数据集是限时免费的，但数据集存储在OBS，从OBS中读取数据需要根据OBS的计费原则收费。

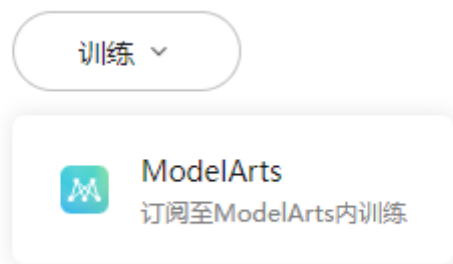
4. 确认无误后，单击确定。页面自动跳转到“我的数据>我的下载”页面，请耐心等待，预计5分钟左右。
5. 下载完成后，您可以单击目标位置跳转至OBS桶中查看是否存在已下载的数据。

## 步骤 3：订阅算法

目前“图像分类-ResNet\_v1\_50”算法发布在AI Gallery中。您可以前往AI Gallery，订阅此算法，然后同步至ModelArts中。

1. 单击[算法链接](#)进入算法详情页。
2. 单击右侧的“训练”后，单击“订阅至ModelArts内训练”，页面将自动跳转至ModelArts的“算法管理>我的订阅”中。

图 10-5 订阅算法



## 步骤 4：使用订阅算法创建训练作业

算法订阅成功后，算法将呈现在“算法管理>我的订阅”中，您可以使用订阅的“图像分类-ResNet\_v1\_50”算法创建训练作业，获得模型。

1. 进入“算法管理 > 我的订阅”页面，选择订阅的“图像分类-ResNet\_v1\_50”算法，单击操作列的“创建训练作业”。

图 10-6 创建训练作业



- 在创建训练作业页面，参考如下说明填写关键参数。
  - “创建方式>我的订阅”：系统默认选择订阅的算法，请勿随意修改。
  - “训练输入”：选择数据存储位置，然后从弹出的窗口中选择**步骤2: 准备训练数据**中下载好的数据dataset-flower。
  - “训练输出”：选择一个OBS空目录存储训练输出的模型。例如：“test-modelartsz/output-flower”
  - “超参”：建议采用默认值。如需进行调优，可参考**运行参数说明**。
  - “资源类型”：可以选择限时免费的GPU规格资源，如果希望训练效率更高，可以选择收费的GPU资源。
  - “计算节点个数”：建议采用默认值1。

图 10-7 训练作业参数-训练输入/输出



- 参数填写完成后，单击“提交”，根据界面提示确认规格，单击“确定”，完成训练作业创建。
- 进入“训练管理 > 训练作业”页面，等待训练作业完成。  
训练作业运行需要几分钟时间，请耐心等待。根据经验，选择样例数据集，使用GPU资源运行，预计3分钟左右可完成。  
当训练作业的状态变更为“已完成”时，表示已运行结束。  
您可以单击训练作业名称，进入详情页面，了解训练作业的“配置信息”、“日志”、“资源占用情况”和“评估结果”等信息。您也可以配置的“训练输出位置”对应的OBS目录下获得训练生成的模型。

## 步骤 5: 创建 AI 应用

- 在训练作业详情页的右上角单击“创建AI应用”，进入创建AI应用页面。

图 10-8 创建 AI 应用



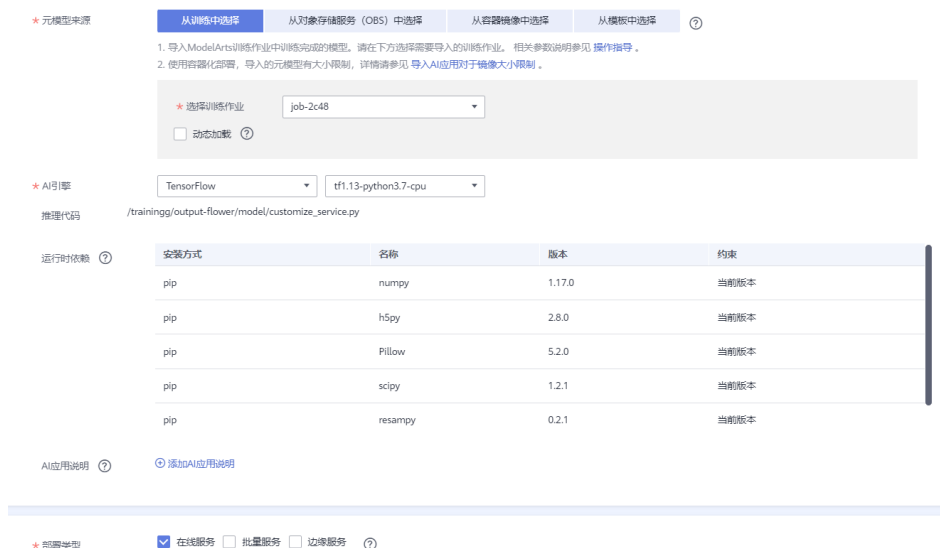
也可以在ModelArts管理控制台，选择“AI应用管理 > AI应用”，在“我的AI应用”页面，单击“创建”，进入创建AI应用页面。

- 在创建AI应用页面，系统会自动根据上一步训练作业填写参数，参考如下说明确认关键参数。  
“元模型来源”：系统自动选择“从训练中选择”。



- “选择训练作业”：系统自动选择上一步创建的训练作业。
- “AI引擎”：系统自动写入该模型的AI引擎，无需修改。
- “推理代码”：系统自动放置推理代码到OBS输出路径，无需修改。
- “部署类型”：默认选择“在线服务”。

图 10-9 从训练中选择



- 参数填写完成后，单击“立即创建”。页面自动跳转至AI应用列表页面，等待创建结果，预计2分钟左右。  
当AI应用的状态变为“正常”时，表示创建成功。

图 10-10 模型导入成功

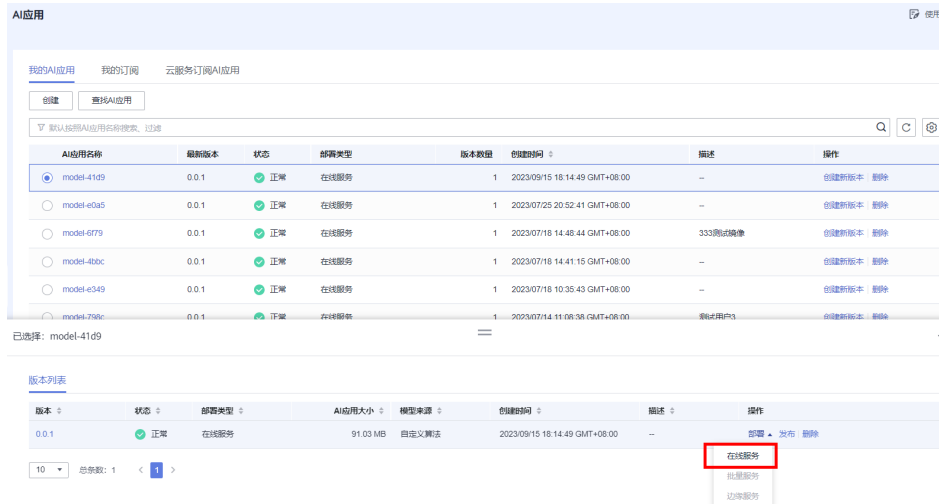
| AI应用名称                           | 最新版本  | 状态                                     |
|----------------------------------|-------|----------------------------------------|
| <input type="radio"/> model-41d9 | 0.0.1 | <input checked="" type="checkbox"/> 正常 |

## 步骤 6：部署为在线服务（CPU）

AI应用创建成功后，可将其部署为在线服务，在部署时可使用CPU资源。

- 单击AI应用名称左侧的单选按钮，在列表页底部展开“版本列表”，在版本的操作列中单击“部署 > 在线服务”。

图 10-11 部署模型



2. 在部署页面，参考如下说明填写关键参数。
  - “资源池”：选择“公共资源池”。
  - “选择AI应用及版本”：AI应用来源及版本会自动选择前面创建的AI应用。
  - “计算节点规格”：在下拉框中选择限时免费的CPU资源，如果限时免费资源售罄，建议选择收费CPU资源进行部署。
  - “计算节点个数”，默认设置为“1”。
  - 其他参数可使用默认值。

**说明**

选择CPU资源部署模型会收取少量费用，具体费用以界面信息为准。

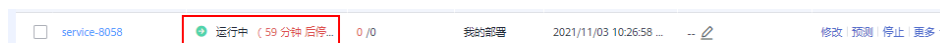
如果需要使用GPU资源部署上线，需要进入模型所在位置，即**步骤4：使用订阅算法创建训练作业**步骤生成的“训练输出”路径，进入“model”目录，打开并编辑“config.json”文件，将“runtime”的配置修改为ModelArts支持的GPU规格，例如“runtime”: “tf1.13-python3.6-gpu”。修改完成后，重新执行**步骤5：创建AI应用**和**步骤6：部署为在线服务（CPU）**。

图 10-12 部署模型



3. 参数设置完成后，单击“下一步”，确认规格参数，单击提交，完成在线服务的部署。
4. 您可以进入“部署上线 > 在线服务”页面，等待服务部署完成，当服务状态变为“运行中”时，表示服务部署成功。预计时长2分钟左右。

图 10-13 运行中的服务



5. 在线服务部署完成后，您可以单击操作列的预测，进入服务详情页的“预测”页面。
6. 在“预测”页签，单击“上传”，上传一个测试图片，单击“预测”进行预测。此处提供一个预测样例图供使用。

图 10-14 预测样例图

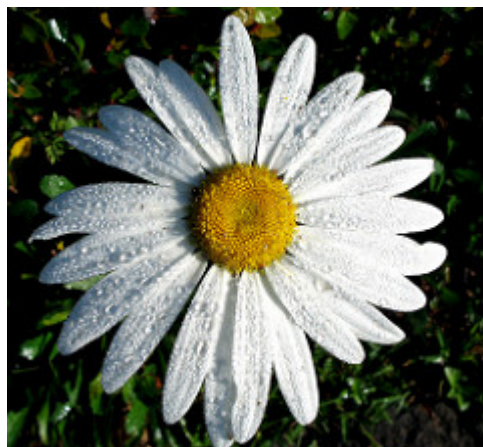


图 10-15 预测结果



## 步骤 7: 清除资源

为避免产生不必要的费用，通过此示例学习订阅算法的使用后，建议您清除相关资源，避免造成资源浪费。

- 停止在线服务：在“在线服务”页面，单击对应服务操作列的“停止”。
- 删除训练作业：在“训练作业”页面，单击操作列的“删除”。
- 删除数据：前往OBS，删除数据，然后删除文件夹及OBS桶。

## 10.2 使用自定义算法构建模型（手写数字识别）

本文为用户提供如何将本地的自定义算法通过简单的代码适配，实现在ModelArts上进行模型训练与部署的全流程指导。

## 场景描述

本案例用于指导用户使用PyTorch1.8实现手写数字图像识别，示例采用的数据集为MNIST官方数据集。

通过学习本案例，您可以了解如何在ModelArts平台上训练作业、部署推理模型并预测的完整流程。

## 步骤 1：准备工作

- 已注册华为账号并开通华为云，且在使用 ModelArts 前检查账号状态，账号不能处于欠费或冻结状态。
- 配置委托访问授权

ModelArts使用过程中涉及到OBS、SWR、IEF等服务交互，首次使用ModelArts需要用户配置委托授权，允许访问这些依赖服务。

- 使用华为云账号登录**ModelArts管理控制台**，在左侧导航栏单击“全局配置”，进入“全局配置”页面，单击“添加授权”。
- 在弹出的“访问授权”窗口中：

**授权对象类型：所有用户**

**委托选择：新增委托**

**权限配置：普通用户**

选择完成后勾选“我已经仔细阅读并同意《ModelArts服务声明》”，然后单击“创建”。

图 10-16 配置委托访问授权



- 完成配置后，在ModelArts控制台的全局配置列表，可查看到此账号的委托配置信息。

图 10-17 查看委托配置信息

| 授权对象 | 授权对象类型 | 授权类型 | 授权内容      | 创建时间                          | 操作                                      |
|------|--------|------|-----------|-------------------------------|-----------------------------------------|
| 所有用户 | 所有用户   | 委托   | ma_agency | 2023/09/15 17:29:30 GMT+08:00 | <a href="#">查看详情</a> <a href="#">删除</a> |

## 步骤 2：准备训练数据

本案例使用的数据是MNIST数据集，您可以从**MNIST官网**下载数据集至本地，以下4个文件均要下载。

图 10-18 MNIST 数据集

Four files are available on this site:

```
train-images-idx3-ubyte.gz: training set images (9912422 bytes)
train-labels-idx1-ubyte.gz: training set labels (28881 bytes)
t10k-images-idx3-ubyte.gz: test set images (1648877 bytes)
t10k-labels-idx1-ubyte.gz: test set labels (4542 bytes)
```

- “train-images-idx3-ubyte.gz”：训练集的压缩包文件，共包含60000个样本。
- “train-labels-idx1-ubyte.gz”：训练集标签的压缩包文件，共包含60000个样本的类别标签。
- “t10k-images-idx3-ubyte.gz”：验证集的压缩包文件，共包含10000个样本。
- “t10k-labels-idx1-ubyte.gz”：验证集标签的压缩包文件，共包含10000个样本的类别标签。

#### 📖 说明

如果单击MNIST官网链接后提示输入登录信息，可在浏览器中直接粘贴此链接免登录：<http://yann.lecun.com/exdb/mnist/>

出现登录提示是由于浏览器使用了https的方式打开了该链接，使用http的方式打开则无需登录信息。

### 步骤 3：准备训练文件和推理文件

针对此案例，ModelArts提供了需使用的训练脚本、推理脚本和推理配置文件。请参考如下文件内容。

#### 📖 说明

粘贴.py文件代码时，请直接新建.py文件，否则会可能出现“SyntaxError: 'gbk' codec can't decode byte 0xa4 in position 324: illegal multibyte sequence”报错。

粘贴完代码后，建议检查代码文件是否出现中文注释变为乱码的情况，如果出现该情况请将编辑器改为utf-8格式后再粘贴代码。

在本地电脑中创建训练脚本“train.py”，内容如下：

```
base on https://github.com/pytorch/examples/blob/main/mnist/main.py

from __future__ import print_function

import os
import gzip
import codecs
import argparse
from typing import IO, Union

import numpy as np

import torch
import torch.nn as nn
import torch.nn.functional as F
import torch.optim as optim
from torchvision import datasets, transforms
from torch.optim.lr_scheduler import StepLR

import shutil
```

```
定义网络模型
class Net(nn.Module):
 def __init__(self):
 super(Net, self).__init__()
 self.conv1 = nn.Conv2d(1, 32, 3, 1)
 self.conv2 = nn.Conv2d(32, 64, 3, 1)
 self.dropout1 = nn.Dropout(0.25)
 self.dropout2 = nn.Dropout(0.5)
 self.fc1 = nn.Linear(9216, 128)
 self.fc2 = nn.Linear(128, 10)

 def forward(self, x):
 x = self.conv1(x)
 x = F.relu(x)
 x = self.conv2(x)
 x = F.relu(x)
 x = F.max_pool2d(x, 2)
 x = self.dropout1(x)
 x = torch.flatten(x, 1)
 x = self.fc1(x)
 x = F.relu(x)
 x = self.dropout2(x)
 x = self.fc2(x)
 output = F.log_softmax(x, dim=1)
 return output

模型训练, 设置模型为训练模式, 加载训练数据, 计算损失函数, 执行梯度下降
def train(args, model, device, train_loader, optimizer, epoch):
 model.train()
 for batch_idx, (data, target) in enumerate(train_loader):
 data, target = data.to(device), target.to(device)
 optimizer.zero_grad()
 output = model(data)
 loss = F.nll_loss(output, target)
 loss.backward()
 optimizer.step()
 if batch_idx % args.log_interval == 0:
 print('Train Epoch: {} [{} / {}] {:.0f}%] \tLoss: {:.6f}'.format(
 epoch, batch_idx * len(data), len(train_loader.dataset),
 100. * batch_idx / len(train_loader), loss.item()))
 if args.dry_run:
 break

模型验证, 设置模型为验证模式, 加载验证数据, 计算损失函数和准确率
def test(model, device, test_loader):
 model.eval()
 test_loss = 0
 correct = 0
 with torch.no_grad():
 for data, target in test_loader:
 data, target = data.to(device), target.to(device)
 output = model(data)
 test_loss += F.nll_loss(output, target, reduction='sum').item()
 pred = output.argmax(dim=1, keepdim=True)
 correct += pred.eq(target.view_as(pred)).sum().item()

 test_loss /= len(test_loader.dataset)

 print('\nTest set: Average loss: {:.4f}, Accuracy: {} / {} {:.0f}%\n'.format(
 test_loss, correct, len(test_loader.dataset),
 100. * correct / len(test_loader.dataset)))

以下为pytorch mnist
https://github.com/pytorch/vision/blob/v0.9.0/torchvision/datasets/mnist.py
def get_int(b: bytes) -> int:
 return int(codecs.encode(b, 'hex'), 16)
```

```
def open_maybe_compressed_file(path: Union[str, IO]) -> Union[IO, gzip.GzipFile]:
 """Return a file object that possibly decompresses 'path' on the fly.
 Decompression occurs when argument 'path' is a string and ends with '.gz' or '.xz'.
 """
 if not isinstance(path, torch._six.string_classes):
 return path
 if path.endswith('.gz'):
 return gzip.open(path, 'rb')
 if path.endswith('.xz'):
 return lzma.open(path, 'rb')
 return open(path, 'rb')

SN3_PASCALVINCENT_TYEMAP = {
 8: (torch.uint8, np.uint8, np.uint8),
 9: (torch.int8, np.int8, np.int8),
 11: (torch.int16, np.dtype('>i2'), 'i2'),
 12: (torch.int32, np.dtype('>i4'), 'i4'),
 13: (torch.float32, np.dtype('>f4'), 'f4'),
 14: (torch.float64, np.dtype('>f8'), 'f8')
}

def read_sn3_pascalvincent_tensor(path: Union[str, IO], strict: bool = True) -> torch.Tensor:
 """Read a SN3 file in "Pascal Vincent" format (Lush file 'libidx/idx-io.lsh').
 Argument may be a filename, compressed filename, or file object.
 """
 # read
 with open_maybe_compressed_file(path) as f:
 data = f.read()
 # parse
 magic = get_int(data[0:4])
 nd = magic % 256
 ty = magic // 256
 assert 1 <= nd <= 3
 assert 8 <= ty <= 14
 m = SN3_PASCALVINCENT_TYEMAP[ty]
 s = [get_int(data[4 * (i + 1): 4 * (i + 2)]) for i in range(nd)]
 parsed = np.frombuffer(data, dtype=m[1], offset=(4 * (nd + 1)))
 assert parsed.shape[0] == np.prod(s) or not strict
 return torch.from_numpy(parsed.astype(m[2], copy=False)).view(*s)

def read_label_file(path: str) -> torch.Tensor:
 with open(path, 'rb') as f:
 x = read_sn3_pascalvincent_tensor(f, strict=False)
 assert(x.dtype == torch.uint8)
 assert(x.ndimension() == 1)
 return x.long()

def read_image_file(path: str) -> torch.Tensor:
 with open(path, 'rb') as f:
 x = read_sn3_pascalvincent_tensor(f, strict=False)
 assert(x.dtype == torch.uint8)
 assert(x.ndimension() == 3)
 return x

def extract_archive(from_path, to_path):
 to_path = os.path.join(to_path, os.path.splitext(os.path.basename(from_path))[0])
 with open(to_path, "wb") as out_f, gzip.GzipFile(from_path) as zip_f:
 out_f.write(zip_f.read())
 # --- 以上为pytorch mnist
 # --- end
```

```
raw mnist 数据处理
def convert_raw_mnist_dataset_to_pytorch_mnist_dataset(data_url):
 """
 raw

 {data_url}/
 train-images-idx3-ubyte.gz
 train-labels-idx1-ubyte.gz
 t10k-images-idx3-ubyte.gz
 t10k-labels-idx1-ubyte.gz

 processed

 {data_url}/
 train-images-idx3-ubyte.gz
 train-labels-idx1-ubyte.gz
 t10k-images-idx3-ubyte.gz
 t10k-labels-idx1-ubyte.gz
 MNIST/raw
 train-images-idx3-ubyte
 train-labels-idx1-ubyte
 t10k-images-idx3-ubyte
 t10k-labels-idx1-ubyte
 MNIST/processed
 training.pt
 test.pt
 """
 resources = [
 "train-images-idx3-ubyte.gz",
 "train-labels-idx1-ubyte.gz",
 "t10k-images-idx3-ubyte.gz",
 "t10k-labels-idx1-ubyte.gz"
]

 pytorch_mnist_dataset = os.path.join(data_url, 'MNIST')

 raw_folder = os.path.join(pytorch_mnist_dataset, 'raw')
 processed_folder = os.path.join(pytorch_mnist_dataset, 'processed')

 os.makedirs(raw_folder, exist_ok=True)
 os.makedirs(processed_folder, exist_ok=True)

 print('Processing...')

 for f in resources:
 extract_archive(os.path.join(data_url, f), raw_folder)

 training_set = (
 read_image_file(os.path.join(raw_folder, 'train-images-idx3-ubyte')),
 read_label_file(os.path.join(raw_folder, 'train-labels-idx1-ubyte'))
)
 test_set = (
 read_image_file(os.path.join(raw_folder, 't10k-images-idx3-ubyte')),
 read_label_file(os.path.join(raw_folder, 't10k-labels-idx1-ubyte'))
)
 with open(os.path.join(processed_folder, 'training.pt'), 'wb') as f:
 torch.save(training_set, f)
 with open(os.path.join(processed_folder, 'test.pt'), 'wb') as f:
 torch.save(test_set, f)

 print('Done!')

def main():
 # 定义可以接收的训练作业运行参数
 parser = argparse.ArgumentParser(description='PyTorch MNIST Example')

 parser.add_argument('--data_url', type=str, default=False,
 help='mnist dataset path')
```



```
parser.add_argument('--train_url', type=str, default=False,
 help='mnist model path')

parser.add_argument('--batch-size', type=int, default=64, metavar='N',
 help='input batch size for training (default: 64)')
parser.add_argument('--test-batch-size', type=int, default=1000, metavar='N',
 help='input batch size for testing (default: 1000)')
parser.add_argument('--epochs', type=int, default=14, metavar='N',
 help='number of epochs to train (default: 14)')
parser.add_argument('--lr', type=float, default=1.0, metavar='LR',
 help='learning rate (default: 1.0)')
parser.add_argument('--gamma', type=float, default=0.7, metavar='M',
 help='Learning rate step gamma (default: 0.7)')
parser.add_argument('--no-cuda', action='store_true', default=False,
 help='disables CUDA training')
parser.add_argument('--dry-run', action='store_true', default=False,
 help='quickly check a single pass')
parser.add_argument('--seed', type=int, default=1, metavar='S',
 help='random seed (default: 1)')
parser.add_argument('--log-interval', type=int, default=10, metavar='N',
 help='how many batches to wait before logging training status')
parser.add_argument('--save-model', action='store_true', default=True,
 help='For Saving the current Model')
args = parser.parse_args()

use_cuda = not args.no_cuda and torch.cuda.is_available()

torch.manual_seed(args.seed)

设置使用 GPU 还是 CPU 来运行算法
device = torch.device("cuda" if use_cuda else "cpu")

train_kwargs = {'batch_size': args.batch_size}
test_kwargs = {'batch_size': args.test_batch_size}
if use_cuda:
 cuda_kwargs = {'num_workers': 1,
 'pin_memory': True,
 'shuffle': True}
 train_kwargs.update(cuda_kwargs)
 test_kwargs.update(cuda_kwargs)

定义数据预处理方法
transform=transforms.Compose([
 transforms.ToTensor(),
 transforms.Normalize((0.1307,), (0.3081,))
])

将 raw mnist 数据集转换为 pytorch mnist 数据集
convert_raw_mnist_dataset_to_pytorch_mnist_dataset(args.data_url)

分别创建训练和验证数据集
dataset1 = datasets.MNIST(args.data_url, train=True, download=False,
 transform=transform)
dataset2 = datasets.MNIST(args.data_url, train=False, download=False,
 transform=transform)

分别构建训练和验证数据迭代器
train_loader = torch.utils.data.DataLoader(dataset1, **train_kwargs)
test_loader = torch.utils.data.DataLoader(dataset2, **test_kwargs)

初始化神经网络模型并复制模型到计算设备上
model = Net().to(device)
定义训练优化器和学习率策略, 用于梯度下降计算
optimizer = optim.Adadelta(model.parameters(), lr=args.lr)
scheduler = StepLR(optimizer, step_size=1, gamma=args.gamma)

训练神经网络, 每一轮进行一次验证
for epoch in range(1, args.epochs + 1):
 train(args, model, device, train_loader, optimizer, epoch)
```

```
test(model, device, test_loader)
scheduler.step()

保存模型与适配 ModelArts 推理模型包规范
if args.save_model:

 # 在 train_url 训练参数对应的路径内创建 model 目录
 model_path = os.path.join(args.train_url, 'model')
 os.makedirs(model_path, exist_ok = True)

 # 按 ModelArts 推理模型包规范, 保存模型到 model 目录内
 torch.save(model.state_dict(), os.path.join(model_path, 'mnist_cnn.pt'))

 # 复制推理代码与配置文件到 model 目录内
 the_path_of_current_file = os.path.dirname(__file__)
 shutil.copyfile(os.path.join(the_path_of_current_file, 'infer/customize_service.py'),
os.path.join(model_path, 'customize_service.py'))
 shutil.copyfile(os.path.join(the_path_of_current_file, 'infer/config.json'), os.path.join(model_path,
'config.json'))

if __name__ == '__main__':
 main()
```

在本地电脑中创建推理脚本“customize\_service.py”，内容如下：

```
import os
import log
import json

import torch.nn.functional as F
import torch.nn as nn
import torch
import torchvision.transforms as transforms

import numpy as np
from PIL import Image

from model_service.pytorch_model_service import PTServingBaseService

logger = log.getLogger(__name__)

定义模型预处理
infer_transformation = transforms.Compose([
 transforms.Resize(28),
 transforms.CenterCrop(28),
 transforms.ToTensor(),
 transforms.Normalize((0.1307,), (0.3081,))
])

模型推理服务
class PTVisionService(PTServingBaseService):

 def __init__(self, model_name, model_path):
 # 调用父类构造方法
 super(PTVisionService, self).__init__(model_name, model_path)

 # 调用自定义函数加载模型
 self.model = Mnist(model_path)

 # 加载标签
 self.label = [0,1,2,3,4,5,6,7,8,9]

 # 接收request数据, 并转换为模型可以接受的输入格式
 def _preprocess(self, data):
 preprocessed_data = {}
 for k, v in data.items():
 input_batch = []
 for file_name, file_content in v.items():
 with Image.open(file_content) as image1:
 # 灰度处理
```

```
 image1 = image1.convert("L")
 if torch.cuda.is_available():
 input_batch.append(infer_transformation(image1).cuda())
 else:
 input_batch.append(infer_transformation(image1))
 input_batch_var = torch.autograd.Variable(torch.stack(input_batch, dim=0), volatile=True)
 print(input_batch_var.shape)
 preprocessed_data[k] = input_batch_var

 return preprocessed_data

将推理的结果进行后处理，得到预期的输出格式，该结果就是最终的返回值
def _postprocess(self, data):
 results = []
 for k, v in data.items():
 result = torch.argmax(v[0])
 result = {k: self.label[result]}
 results.append(result)
 return results

对于输入数据进行前向推理，得到推理结果
def _inference(self, data):

 result = {}
 for k, v in data.items():
 result[k] = self.model(v)

 return result

定义网络
class Net(nn.Module):
 def __init__(self):
 super(Net, self).__init__()
 self.conv1 = nn.Conv2d(1, 32, 3, 1)
 self.conv2 = nn.Conv2d(32, 64, 3, 1)
 self.dropout1 = nn.Dropout(0.25)
 self.dropout2 = nn.Dropout(0.5)
 self.fc1 = nn.Linear(9216, 128)
 self.fc2 = nn.Linear(128, 10)

 def forward(self, x):
 x = self.conv1(x)
 x = F.relu(x)
 x = self.conv2(x)
 x = F.relu(x)
 x = F.max_pool2d(x, 2)
 x = self.dropout1(x)
 x = torch.flatten(x, 1)
 x = self.fc1(x)
 x = F.relu(x)
 x = self.dropout2(x)
 x = self.fc2(x)
 output = F.log_softmax(x, dim=1)
 return output

def Mnist(model_path, **kwargs):
 # 生成网络
 model = Net()

 # 加载模型
 if torch.cuda.is_available():
 device = torch.device('cuda')
 model.load_state_dict(torch.load(model_path, map_location="cuda:0"))
 else:
 device = torch.device('cpu')
 model.load_state_dict(torch.load(model_path, map_location=device))

 # CPU 或者 GPU 映射
```

```
model.to(device)

声明为推理模式
model.eval()

return model
```

在本地电脑中推理配置文件“config.json”，内容如下：

```
{
 "model_algorithm": "image_classification",
 "model_type": "PyTorch",
 "runtime": "pytorch_1.8.0-cuda_10.2-py_3.7-ubuntu_18.04-x86_64"
}
```

## 步骤 4：创建 OBS 桶并上传文件

将上一步中的数据和代码文件、推理代码文件与推理配置文件，从本地上传到OBS桶中。在 ModelArts 上运行训练作业时，需要从OBS桶中读取数据和代码文件。

1. 登录OBS管理控制台，按照如下示例创建OBS桶和文件夹，创建后如图10-19所示。创建OBS桶和文件夹的操作指导请参见[创建桶](#)和[新建文件夹](#)。

```
{OBS桶} # OBS对象桶，用户可以自定义名称，例如：test-modelarts-xx
-{OBS文件夹} # OBS文件夹，自定义名称，此处举例为pytorch
- mnist-data # OBS文件夹，用于存放训练数据集，可以自定义名称，此处举例为mnist-data
- mnist-code # OBS文件夹，用于存放训练脚本train.py，可以自定义名称，此处举例为mnist-code
- infer # OBS文件夹，用于存放推理脚本customize_service.py和配置文件config.json
- mnist-output # OBS文件夹，用于存放训练输出模型，可以自定义名称，此处举例为mnist-output
```

### 注意

- 创建的OBS桶所在区域和后续使用ModelArts必须在同一个区域Region，否则会导致训练时找不到OBS桶。具体操作可参见[查看OBS桶与ModelArts是否在同一区域](#)。
- 创建OBS桶时，桶的存储类别请勿选择“归档存储”，归档存储的OBS桶会导致模型训练失败。

图 10-19 OBS 文件目录



2. 上传[Step1 准备训练数据](#)下载的MNIST数据集压缩包文件到OBS中。上传文件至OBS的操作指导请参见[上传对象](#)。

**注意**

- 上传数据到OBS中时，请不要加密，否则会导致训练失败。
- 文件无需解压，直接上传压缩包至OBS中即可。

图 10-20 上传数据集到“mnist-data”文件夹中



3. 上传训练脚本“train.py”到“mnist-code”文件夹中。

图 10-21 上传训练脚本“train.py”到“mnist-code”文件夹中



4. 上传推理脚本“customize\_service.py”和推理配置文件“config.json”到“infer”文件中。

图 10-22 上传 “customize\_service.py” 和 “config.json” 到 “infer” 文件夹中



## 步骤 5：创建训练作业

1. 登录ModelArts管理控制台，选择和OBS桶相同的区域。
2. 在“全局配置”中检查当前账号是否已完成访问授权的配置。如未完成，请参考[使用委托授权](#)。针对之前使用访问密钥授权的用户，建议清空授权，然后使用委托进行授权。
3. 在左侧导航栏选择“训练管理 > 训练作业”进入训练作业页面，单击“创建训练作业”。
4. 填写创建训练作业相关信息。
  - “创建方式”：选择“自定义算法”。
  - “启动方式”：选择“预置框架”，下拉框中选择PyTorch，pytorch\_1.8.0-cuda\_10.2-py\_3.7-ubuntu\_18.04-x86\_64。
  - “代码目录”：选择已创建的OBS代码目录路径，例如“/test-modelarts-xx/pytorch/mnist-code/”（test-modelarts-xx需替换为您的OBS桶名称）。
  - “启动文件”：选择代码目录下上传的训练脚本“train.py”。
  - “输入”：单击“增加训练输入”，设置训练输入的“参数名称”为“data\_url”。设置数据存储位置为您的OBS目录，例如“/test-modelarts-xx/pytorch/mnist-data/”（test-modelarts-xx需替换为您的OBS桶名称）。
  - “输出”：单击“增加训练输出”，设置训练输出的“参数名称”为“train\_url”。设置数据存储位置为您的OBS目录，例如“/test-modelarts-xx/pytorch/mnist-output/”（test-modelarts-xx需替换为您的OBS桶名称）。预下载至本地目录选择“不下载”。



- “资源类型”：选择 GPU 单卡的规格。如果有免费GPU规格，可以选择免费规格进行训练。
- 其他参数保持默认即可。

**说明**

本样例代码为单机单卡场景，选择GPU多卡规格会导致训练失败。

**图 10-23 训练作业设置**

**图 10-24 训练输入和输入设置**

**图 10-25 资源类型设置**

5. 单击“提交”，确认训练作业的参数信息，确认无误后单击“确定”。  
页面自动返回“训练作业”列表页，当训练作业状态变为“已完成”时，即完成了模型训练过程。

**说明**

本案例的训练作业预计运行十分钟。

6. 单击训练作业名称，进入作业详情界面查看训练作业日志信息，观察日志是否有明显的Error信息，如果有则表示训练失败，请根据日志提示定位原因并解决。

7. 在训练详情页左下方单击训练输出路径（如图10-26），跳转到OBS目录，查看是否存在model文件夹，且model文件夹中是否有生成训练模型（如图10-27）。如果未生成model文件夹或者训练模型，可能是训练输入数据不完整导致，请检查训练数据上传是否完整，并重新训练。

图 10-26 训练输出路径

训练输入

| 输入路径                 | 训练参数...  | 获取方式 | 本地路径（训练参...    |
|----------------------|----------|------|----------------|
| /test-modelarts-x... | data_url | 超参   | /home/ma-us... |

训练输出

| 输出路径                 | 训练参数...   | 获取方式 | 本地路径（训练参...    |
|----------------------|-----------|------|----------------|
| /test-modelarts-x... | train_url | 超参   | /home/ma-us... |

图 10-27 训练生成的模型



## 步骤 6：推理部署

模型训练完成后，可以创建AI应用，将AI应用部署为在线服务。

1. 在ModelArts管理控制台，单击左侧导航栏中的“AI应用管理>AI应用”，进入“我的AI应用”页面，单击“创建”。
2. 在“创建AI应用”页面，填写相关参数，然后单击“立即创建”。

在“元模型来源”中，选择“从训练中选择”页签，选择**步骤5：创建训练作业**中完成的训练作业，勾选“动态加载”。AI引擎的值是系统自动写入的，无需设置。

图 10-28 设置元模型来源



3. 在AI应用列表页面，当AI应用状态变为“正常”时，表示AI应用创建成功。单击AI应用名称左侧的单选按钮，在列表页底部展开“版本列表”，单击操作列“部署>在线服务”，将AI应用部署为在线服务。

图 10-29 部署在线服务



4. 在“部署”页面，参考下图填写参数，然后根据界面提示完成在线服务创建。本案例适用于CPU规格，节点规格需选择CPU。如果有免费CPU规格，可选择免费规格进行部署（每名用户限部署一个免费的在线服务，如果您已经部署了一个免费在线服务，需要先将其删除才能部署新的免费在线服务）。

图 10-30 部署模型



完成服务部署后，返回在线服务页面列表页，等待服务部署完成，当服务状态显示为“运行中”，表示服务已部署成功。

图 10-31 部署成功



## 步骤 7：预测结果

1. 在“在线服务”页面，单击在线服务名称，进入服务详情页面。

- 单击“预测”页签，请求类型选择“multipart/form-data”，请求参数填写“image”，单击“上传”按钮上传示例图片，然后单击“预测”。

预测完成后，预测结果显示区域将展示预测结果，根据预测结果内容，可识别出此图片的数字是“2”。

### 📖 说明

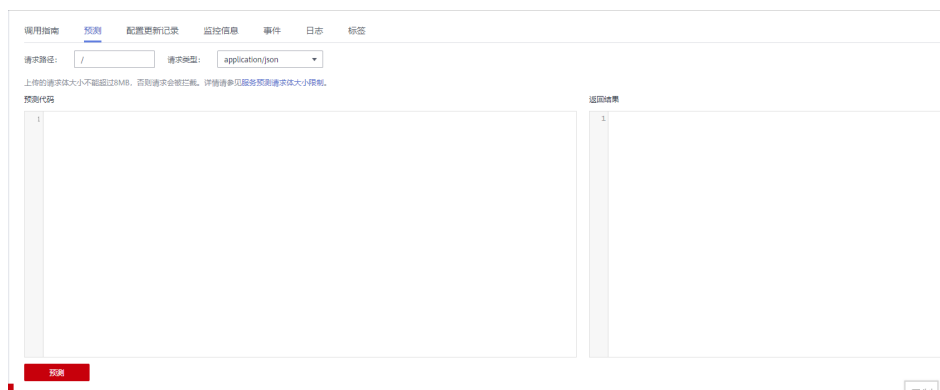
本案例中使用的MNIST是比较简单的用做demo的数据集，配套算法也是比较简单的用于教学的神经网络算法。这样的数据和算法生成的模型仅适用于教学模式，并不能应对复杂的预测场景。即生成的模型对预测图片有一定范围和要求，预测图片必须和训练集中的图片相似（黑底白字）才可能预测准确。

ModelArts的AI Gallery中提供了常见的精度较高的算法和相应的训练数据集，用户可以在[AI Gallery的资产集市](#)中获取。

图 10-32 示例图片



图 10-33 预测结果展示



## 步骤 8：清除资源

如果不再需要使用此模型及在线服务，建议清除相关资源，避免产生不必要的费用。

- 在“在线服务”页面，“停止”或“删除”刚创建的在线服务。
- 在“AI应用管理”页面，“删除”刚创建的AI应用。
- 在“训练作业”页面，“删除”运行结束的训练作业。
- 进入OBS，删除本示例使用的OBS桶及文件夹，以及文件夹的文件。

## 常见问题

- 训练作业一直在等待中（排队）？  
训练作业状态一直在等待中状态表示当前所选的资源池规格资源紧张，作业需要进行排队，请耐心等待。请参考[训练作业一直在等待中（排队）？](#)。
- 在ModelArts中选择OBS路径时，找不到已创建的OBS桶？  
请确保创建的桶和ModelArts服务在同一区域，详细操作请参考[查看OBS桶与ModelArts是否在同一区域](#)。

## 10.3 示例：从 0 到 1 制作自定义镜像并用于训练（Pytorch +CPU/GPU）

本章节介绍如何从0到1制作镜像，并使用该镜像在ModelArts平台上进行训练。镜像中使用的AI引擎是Pytorch，训练使用的资源是CPU或GPU。

### 📖 说明

本实践教程仅适用于新版训练作业。

### 场景描述

本示例使用 Linux x86\_64 架构的主机，操作系统ubuntu-18.04，通过编写 Dockerfile 文件制作自定义镜像。

目标：构建安装如下软件的容器镜像，并在ModelArts平台上使用CPU/GPU规格资源运行训练任务。

- ubuntu-18.04
- cuda-11.1
- python-3.7.13
- pytorch-1.8.1

### 操作流程

使用自定义镜像创建训练作业时，需要您熟悉 docker 软件的使用，并具备一定的开发经验。详细步骤如下所示：

1. [前提条件](#)
2. [Step1 创建OBS桶和文件夹](#)
3. [Step2 准备训练脚本并上传至OBS](#)
4. [Step3 准备镜像主机](#)
5. [Step4 制作自定义镜像](#)
6. [Step5 上传镜像至SWR服务](#)
7. [Step6 在ModelArts上创建训练作业](#)

### 前提条件

已注册华为账号并开通华为云，且在使用 ModelArts 前检查账号状态，账号不能处于欠费或冻结状态。

### Step1 创建 OBS 桶和文件夹

在 OBS 服务中创建桶和文件夹，用于存放样例数据集以及训练代码。需要创建的文件列表如[表10-1](#)所示，示例中的桶名称“test-modelarts”和文件夹名称均为举例，请替换为用户自定义的名称。

创建 OBS 桶和文件夹的操作指导请参见[创建桶](#)和[新建文件夹](#)。

请确保您使用的 OBS 与 ModelArts 在同一区域。

表 10-1 OBS 桶文件夹列表

| 文件夹名称                                     | 用途          |
|-------------------------------------------|-------------|
| “obs://test-modelarts/pytorch/demo-code/” | 用于存储训练脚本文件。 |
| “obs://test-modelarts/pytorch/log/”       | 用于存储训练日志文件。 |

## Step2 准备训练脚本并上传至 OBS

准备本案例所需的训练脚本pytorch-verification.py 文件，并上传至OBS桶的 “obs://test-modelarts/pytorch/demo-code/” 文件夹下。

pytorch-verification.py 文件内容如下：

```
import torch
import torch.nn as nn

x = torch.randn(5, 3)
print(x)

available_dev = torch.device("cuda") if torch.cuda.is_available() else torch.device("cpu")
y = torch.randn(5, 3).to(available_dev)
print(y)
```

## Step3 准备镜像主机

准备一台Linux x86\_64架构的主机，操作系统使用ubuntu-18.04。您可以准备相同规格的弹性云服务器ECS或者应用本地已有的主机进行自定义镜像的制作。

购买ECS服务器的具体操作请参考[购买并登录Linux弹性云服务器](#)。镜像选择公共镜像，推荐使用ubuntu18.04的镜像。

图 10-34 创建 ECS 服务器-选择 X86 架构的公共镜像



## Step4 制作自定义镜像

目标：构建安装好如下软件的容器镜像，并使用 ModelArts训练服务运行。

- ubuntu-18.04
- cuda-11.1
- python-3.7.13
- pytorch-1.8.1

此处介绍如何通过编写Dockerfile文件制作自定义镜像的操作步骤。

1. 安装Docker。

以Linux x86\_64架构的操作系统为例，获取Docker安装包。您可以执行以下指令安装Docker。关于安装Docker的更多指导内容参见 [Docker 官方文档](#)。

```
curl -fsSL get.docker.com -o get-docker.sh
sh get-docker.sh
```

如果 **docker images** 命令可以执行成功，表示 Docker 已安装，此步骤可跳过。

2. 执行如下命令确认Docker Engine版本。

```
docker version | grep -A 1 Engine
```

命令回显如下。

```
...
Engine:
Version: 18.09.0
```

 说明

推荐使用大于等于该版本的Docker Engine来制作自定义镜像。

3. 准备名为context的文件夹。

```
mkdir -p context
```

4. 准备可用的pip源文件pip.conf。本示例使用华为开源镜像站提供的pip源，其pip.conf文件内容如下。

```
[global]
index-url = https://repo.huaweicloud.com/repository/pypi/simple
trusted-host = repo.huaweicloud.com
timeout = 120
```

 说明

在华为开源镜像站 <https://mirrors.huaweicloud.com/home> 中，搜索 pypi，也可以查看 pip.conf 文件内容。

5. 下载torch\*.whl 文件。

在网站[https://download.pytorch.org/whl/torch\\_stable.html](https://download.pytorch.org/whl/torch_stable.html) 搜索并下载如下whl文件。

- torch-1.8.1+cu111-cp37-cp37m-linux\_x86\_64.whl
- torchaudio-0.8.1-cp37-cp37m-linux\_x86\_64.whl
- torchvision-0.9.1+cu111-cp37-cp37m-linux\_x86\_64.whl

 说明

+ 符号的 URL 编码为 %2B；在上述网站中搜索目标文件名时，需要将原文件名中的 + 符号替换为 %2B。

例如 torch-1.8.1%2Bcu111-cp37-cp37m-linux\_x86\_64.whl。

6. 下载Miniconda3安装文件。

使用地址[https://repo.anaconda.com/miniconda/Miniconda3-py37\\_4.12.0-Linux-x86\\_64.sh](https://repo.anaconda.com/miniconda/Miniconda3-py37_4.12.0-Linux-x86_64.sh)，下载Miniconda3 py37 4.12.0安装文件（对应python 3.7.13）。

7. 将上述pip 源文件、torch\*.whl 文件、Miniconda3安装文件放置在context文件夹内，context 文件夹内容如下。



```
context
├── Miniconda3-py37_4.12.0-Linux-x86_64.sh
├── pip.conf
├── torch-1.8.1+cu111-cp37-cp37m-linux_x86_64.whl
├── torchaudio-0.8.1-cp37-cp37m-linux_x86_64.whl
└── torchvision-0.9.1+cu111-cp37-cp37m-linux_x86_64.whl
```

## 8. 编写容器镜像Dockerfile文件。

在context文件夹内新建名为Dockerfile的空文件，并将下述内容写入其中。

```
容器镜像构建主机需要连通公网

基础容器镜像, https://github.com/NVIDIA/nvidia-docker/wiki/CUDA
#
https://docs.docker.com/develop/develop-images/multistage-build/#use-multi-stage-builds
require Docker Engine >= 17.05
#
builder stage
FROM nvidia/cuda:11.1.1-runtime-ubuntu18.04 AS builder

基础容器镜像的默认用户已经是 root
USER root

使用华为开源镜像站提供的 pypi 配置
RUN mkdir -p /root/.pip/
COPY pip.conf /root/.pip/pip.conf

复制待安装文件到基础容器镜像中的 /tmp 目录
COPY Miniconda3-py37_4.12.0-Linux-x86_64.sh /tmp
COPY torch-1.8.1+cu111-cp37-cp37m-linux_x86_64.whl /tmp
COPY torchvision-0.9.1+cu111-cp37-cp37m-linux_x86_64.whl /tmp
COPY torchaudio-0.8.1-cp37-cp37m-linux_x86_64.whl /tmp

https://conda.io/projects/conda/en/latest/user-guide/install/linux.html#installing-on-linux
安装 Miniconda3 到基础容器镜像的 /home/ma-user/miniconda3 目录中
RUN bash /tmp/Miniconda3-py37_4.12.0-Linux-x86_64.sh -b -p /home/ma-user/miniconda3

使用 Miniconda3 默认 python 环境 (即 /home/ma-user/miniconda3/bin/pip) 安装 torch*.whl
RUN cd /tmp && \
 /home/ma-user/miniconda3/bin/pip install --no-cache-dir \
 /tmp/torch-1.8.1+cu111-cp37-cp37m-linux_x86_64.whl \
 /tmp/torchvision-0.9.1+cu111-cp37-cp37m-linux_x86_64.whl \
 /tmp/torchaudio-0.8.1-cp37-cp37m-linux_x86_64.whl

构建最终容器镜像
FROM nvidia/cuda:11.1.1-runtime-ubuntu18.04

安装 vim和curl 工具 (依然使用华为开源镜像站)
RUN cp -a /etc/apt/sources.list /etc/apt/sources.list.bak && \
 sed -i "s@http://.*archive.ubuntu.com@http://repo.huaweicloud.com@g" /etc/apt/sources.list && \
 sed -i "s@http://.*security.ubuntu.com@http://repo.huaweicloud.com@g" /etc/apt/sources.list && \
 apt-get update && \
 apt-get install -y vim curl && \
 apt-get clean && \
 mv /etc/apt/sources.list.bak /etc/apt/sources.list

增加 ma-user 用户 (uid = 1000, gid = 100)
注意到基础容器镜像已存在 gid = 100 的组, 因此 ma-user 用户可直接使用
RUN useradd -m -d /home/ma-user -s /bin/bash -g 100 -u 1000 ma-user

从上述 builder stage 中复制 /home/ma-user/miniconda3 目录到当前容器镜像的同名目录
COPY --chown=ma-user:100 --from=builder /home/ma-user/miniconda3 /home/ma-user/miniconda3

设置容器镜像预置环境变量
请务必设置 PYTHONUNBUFFERED=1, 以免日志丢失
ENV PATH=$PATH:/home/ma-user/miniconda3/bin \
 PYTHONUNBUFFERED=1

设置容器镜像默认用户与工作目录
```

```
USER ma-user
WORKDIR /home/ma-user
```

关于Dockerfile文件编写的更多指导内容参见 [Docker 官方文档](#)。

9. 确认已创建完成Dockerfile文件。此时context文件夹内容如下。

```
context
├── Dockerfile
├── Miniconda3-py37_4.12.0-Linux-x86_64.sh
├── pip.conf
├── torch-1.8.1+cu111-cp37-cp37m-linux_x86_64.whl
├── torchaudio-0.8.1-cp37-cp37m-linux_x86_64.whl
└── torchvision-0.9.1+cu111-cp37-cp37m-linux_x86_64.whl
```

10. 构建容器镜像。在 Dockerfile文件所在的目录执行如下命令构建容器镜像 pytorch:1.8.1-cuda11.1。

```
docker build . -t pytorch:1.8.1-cuda11.1
```

构建过程结束时出现如下构建日志说明镜像构建成功。

```
Successfully tagged pytorch:1.8.1-cuda11.1
```

## Step5 上传镜像至 SWR 服务

1. 登录容器镜像服务控制台，选择区域。

图 10-35 容器镜像服务控制台



2. 单击右上角“创建组织”，输入组织名称完成组织创建。请自定义组织名称，本示例使用“deep-learning”，下面的命令中涉及到组织名称“deep-learning”也请替换为自定义的值。

图 10-36 创建组织

### 创建组织

1. 组织名称，全局唯一。
2. 当前租户最多可创建5个组织。
3. 建议一个组织对应一个公司、部门或个人，以便集中高效地管理镜像资源。

示例：

以公司、部门作为组织: cloud-hangzhou、cloud-develop

以个人作为组织: john

组织名称

3. 单击右上角“登录指令”，获取登录访问指令。

图 10-37 登录指令



4. 以root用户登录本地环境，输入登录访问指令。
5. 上传镜像至容器镜像服务镜像仓库。
  - a. 使用docker tag命令给上传镜像打标签。

```
#region和domain信息请替换为实际值，组织名称deep-learning也请替换为自定义的值。
sudo docker tag pytorch:1.8.1-cuda11.1 swr.{region-id}.{domain}/deep-learning/pytorch:1.8.1-cuda11.1
#此处以华为云cn-north-4为例
sudo docker tag pytorch:1.8.1-cuda11.1 swr.cn-north-4.myhuaweicloud.com/deep-learning/pytorch:1.8.1-cuda11.1
```
  - b. 使用docker push命令上传镜像。

```
#region和domain信息请替换为实际值，组织名称deep-learning也请替换为自定义的值。
sudo docker push swr.{region-id}.{domain}/deep-learning/pytorch:1.8.1-cuda11.1
#此处以华为云cn-north-4为例
sudo docker push swr.cn-north-4.myhuaweicloud.com/deep-learning/pytorch:1.8.1-cuda11.1
```
6. 完成镜像上传后，在容器镜像服务控制台的“我的镜像”页面可查看已上传的自定义镜像。  
“swr.cn-north-4.myhuaweicloud.com/deep-learning/pytorch:1.8.1-cuda11.1”即为此自定义镜像的“SWR\_URL”。

## Step6 在 ModelArts 上创建训练作业

1. 登录ModelArts管理控制台，检查当前账号是否已完成访问授权的配置。如未完成，请参考[使用委托授权](#)。针对之前使用访问密钥授权的用户，建议清空授权，然后使用委托进行授权。
2. 在左侧导航栏中选择“训练管理 > 训练作业”，默认进入“训练作业”列表。
3. 在“创建训练作业”页面，填写相关参数信息，然后单击“提交”。
  - 创建方式：选择“自定义算法”
  - 启动方式：选择“自定义”
  - 镜像地址：[Step5 上传镜像至SWR服务](#)中创建的镜像。“swr.cn-north-4.myhuaweicloud.com/deep-learning/pytorch:1.8.1-cuda11.1”
  - 代码目录：设置为OBS中存放启动脚本文件的目录，例如：“obs://test-modelarts/pytorch/demo-code/”，训练代码会被自动下载至训练容器的“\${MA\_JOB\_DIR}/demo-code”目录中，“demo-code”为OBS存放代码路径的最后一级目录，可以根据实际修改。
  - 启动命令：“/home/ma-user/miniconda3/bin/python \${MA\_JOB\_DIR}/demo-code/pytorch-verification.py”，此处的“demo-code”为用户自定义的OBS存放代码路径的最后一级目录，可以根据实际修改。
  - 资源池：选择公共资源池
  - 类型：选择GPU或者CPU规格。

- 永久保存日志：打开
  - 作业日志路径：设置为OBS中存放训练日志的路径。例如：“obs://test-modelarts/pytorch/log/”
4. 在“规格确认”页面，确认训练作业的参数信息，确认无误后单击“提交”。
  5. 训练作业创建完成后，后台将自动完成容器镜像下载、代码目录下载、执行启动命令等动作。

训练作业一般需要运行一段时间，根据您的训练业务逻辑和选择的资源不同，训练时长将持续几十分钟到几小时不等。训练作业执行成功后，日志信息如下所示。

图 10-38 GPU 规格运行日志信息



图 10-39 CPU 规格运行日志信息

```
 系统日志 | 当前日志文件0.01MB;

1 tensor([[0.8945, -0.6946, 0.3807],
2 [0.6665, 0.3133, 0.8285],
3 [-0.5353, -0.1730, -0.5419],
4 [0.4870, 0.5183, 0.2505],
5 [0.2679, -0.4996, 0.7919]])
6 tensor([[0.9692, 0.4652, 0.5659],
7 [2.2032, 1.4157, -0.1755],
8 [-0.6296, 0.5466, 0.6994],
9 [0.2353, -0.0089, -1.9546],
10 [0.9319, 1.1781, -0.4587]])
11
```

## 10.4 示例：从 0 到 1 制作自定义镜像并用于训练（MPI +CPU/GPU）

本章节介绍如何从0到1制作镜像，并使用该镜像在ModelArts平台上进行训练。镜像中使用的AI引擎是MPI，训练使用的资源是CPU或GPU。

### 说明

本实践教程仅适用于新版训练作业。

### 场景描述

本示例使用 Linux x86\_64 架构的主机，操作系统ubuntu-18.04，通过编写 Dockerfile 文件制作自定义镜像。

目标：构建安装如下软件的容器镜像，并在ModelArts平台上使用CPU/GPU规格资源运行训练任务。

- ubuntu-18.04
- cuda-11.1
- python-3.7.13
- openmpi-3.0.0

## 操作流程

使用自定义镜像创建训练作业时，需要您熟悉docker软件的使用，并具备一定的开发经验。详细步骤如下所示：

1. [前提条件](#)
2. [Step1 创建OBS桶和文件夹](#)
3. [Step2 准备脚本文件并上传至OBS中](#)
4. [Step3 准备镜像主机](#)
5. [Step4 制作自定义镜像](#)
6. [Step5 上传镜像至SWR服务](#)
7. [Step6 在ModelArts上创建训练作业](#)

## 前提条件

已注册华为账号并开通华为云，且在使用ModelArts前检查账号状态，账号不能处于欠费或冻结状态。

### Step1 创建 OBS 桶和文件夹

在OBS服务中创建桶和文件夹，用于存放样例数据集以及训练代码。需要创建的文件夹列表如表10-2所示，示例中的桶名称“test-modelarts”和文件夹名称均为举例，请替换为用户自定义的名称。

创建 OBS 桶和文件夹的操作指导请参见[创建桶](#)和[新建文件夹](#)。

请确保您使用的 OBS 与 ModelArts 在同一区域。

表 10-2 OBS 桶文件夹列表

| 文件夹名称                                 | 用途                    |
|---------------------------------------|-----------------------|
| “obs://test-modelarts/mpi/demo-code/” | 用于存储 MPI 启动脚本与训练脚本文件。 |
| “obs://test-modelarts/mpi/log/”       | 用于存储训练日志文件。           |

### Step2 准备脚本文件并上传至 OBS 中

准备本案例所需的MPI启动脚本run\_mpi.sh文件和训练脚本mpi-verification.py文件，并上传至OBS桶的“obs://test-modelarts/mpi/demo-code/”文件夹下。

- MPI启动脚本run\_mpi.sh文件内容如下：

```
#!/bin/bash
MY_HOME=/home/ma-user

MY_SSHD_PORT=${MY_SSHD_PORT:-"38888"}

MY_TASK_INDEX=${MA_TASK_INDEX:-${VC_TASK_INDEX:-${VK_TASK_INDEX}}}

MY_MPI_SLOTS=${MY_MPI_SLOTS:-"${MA_NUM_GPUS}"}

MY_MPI_TUNE_FILE="${MY_HOME}/env_for_user_process"
```

```
if [-z ${MY_MPI_SLOTS}]; then
 echo "[run_mpi] MY_MPI_SLOTS is empty, set it be 1"
 MY_MPI_SLOTS="1"
fi

printf "MY_HOME: ${MY_HOME}\nMY_SSHD_PORT: ${MY_SSHD_PORT}\nMY_MPI_BTL_TCP_IF: ${MY_MPI_BTL_TCP_IF}\nMY_TASK_INDEX: ${MY_TASK_INDEX}\nMY_MPI_SLOTS: ${MY_MPI_SLOTS}\n"

env | grep -E '^MA_|SHARED_|^S3_|^PATH|^VC_WORKER_|^SCC|^CRED' | grep -v '=' > ${MY_MPI_TUNE_FILE}
add -x to each line
sed -i 's/^-x /' ${MY_MPI_TUNE_FILE}

sed -i "s|${MY_SSHD_PORT}|${MY_SSHD_PORT}|g" ${MY_HOME}/etc/ssh/sshd_config

start sshd service
bash -c "$(which sshd) -f ${MY_HOME}/etc/ssh/sshd_config"

confirm the sshd is up
netstat -anp | grep LIS | grep ${MY_SSHD_PORT}

if [$MY_TASK_INDEX -eq 0]; then
 # generate the hostfile of mpi
 for ((i=0; i<${MA_NUM_HOSTS}; i++))
 do
 eval hostname=${MA_VJ_NAME}-${MA_TASK_NAME}-${i}.${MA_VJ_NAME}
 echo "[run_mpi] hostname: ${hostname}"

 ip=""
 while [-z "$ip"]; do
 ip=$(ping -c 1 ${hostname} | grep "PING" | sed -E 's/PING .* .([0-9.]+) .*/\1/g')
 sleep 1
 done
 echo "[run_mpi] resolved ip: ${ip}"

 # test the sshd is up
 while :
 do
 if [cat < /dev/null > /dev/tcp/${ip}/${MY_SSHD_PORT}]; then
 break
 fi
 sleep 1
 done

 echo "[run_mpi] the sshd of ip ${ip} is up"

 echo "${ip} slots=${MY_MPI_SLOTS}" >> ${MY_HOME}/hostfile
 done

 printf "[run_mpi] hostfile:\n`cat ${MY_HOME}/hostfile`\n"
fi

RET_CODE=0

if [$MY_TASK_INDEX -eq 0]; then

 echo "[run_mpi] start exec command time: "$(date +"%Y-%m-%d-%H:%M:%S")

 np=$((${MA_NUM_HOSTS} * ${MY_MPI_SLOTS}))

 echo "[run_mpi] command: mpirun -np ${np} -hostfile ${MY_HOME}/hostfile -mca plm_rsh_args \"-p ${MY_SSHD_PORT}\" -tune ${MY_MPI_TUNE_FILE} ... @$@"

 # execute mpirun at worker-0
 # mpirun
 mpirun \
 -np ${np} \
 -hostfile ${MY_HOME}/hostfile \
 -mca plm_rsh_args "-p ${MY_SSHD_PORT}" \
```

```
-tune ${MY_MPI_TUNE_FILE} \
-bind-to none -map-by slot \
-x NCCL_DEBUG -x NCCL_SOCKET_IFNAME -x NCCL_IB_HCA -x NCCL_IB_TIMEOUT -x
NCCL_IB_GID_INDEX -x NCCL_IB_TC \
-x HOROVOD_MPI_THREADS_DISABLE=1 \
-x PATH -x LD_LIBRARY_PATH \
-mca pml ob1 -mca btl ^openib -mca plm_rsh_no_tree_spawn true \
"$@"

RET_CODE=?

if [$RET_CODE -ne 0]; then
 echo "[run_mpi] exec command failed, exited with $RET_CODE"
else
 echo "[run_mpi] exec command successfully, exited with $RET_CODE"
fi

stop 1...N worker by killing the sleep proc
sed -i '1d' ${MY_HOME}/hostfile
if [`cat ${MY_HOME}/hostfile | wc -l` -ne 0]; then
 echo "[run_mpi] stop 1 to (N - 1) worker by killing the sleep proc"

 sed -i 's/${MY_MPI_SLOTS}/1/g' ${MY_HOME}/hostfile
 printf "[run_mpi] hostfile:\n`cat ${MY_HOME}/hostfile`\n"

 mpirun \
 --hostfile ${MY_HOME}/hostfile \
 --mca plm_rsh_args "-p ${MY_SSHD_PORT}" \
 -x PATH -x LD_LIBRARY_PATH \
 pkill sleep \
 > /dev/null 2>&1
fi

echo "[run_mpi] exit time: "$(date +"%Y-%m-%d-%H:%M:%S")"
else
 echo "[run_mpi] the training log is in worker-0"
 sleep 365d
 echo "[run_mpi] exit time: "$(date +"%Y-%m-%d-%H:%M:%S")"
fi

exit $RET_CODE
```

### 📖 说明

run\_mpi.sh脚本需要以LF作为换行符。使用CRLF作为换行符会导致训练作业运行失败，日志中会打印 '\$\r': command not found 的错误信息。

- 训练脚本mpi-verification.py文件内容如下：

```
import os
import socket

if __name__ == '__main__':
 print(socket.gethostname())

https://www.open-mpi.org/faq/?category=running#mpi-environmental-variables
print('OMPI_COMM_WORLD_SIZE: ' + os.environ['OMPI_COMM_WORLD_SIZE'])
print('OMPI_COMM_WORLD_RANK: ' + os.environ['OMPI_COMM_WORLD_RANK'])
print('OMPI_COMM_WORLD_LOCAL_RANK: ' + os.environ['OMPI_COMM_WORLD_LOCAL_RANK'])
```

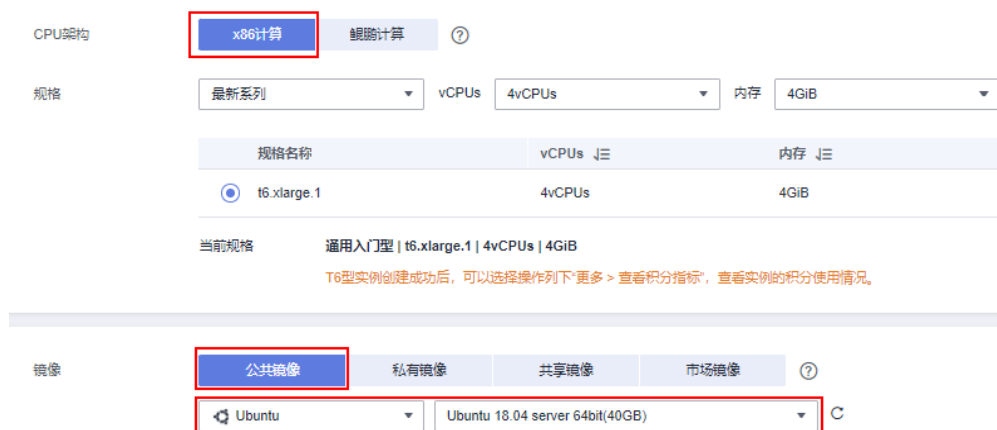
## Step3 准备镜像主机

准备一台Linux x86\_64架构的主机，操作系统使用ubuntu-18.04。您可以准备相同规格的弹性云服务器ECS或者应用本地已有的主机进行自定义镜像的制作。

购买ECS服务器的具体操作请参考[购买并登录Linux弹性云服务器](#)。镜像选择公共镜像，推荐使用ubuntu18.04的镜像。



图 10-40 创建 ECS 服务器-选择 X86 架构的公共镜像



## Step4 制作自定义镜像

目标：构建安装好如下软件的容器镜像，并使用 ModelArts 训练服务运行。

- ubuntu-18.04
- cuda-11.1
- python-3.7.13
- openmpi-3.0.0

此处介绍如何通过编写 Dockerfile 文件制作自定义镜像的操作步骤。

### 1. 安装Docker。

以 Linux x86\_64架构的操作系统为例，获取 Docker 安装包。您可以使用以下指令安装Docker。关于安装Docker的更多指导内容参见 [Docker 官方文档](#)。

```
curl -fsSL get.docker.com -o get-docker.sh
sh get-docker.sh
```

如果 **docker images** 命令可以执行成功，表示 Docker 已安装，此步骤可跳过。

### 2. 确认Docker Engine版本。执行如下命令。

```
docker version | grep -A 1 Engine
```

命令回显如下。

```
Engine:
Version: 18.09.0
```

### 📖 说明

推荐使用大于等于该版本的 Docker Engine 来制作自定义镜像。

### 3. 准备名为 context 的文件夹。

```
mkdir -p context
```

### 4. 下载 Miniconda3 安装文件。

使用地址 [https://repo.anaconda.com/miniconda/Miniconda3-py37\\_4.12.0-Linux-x86\\_64.sh](https://repo.anaconda.com/miniconda/Miniconda3-py37_4.12.0-Linux-x86_64.sh)，下载Miniconda3 py37 4.12.0安装文件（对应 python 3.7.13）。

### 5. 下载 openmpi 3.0.0安装文件。

使用地址<https://github.com/horovod/horovod/files/1596799/openmpi-3.0.0-bin.tar.gz>，下载 horovod v0.22.1已经编译好的 openmpi 3.0.0 文件。

6. 将上述Miniconda3安装文件、openmpi 3.0.0文件放置在context文件夹内，context 文件夹内容如下。

```
context
├── Miniconda3-py37_4.12.0-Linux-x86_64.sh
└── openmpi-3.0.0-bin.tar.gz
```

7. 编写容器镜像Dockerfile文件。

在context 文件夹内新建名为Dockerfile 的空文件，并将下述内容写入其中。

```
容器镜像构建主机需要连通公网

基础容器镜像, https://github.com/NVIDIA/nvidia-docker/wiki/CUDA
#
https://docs.docker.com/develop/develop-images/multistage-build/#use-multi-stage-builds
require Docker Engine >= 17.05
#
builder stage
FROM nvidia/cuda:11.1.1-runtime-ubuntu18.04 AS builder

基础容器镜像的默认用户已经是 root
USER root

复制 Miniconda3 (python 3.7.13) 安装文件到基础容器镜像中的 /tmp 目录
COPY Miniconda3-py37_4.12.0-Linux-x86_64.sh /tmp

安装 Miniconda3 到基础容器镜像的 /home/ma-user/miniconda3 目录中
https://conda.io/projects/conda/en/latest/user-guide/install/linux.html#installing-on-linux
RUN bash /tmp/Miniconda3-py37_4.12.0-Linux-x86_64.sh -b -p /home/ma-user/miniconda3

构建最终容器镜像
FROM nvidia/cuda:11.1.1-runtime-ubuntu18.04

安装 vim / curl / net-tools / ssh 工具 (依然使用华为开源镜像站)
RUN cp -a /etc/apt/sources.list /etc/apt/sources.list.bak && \
 sed -i "s@http://.*archive.ubuntu.com@http://repo.huaweicloud.com@g" /etc/apt/sources.list && \
 sed -i "s@http://.*security.ubuntu.com@http://repo.huaweicloud.com@g" /etc/apt/sources.list && \
 echo > /etc/apt/apt.conf.d/00skip-verify-peer.conf "Acquire { https::Verify-Peer false }" && \
 apt-get update && \
 apt-get install -y vim curl net-tools iputils-ping \
 openssh-client openssh-server && \
 ssh -V && \
 mkdir -p /run/ssh && \
 apt-get clean && \
 mv /etc/apt/sources.list.bak /etc/apt/sources.list && \
 rm /etc/apt/apt.conf.d/00skip-verify-peer.conf

安装 horovod v0.22.1 已经编译好的 openmpi 3.0.0 文件
https://github.com/horovod/horovod/blob/v0.22.1/docker/horovod/Dockerfile
https://github.com/horovod/horovod/files/1596799/openmpi-3.0.0-bin.tar.gz
COPY openmpi-3.0.0-bin.tar.gz /tmp
RUN cd /usr/local && \
 tar -zxf /tmp/openmpi-3.0.0-bin.tar.gz && \
 ldconfig && \
 mpirun --version

增加 ma-user 用户 (uid = 1000, gid = 100)
注意到基础容器镜像已存在 gid = 100 的组, 因此 ma-user 用户可直接使用
RUN useradd -m -d /home/ma-user -s /bin/bash -g 100 -u 1000 ma-user

从上述 builder stage 中复制 /home/ma-user/miniconda3 目录到当前容器镜像的同名目录
COPY --chown=ma-user:100 --from=builder /home/ma-user/miniconda3 /home/ma-user/miniconda3

设置容器镜像预置环境变量
请务必设置 PYTHONUNBUFFERED=1, 以免日志丢失
ENV PATH=$PATH:/home/ma-user/miniconda3/bin \
 PYTHONUNBUFFERED=1

设置容器镜像默认用户与工作目录
USER ma-user
WORKDIR /home/ma-user
```

```
配置 sshd, 使得 ssh 可以免密登录
RUN MA_HOME=/home/ma-user && \
 # setup sshd dir
 mkdir -p ${MA_HOME}/etc && \
 ssh-keygen -f ${MA_HOME}/etc/ssh_host_rsa_key -N "" -t rsa && \
 mkdir -p ${MA_HOME}/etc/ssh ${MA_HOME}/var/run && \
 # setup sshd config (listen at {{MY_SSHD_PORT}} port)
 echo "Port {{MY_SSHD_PORT}}\n\
HostKey ${MA_HOME}/etc/ssh_host_rsa_key\n\
AuthorizedKeysFile ${MA_HOME}/.ssh/authorized_keys\n\
PidFile ${MA_HOME}/var/run/sshd.pid\n\
StrictModes no\n\
UsePAM no" > ${MA_HOME}/etc/ssh/sshd_config && \
 # generate ssh key
 ssh-keygen -t rsa -f ${MA_HOME}/.ssh/id_rsa -P "" && \
 cat ${MA_HOME}/.ssh/id_rsa.pub >> ${MA_HOME}/.ssh/authorized_keys && \
 # disable ssh host key checking for all hosts
 echo "Host *\n\
StrictHostKeyChecking no" > ${MA_HOME}/.ssh/config
```

关于 Dockerfile 文件编写的更多指导内容参见 [Docker 官方文档](#)。

8. 确认已创建完成 Dockerfile 文件。此时 context 文件夹内容如下。

```
context
├── Dockerfile
├── Miniconda3-py37_4.12.0-Linux-x86_64.sh
└── openmpi-3.0.0-bin.tar.gz
```

9. 构建容器镜像。在 Dockerfile 文件所在的目录执行如下命令构建容器镜像 mpi:3.0.0-cuda11.1。

```
docker build . -t mpi:3.0.0-cuda11.1
```

构建过程结束时出现如下构建日志说明镜像构建成功。

```
naming to docker.io/library/mpi:3.0.0-cuda11.1
```

## Step5 上传镜像至 SWR 服务

1. 登录容器镜像服务控制台，选择区域。

图 10-41 容器镜像服务控制台



2. 单击右上角“创建组织”，输入组织名称完成组织创建。请自定义组织名称，本示例使用“deep-learning”，下面的命令中涉及到组织名称“deep-learning”也请替换为自定义的值。

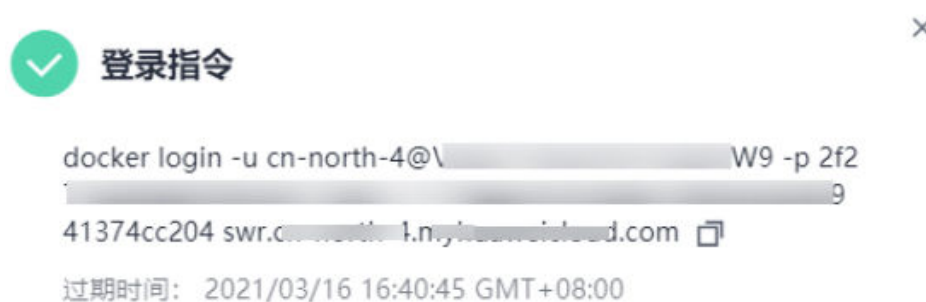
图 10-42 创建组织

### 创建组织



- 单击右上角“登录指令”，获取登录访问指令。

图 10-43 登录指令



- 以root用户登录本地环境，输入登录访问指令。
- 上传镜像至容器镜像服务镜像仓库。
  - 使用docker tag命令给上传镜像打标签。  
#region和domain信息请替换为实际值，组织名称deep-learning也请替换为自定义的值。  

```
sudo docker tag mpi:3.0.0-cuda11.1 swr.cn-north-4.myhuaweicloud.com/deep-learning/mpi:3.0.0-cuda11.1
```
  - 使用docker push命令上传镜像。  
#region和domain信息请替换为实际值，组织名称deep-learning也请替换为自定义的值。  

```
sudo docker push swr.cn-north-4.myhuaweicloud.com/deep-learning/mpi:3.0.0-cuda11.1
```
- 完成镜像上传后，在“容器镜像服务控制台>我的镜像”页面可查看已上传的自定义镜像。  
“swr.cn-north-4.myhuaweicloud.com/deep-learning/mpi:3.0.0-cuda11.1”即为此自定义镜像的“SWR\_URL”。

## Step6 在 ModelArts 上创建训练作业

- 登录ModelArts管理控制台，检查当前账号是否已完成访问授权的配置。如未完成，请参考[使用委托授权](#)。针对之前使用访问密钥授权的用户，建议清空授权，然后使用委托进行授权。
- 在ModelArts管理控制台，左侧导航栏中选择“训练管理 > 训练作业 New”，默认进入“训练作业”列表。

3. 在“创建训练作业”页面，填写相关参数信息，然后单击“提交”。
  - 创建方式：选择“自定义算法”
  - 启动方式：选择“自定义”
  - 镜像地址：“swr.cn-north-4.myhuaweicloud.com/deep-learning/mpi:3.0.0-cuda11.1”
  - 代码目录：设置为OBS中存放启动脚本文件的目录，例如：“obs://test-modelarts/mpi/demo-code/”
  - 启动命令：bash \${MA\_JOB\_DIR}/demo-code/run\_mpi.sh python \${MA\_JOB\_DIR}/demo-code/mpi-verification.py
  - 环境变量：添加 MY\_SSHD\_PORT = 38888

图 10-44 添加环境变量示意



- 资源池：选择公共资源池
  - 类型：选择GPU规格
  - 计算节点个数：选择 1或 2
  - 永久保存日志：打开
  - 作业日志路径：设置为OBS中存放训练日志的路径。例如：“obs://test-modelarts/mpi/log/”
4. 在“规格确认”页面，确认训练作业的参数信息，确认无误后单击“提交”。
  5. 训练作业创建完成后，后台将自动完成容器镜像下载、代码目录下载、执行启动命令等动作。

训练作业一般需要运行一段时间，根据您的训练业务逻辑和选择的资源不同，训练时长将持续几十分钟到几小时不等。训练作业执行成功后，日志信息如图10-45所示。

图 10-45 1 个计算节点 GPU 规格 worker-0 运行日志信息

```

MY_HOME: /home/ma-user
MY_SSHD_PORT: 38888
MY_MPI_BTL_TCP_IF: eth0,bond0
MY_TASK_INDEX: 0
MY_MPI_SLOTS: 1
tcp 0 0 0.0.0.0:38888 0.0.0.0:* LISTEN 60/sshd
tcp6 0 0 :::38888 :::* LISTEN 60/sshd
172.16.0.122 s1ots=1
modelarts-job-8cf8a682-21cb-4d73-9bb3-789cecdc458b-worker-0
OMPI_COMM_WORLD_SIZE: 1
OMPI_COMM_WORLD_RANK: 0
OMPI_COMM_WORLD_LOCAL_RANK: 0

```

计算节点个数选择为 2，训练作业也可以运行。日志信息如图10-46和图10-47所示。

图 10-46 2 个计算节点 worker-0 运行日志信息

```

MY_HOME: /home/ma-user
MY_SSHD_PORT: 38888
MY_MPI_BTL_TCP_IF: eth0,bond0
MY_TASK_INDEX: 0
MY_MPI_SLOTS: 1
tcp 0 0 0.0.0.0:38888 0.0.0.0:* LISTEN 61/sshd
tcp6 0 0 :::38888 :::* LISTEN 61/sshd
172.16.0.39 slots=1
172.16.0.123 slots=1
Warning: Permanently added '[172.16.0.123]:38888' (RSA) to the list of known hosts.
modelarts-job-31732752-6857-4e33-96ff-7a28afae26fb-worker-0
OMPI_COMM_WORLD_SIZE: 2
OMPI_COMM_WORLD_RANK: 0
OMPI_COMM_WORLD_LOCAL_RANK: 0
modelarts-job-31732752-6857-4e33-96ff-7a28afae26fb-worker-1
OMPI_COMM_WORLD_SIZE: 2
OMPI_COMM_WORLD_RANK: 1
OMPI_COMM_WORLD_LOCAL_RANK: 0

```

图 10-47 2 个计算节点 worker-1 运行日志信息

```

MY_HOME: /home/ma-user
MY_SSHD_PORT: 38888
MY_MPI_BTL_TCP_IF: eth0,bond0
MY_TASK_INDEX: 1
MY_MPI_SLOTS: 1
tcp 0 0 0.0.0.0:38888 0.0.0.0:* LISTEN 62/sshd
tcp6 0 0 :::38888 :::* LISTEN 62/sshd
/home/ma-user/modelarts/user-job-dir/xxx/run_mpi.sh: line 109: 66 Terminated sleep 365d

```

## 10.5 示例：从 0 到 1 制作自定义镜像并用于训练 (Horovod-PyTorch+GPU)

本章节介绍如何从 0 到 1 制作镜像，并使用该镜像在 ModelArts 平台上进行训练。镜像中使用的 AI 引擎是 Horovod 0.22.1 + Pytorch 1.8.1，训练使用的资源是 GPU。

### 📖 说明

本实践教程仅适用于新版训练作业。

### 场景描述

本示例使用Linux x86\_64架构的主机，操作系统ubuntu-18.04，通过编写 Dockerfile 文件制作自定义镜像。

目标：构建安装如下软件的容器镜像，并在 ModelArts 平台上使用 CPU/GPU 规格资源运行训练任务。

- ubuntu-18.04
- cuda-11.1
- python-3.7.13
- mlnx ofed-5.4
- pytorch-1.8.1
- horovod-0.22.1

## 操作流程

使用自定义镜像创建训练作业时，需要您熟悉 docker 软件的使用，并具备一定的开发经验。详细步骤如下所示：

1. [前提条件](#)
2. [Step1 创建OBS桶和文件夹](#)
3. [Step2 准备训练脚本并上传至OBS](#)
4. [Step3 准备镜像主机](#)
5. [Step4 制作自定义镜像](#)
6. [Step5 上传镜像至SWR服务](#)
7. [Step6 在ModelArts上创建训练作业](#)

## 前提条件

已注册华为账号并开通华为云，且在使用 ModelArts前检查账号状态，账号不能处于欠费或冻结状态。

### Step1 创建 OBS 桶和文件夹

在 OBS 服务中创建桶和文件夹，用于存放样例数据集以及训练代码。需要创建的文件夹列表如表10-3所示，示例中的桶名称“test-modelarts”和文件夹名称均为举例，请替换为用户自定义的名称。

创建 OBS 桶和文件夹的操作指导请参见[创建桶](#)和[新建文件夹](#)。

请确保您使用的 OBS 与 ModelArts 在同一区域。

表 10-3 OBS 桶文件夹列表

| 文件夹名称                                     | 用途          |
|-------------------------------------------|-------------|
| “obs://test-modelarts/pytorch/demo-code/” | 用于存储训练脚本文件。 |
| “obs://test-modelarts/pytorch/log/”       | 用于存储训练日志文件。 |

### Step2 准备训练脚本并上传至 OBS

准备本案例所需的训练脚本pytorch\_synthetic\_benchmark.py和run\_mpi.sh文件，并上传至OBS桶的“obs://test-modelarts/horovod/demo-code/”文件夹下。

pytorch\_synthetic\_benchmark.py文件内容如下：

```
import argparse
import torch.backends.cudnn as cudnn
import torch.nn.functional as F
import torch.optim as optim
import torch.utils.data.distributed
from torchvision import models
import horovod.torch as hvd
import timeit
import numpy as np
```

```
Benchmark settings
parser = argparse.ArgumentParser(description='PyTorch Synthetic Benchmark',
 formatter_class=argparse.ArgumentDefaultsHelpFormatter)
parser.add_argument('--fp16-allreduce', action='store_true', default=False,
 help='use fp16 compression during allreduce')

parser.add_argument('--model', type=str, default='resnet50',
 help='model to benchmark')
parser.add_argument('--batch-size', type=int, default=32,
 help='input batch size')

parser.add_argument('--num-warmup-batches', type=int, default=10,
 help='number of warm-up batches that don\'t count towards benchmark')
parser.add_argument('--num-batches-per-iter', type=int, default=10,
 help='number of batches per benchmark iteration')
parser.add_argument('--num-iters', type=int, default=10,
 help='number of benchmark iterations')

parser.add_argument('--no-cuda', action='store_true', default=False,
 help='disables CUDA training')

parser.add_argument('--use-adasum', action='store_true', default=False,
 help='use adasum algorithm to do reduction')

args = parser.parse_args()
args.cuda = not args.no_cuda and torch.cuda.is_available()

hvd.init()

if args.cuda:
 # Horovod: pin GPU to local rank.
 torch.cuda.set_device(hvd.local_rank())

cudnn.benchmark = True

Set up standard model.
model = getattr(models, args.model)()

By default, Adasum doesn't need scaling up learning rate.
lr_scaler = hvd.size() if not args.use_adasum else 1

if args.cuda:
 # Move model to GPU.
 model.cuda()
 # If using GPU Adasum allreduce, scale learning rate by local_size.
 if args.use_adasum and hvd.nccl_built():
 lr_scaler = hvd.local_size()

optimizer = optim.SGD(model.parameters(), lr=0.01 * lr_scaler)

Horovod: (optional) compression algorithm.
compression = hvd.Compression.fp16 if args.fp16_allreduce else hvd.Compression.none

Horovod: wrap optimizer with DistributedOptimizer.
optimizer = hvd.DistributedOptimizer(optimizer,
 named_parameters=model.named_parameters(),
 compression=compression,
 op=hvd.Adasum if args.use_adasum else hvd.Average)

Horovod: broadcast parameters & optimizer state.
hvd.broadcast_parameters(model.state_dict(), root_rank=0)
hvd.broadcast_optimizer_state(optimizer, root_rank=0)

Set up fixed fake data
data = torch.randn(args.batch_size, 3, 224, 224)
target = torch.LongTensor(args.batch_size).random_() % 1000
if args.cuda:
 data, target = data.cuda(), target.cuda()
```



```
def benchmark_step():
 optimizer.zero_grad()
 output = model(data)
 loss = F.cross_entropy(output, target)
 loss.backward()
 optimizer.step()

def log(s, nl=True):
 if hvd.rank() != 0:
 return
 print(s, end='\n' if nl else '')

log('Model: %s' % args.model)
log('Batch size: %d' % args.batch_size)
device = 'GPU' if args.cuda else 'CPU'
log('Number of %ss: %d' % (device, hvd.size()))

Warm-up
log('Running warmup...')
timeit.timeit(benchmark_step, number=args.num_warmup_batches)

Benchmark
log('Running benchmark...')
img_secs = []
for x in range(args.num_iters):
 time = timeit.timeit(benchmark_step, number=args.num_batches_per_iter)
 img_sec = args.batch_size * args.num_batches_per_iter / time
 log('Iter #%d: %.1f img/sec per %s' % (x, img_sec, device))
 img_secs.append(img_sec)

Results
img_sec_mean = np.mean(img_secs)
img_sec_conf = 1.96 * np.std(img_secs)
log('Img/sec per %s: %.1f +-%.1f' % (device, img_sec_mean, img_sec_conf))
log('Total img/sec on %d %s(s): %.1f +-%.1f' %
 (hvd.size(), device, hvd.size() * img_sec_mean, hvd.size() * img_sec_conf))
```

run\_mpi.sh文件内容如下:

```
#!/bin/bash
MY_HOME=/home/ma-user

MY_SSHD_PORT=${MY_SSHD_PORT:-"36666"}

MY_MPI_BTL_TCP_IF=${MY_MPI_BTL_TCP_IF:-"eth0,bond0"}

MY_TASK_INDEX=${MA_TASK_INDEX:-${VC_TASK_INDEX:-${VK_TASK_INDEX}}}

MY_MPI_SLOTS=${MY_MPI_SLOTS:-"${MA_NUM_GPUS}"}

MY_MPI_TUNE_FILE="${MY_HOME}/env_for_user_process"

if [-z ${MY_MPI_SLOTS}]; then
 echo "[run_mpi] MY_MPI_SLOTS is empty, set it be 1"
 MY_MPI_SLOTS="1"
fi

printf "MY_HOME: ${MY_HOME}\nMY_SSHD_PORT: ${MY_SSHD_PORT}\nMY_MPI_BTL_TCP_IF: $
{MY_MPI_BTL_TCP_IF}\nMY_TASK_INDEX: ${MY_TASK_INDEX}\nMY_MPI_SLOTS: ${MY_MPI_SLOTS}\n"

env | grep -E '^MA_[SHARED_]^[S3_]^[PATH|^VC_WORKER|^SCC|^CRED' | grep -v '=' > $
{MY_MPI_TUNE_FILE}
add -x to each line
sed -i 's/^\-x /' ${MY_MPI_TUNE_FILE}

sed -i 's|{MY_SSHD_PORT}|{MY_SSHD_PORT}|g' ${MY_HOME}/etc/ssh/sshd_config
```

```
start sshd service
bash -c "$(which sshd) -f ${MY_HOME}/etc/ssh/sshd_config"

confirm the sshd is up
netstat -anp | grep LIS | grep ${MY_SSHD_PORT}

if [$MY_TASK_INDEX -eq 0]; then
 # generate the hostfile of mpi
 for ((i=0; i<${MA_NUM_HOSTS}; i++))
 do
 eval hostname=${MA_VJ_NAME}-${MA_TASK_NAME}-${i}-${MA_VJ_NAME}
 echo "[run_mpi] hostname: ${hostname}"

 ip=""
 while [-z "$ip"]; do
 ip=$(ping -c 1 ${hostname} | grep "PING" | sed -E 's/PING .* \.[0-9.]+. */\1/g')
 sleep 1
 done
 echo "[run_mpi] resolved ip: ${ip}"

 # test the sshd is up
 while :
 do
 if [cat < /dev/null >/dev/tcp/${ip}/${MY_SSHD_PORT}]; then
 break
 fi
 sleep 1
 done

 echo "[run_mpi] the sshd of ip ${ip} is up"

 echo "${ip} slots=${MY_MPI_SLOTS}" >> ${MY_HOME}/hostfile
 done

 printf "[run_mpi] hostfile:\n`cat ${MY_HOME}/hostfile`\n"
fi

RET_CODE=0

if [$MY_TASK_INDEX -eq 0]; then

 echo "[run_mpi] start exec command time: "$(date +"%Y-%m-%d-%H:%M:%S")

 np=$((${MA_NUM_HOSTS} * ${MY_MPI_SLOTS}))

 echo "[run_mpi] command: mpirun -np ${np} -hostfile ${MY_HOME}/hostfile -mca plm_rsh_args \"-p $
${MY_SSHD_PORT}\" -tune ${MY_MPI_TUNE_FILE} ... @$"

 # execute mpirun at worker-0
 # mpirun
 mpirun \
 -np ${np} \
 -hostfile ${MY_HOME}/hostfile \
 -mca plm_rsh_args "-p ${MY_SSHD_PORT}" \
 -tune ${MY_MPI_TUNE_FILE} \
 -bind-to none -map-by slot \
 -x NCCL_DEBUG=INFO -x NCCL_SOCKET_IFNAME=${MY_MPI_BTL_TCP_IF} -x
NCCL_SOCKET_FAMILY=AF_INET \
 -x HOROVOD_MPI_THREADS_DISABLE=1 \
 -x LD_LIBRARY_PATH \
 -mca pml ob1 -mca btl ^openib -mca plm_rsh_no_tree_spawn true \
 "$@"

 RET_CODE=$?

 if [$RET_CODE -ne 0]; then
 echo "[run_mpi] exec command failed, exited with $RET_CODE"
 else

```

```

echo "[run_mpi] exec command successfully, exited with $RET_CODE"
fi

stop 1...N worker by killing the sleep proc
sed -i '1d' ${MY_HOME}/hostfile
if [`cat ${MY_HOME}/hostfile | wc -l` -ne 0]; then
 echo "[run_mpi] stop 1 to (N - 1) worker by killing the sleep proc"

 sed -i 's/${MY_MPI_SLOTS}/1/g' ${MY_HOME}/hostfile
 printf "[run_mpi] hostfile:\n`cat ${MY_HOME}/hostfile`\n"

 mpirun \
 --hostfile ${MY_HOME}/hostfile \
 --mca btl_tcp_if_include ${MY_MPI_BTL_TCP_IF} \
 --mca plm_rsh_args "-p ${MY_SSHD_PORT}" \
 -x PATH -x LD_LIBRARY_PATH \
 pkill sleep \
 > /dev/null 2>&1
fi

echo "[run_mpi] exit time: "$(date +"%Y-%m-%d-%H:%M:%S")
else
echo "[run_mpi] the training log is in worker-0"
sleep 365d
echo "[run_mpi] exit time: "$(date +"%Y-%m-%d-%H:%M:%S")
fi

exit $RET_CODE

```

### Step3 准备镜像主机

准备一台 Linux x86\_64 架构的主机，操作系统使用 ubuntu-18.04。您可以准备相同规格的 弹性云服务器 ECS 或者应用本地已有的主机进行自定义镜像的制作。

购买ECS服务器的具体操作请参考[购买并登录Linux弹性云服务器](#)。镜像选择公共镜像，推荐使用ubuntu18.04的镜像。

图 10-48 创建 ECS 服务器-选择 X86 架构的公共镜像



### Step4 制作自定义镜像

目标：构建安装好如下软件的容器镜像，并使用 ModelArts 训练服务运行。

- ubuntu-18.04
- cuda-11.1

- python-3.7.13
- mlnx ofed-5.4
- pytorch-1.8.1
- horovod-0.22.1

此处介绍如何通过编写 Dockerfile 文件制作自定义镜像的操作步骤。

#### 1. 安装 Docker。

以 Linux x86\_64 架构的操作系统为例，获取 Docker 安装包。您可以使用以下指令安装 Docker。关于安装 Docker 的更多指导内容参见 [Docker 官方文档](#)。

```
curl -fsSL get.docker.com -o get-docker.sh
sh get-docker.sh
```

如果 `docker images` 命令可以执行成功，表示 Docker 已安装，此步骤可跳过。

#### 2. 确认 Docker Engine 版本。执行如下命令。

```
docker version | grep -A 1 Engine
```

命令回显如下。

```
Engine:
Version: 18.09.0
```

#### 📖 说明

推荐使用大于等于该版本的 Docker Engine 来制作自定义镜像。

#### 3. 准备名为 context 的文件夹。

```
mkdir -p context
```

#### 4. 准备可用的 pip 源文件 pip.conf。本示例使用华为开源镜像站提供的 pip 源，其 pip.conf 文件内容如下。

```
[global]
index-url = https://repo.huaweicloud.com/repository/pypi/simple
trusted-host = repo.huaweicloud.com
timeout = 120
```

#### 📖 说明

在华为开源镜像站 <https://mirrors.huaweicloud.com/home> 中，搜索 pypi，也可以查看 pip.conf 文件内容。

#### 5. 下载 horovod 源码文件。

进入网站 <https://pypi.org/project/horovod/0.22.1/#files>，下载 horovod-0.22.1.tar.gz 文件。

#### 6. 下载 torch\*.whl 文件。

在网站 [https://download.pytorch.org/whl/torch\\_stable.html](https://download.pytorch.org/whl/torch_stable.html) 搜索并下载如下 whl 文件。

- torch-1.8.1+cu111-cp37-cp37m-linux\_x86\_64.whl
- torchaudio-0.8.1-cp37-cp37m-linux\_x86\_64.whl
- torchvision-0.9.1+cu111-cp37-cp37m-linux\_x86\_64.whl

#### 📖 说明

+ 符号的 URL 编码为 %2B；在上述网站中搜索目标文件名时，需要将原文件名中的 + 符号替换为 %2B。

例如 torch-1.8.1%2Bcu111-cp37-cp37m-linux\_x86\_64.whl。

#### 7. 下载 Miniconda3 安装文件。

使用地址 [https://repo.anaconda.com/miniconda/Miniconda3-py37\\_4.12.0-Linux-x86\\_64.sh](https://repo.anaconda.com/miniconda/Miniconda3-py37_4.12.0-Linux-x86_64.sh)，下载 Miniconda3 py37 4.12.0 安装文件（对应 python 3.7.13）。

#### 8. 编写容器镜像Dockerfile文件。

在 context 文件夹内新建名为Dockerfile的空文件，并将下述内容写入其中。

```
容器镜像构建主机需要连通公网

基础容器镜像, https://github.com/NVIDIA/nvidia-docker/wiki/CUDA
#
https://docs.docker.com/develop/develop-images/multistage-build/#use-multi-stage-builds
require Docker Engine >= 17.05
#
builder stage
FROM nvidia/cuda:11.1.1-devel-ubuntu18.04 AS builder

安装 cmake 工具（使用华为开源镜像站）
RUN cp -a /etc/apt/sources.list /etc/apt/sources.list.bak && \
 sed -i "s@http://.*archive.ubuntu.com@http://repo.huaweicloud.com@g" /etc/apt/sources.list && \
 sed -i "s@http://.*security.ubuntu.com@http://repo.huaweicloud.com@g" /etc/apt/sources.list && \
 echo > /etc/apt/apt.conf.d/00skip-verify-peer.conf "Acquire { https::Verify-Peer false }" && \
 apt-get update && \
 apt-get install -y build-essential cmake g++-7 && \
 apt-get clean && \
 mv /etc/apt/sources.list.bak /etc/apt/sources.list && \
 rm /etc/apt/apt.conf.d/00skip-verify-peer.conf

基础容器镜像的默认用户已经是 root
USER root

使用华为开源镜像站提供的 pypi 配置
RUN mkdir -p /root/.pip/
COPY pip.conf /root/.pip/pip.conf

复制待安装文件到基础容器镜像中的 /tmp 目录
COPY Miniconda3-py37_4.12.0-Linux-x86_64.sh /tmp
COPY torch-1.8.1+cu111-cp37-cp37m-linux_x86_64.whl /tmp
COPY torchvision-0.9.1+cu111-cp37-cp37m-linux_x86_64.whl /tmp
COPY torchaudio-0.8.1-cp37-cp37m-linux_x86_64.whl /tmp
COPY openmpi-3.0.0-bin.tar.gz /tmp
COPY horovod-0.22.1.tar.gz /tmp

https://conda.io/projects/conda/en/latest/user-guide/install/linux.html#installing-on-linux
安装 Miniconda3 到基础容器镜像的 /home/ma-user/miniconda3 目录中
RUN bash /tmp/Miniconda3-py37_4.12.0-Linux-x86_64.sh -b -p /home/ma-user/miniconda3

安装 horovod v0.22.1 已经编译好的 openmpi 3.0.0 文件
https://github.com/horovod/horovod/blob/v0.22.1/docker/horovod/Dockerfile
https://github.com/horovod/horovod/files/1596799/openmpi-3.0.0-bin.tar.gz
RUN cd /usr/local && \
 tar -zxf /tmp/openmpi-3.0.0-bin.tar.gz && \
 ldconfig && \
 mpirun --version

编译 Horovod with Pytorch 所需的环境变量
ENV HOROVOD_NCCL_INCLUDE=/usr/include \
 HOROVOD_NCCL_LIB=/usr/lib/x86_64-linux-gnu \
 HOROVOD_MPICXX_SHOW="/usr/local/openmpi/bin/mpicxx -show" \
 HOROVOD_GPU_OPERATIONS=NCCL \
 HOROVOD_WITH_PYTORCH=1

使用 Miniconda3 默认 python 环境（即 /home/ma-user/miniconda3/bin/pip）安装 torch*.whl
RUN cd /tmp && \
 /home/ma-user/miniconda3/bin/pip install --no-cache-dir \
 /tmp/torch-1.8.1+cu111-cp37-cp37m-linux_x86_64.whl \
 /tmp/torchvision-0.9.1+cu111-cp37-cp37m-linux_x86_64.whl \
 /tmp/torchaudio-0.8.1-cp37-cp37m-linux_x86_64.whl
```

```
使用 Miniconda3 默认 python 环境 (即 /home/ma-user/miniconda3/bin/pip) 编译安装
horovod-0.22.1.tar.gz
RUN cd /tmp && \
 /home/ma-user/miniconda3/bin/pip install --no-cache-dir \
 /tmp/horovod-0.22.1.tar.gz

构建最终容器镜像
FROM nvidia/cuda:11.1.1-runtime-ubuntu18.04

COPY MLNX_OFED_LINUX-5.4-3.5.8.0-ubuntu18.04-x86_64.tgz /tmp

安装 vim / curl / net-tools / mlnx ofed / ssh 工具 (依然使用华为开源镜像站)
RUN cp -a /etc/apt/sources.list /etc/apt/sources.list.bak && \
 sed -i "s@http://.*archive.ubuntu.com@http://repo.huaweicloud.com@g" /etc/apt/sources.list && \
 sed -i "s@http://.*security.ubuntu.com@http://repo.huaweicloud.com@g" /etc/apt/sources.list && \
 echo > /etc/apt/apt.conf.d/00skip-verify-peer.conf "Acquire { https::Verify-Peer false }" && \
 apt-get update && \
 apt-get install -y vim curl net-tools iputils-ping libfile-find-rule-perl-perl \
 openssh-client openssh-server && \
 ssh -V && \
 mkdir -p /run/sshd && \
 # mlnx ofed
 apt-get install -y python libfuse2 dpatch libnl-3-dev autoconf libnl-route-3-dev pciutils libnuma1
 libpci3 m4 libelf1 debhelper automake graphviz bison lsof kmod libusb-1.0-0 swig libmnl0 autotools-
 dev flex chrpath libltdl-dev && \
 cd /tmp && \
 tar -xvf MLNX_OFED_LINUX-5.4-3.5.8.0-ubuntu18.04-x86_64.tgz && \
 MLNX_OFED_LINUX-5.4-3.5.8.0-ubuntu18.04-x86_64/mlnxofedinstall --user-space-only --basic --
 without-fw-update -q && \
 cd - && \
 rm -rf /tmp/* && \
 apt-get clean && \
 mv /etc/apt/sources.list.bak /etc/apt/sources.list && \
 rm /etc/apt/apt.conf.d/00skip-verify-peer.conf

安装 horovod v0.22.1 已经编译好的 openmpi 3.0.0 文件
https://github.com/horovod/horovod/blob/v0.22.1/docker/horovod/Dockerfile
https://github.com/horovod/horovod/files/1596799/openmpi-3.0.0-bin.tar.gz
COPY openmpi-3.0.0-bin.tar.gz /tmp
RUN cd /usr/local && \
 tar -zxf /tmp/openmpi-3.0.0-bin.tar.gz && \
 ldconfig && \
 mpirun --version

增加 ma-user 用户 (uid = 1000, gid = 100)
注意到基础容器镜像已存在 gid = 100 的组, 因此 ma-user 用户可直接使用
RUN useradd -m -d /home/ma-user -s /bin/bash -g 100 -u 1000 ma-user

从上述 builder stage 中复制 /home/ma-user/miniconda3 目录到当前容器镜像的同名目录
COPY --chown=ma-user:100 --from=builder /home/ma-user/miniconda3 /home/ma-user/miniconda3

设置容器镜像默认用户与工作目录
USER ma-user
WORKDIR /home/ma-user

配置 sshd, 使得 ssh 可以免密登录
RUN MA_HOME=/home/ma-user && \
 # setup sshd dir
 mkdir -p ${MA_HOME}/etc && \
 ssh-keygen -f ${MA_HOME}/etc/ssh_host_rsa_key -N "" -t rsa && \
 mkdir -p ${MA_HOME}/etc/ssh ${MA_HOME}/var/run && \
 # setup sshd config (listen at {{MY_SSHD_PORT}} port)
 echo "Port {{MY_SSHD_PORT}}\n\
 HostKey ${MA_HOME}/etc/ssh_host_rsa_key\n\
 AuthorizedKeysFile ${MA_HOME}/.ssh/authorized_keys\n\
 PidFile ${MA_HOME}/var/run/sshd.pid\n\
 StrictModes no\n\
 UsePAM no" > ${MA_HOME}/etc/ssh/sshd_config && \
 # generate ssh key
```

```
ssh-keygen -t rsa -f ${MA_HOME}/.ssh/id_rsa -P "" && \
cat ${MA_HOME}/.ssh/id_rsa.pub >> ${MA_HOME}/.ssh/authorized_keys && \
disable ssh host key checking for all hosts
echo "Host *\n\
StrictHostKeyChecking no" > ${MA_HOME}/.ssh/config

设置容器镜像预置环境变量
请务必设置 PYTHONUNBUFFERED=1, 以免日志丢失
ENV PATH=/home/ma-user/miniconda3/bin:$PATH \
PYTHONUNBUFFERED=1
```

关于 Dockerfile 文件编写的更多指导内容参见 [Docker 官方文档](#)。

9. 下载MLNX\_OFED安装包。

进入[地址](#)，单击“Download”，在“Current Versions”和“Archive Versions”中选择合适的安装包下载。本文示例中选择“Archive Versions”，“Version”选择“5.4-3.5.8.0-LTS”，“OS Distribution”选择“Ubuntu”，“OS Distribution Version”选择“Ubuntu 18.04”，“Architecture”选择“x86\_64”，下载MLNX\_OFED\_LINUX-5.4-3.5.8.0-ubuntu18.04-x86\_64.tgz。

10. 下载openmpi-3.0.0-bin.tar.gz。

使用地址<https://github.com/horovod/horovod/files/1596799/openmpi-3.0.0-bin.tar.gz>，下载openmpi-3.0.0-bin.tar.gz文件。

11. 将上述 pip 源文件、torch\*.whl 文件、Miniconda3 安装文件等放置在 context 文件夹内，context 文件夹内容如下。

```
context
├── Dockerfile
├── MLNX_OFED_LINUX-5.4-3.5.8.0-ubuntu18.04-x86_64.tgz
├── Miniconda3-py37_4.12.0-Linux-x86_64.sh
├── horovod-0.22.1.tar.gz
├── openmpi-3.0.0-bin.tar.gz
├── pip.conf
├── torch-1.8.1+cu111-cp37-cp37m-linux_x86_64.whl
├── torchaudio-0.8.1-cp37-cp37m-linux_x86_64.whl
└── torchvision-0.9.1+cu111-cp37-cp37m-linux_x86_64.whl
```

12. 构建容器镜像。在Dockerfile文件所在的目录执行如下命令构建容器镜像horovod-pytorch:0.22.1-1.8.1-ofed-cuda11.1。

```
docker build -t horovod-pytorch:0.22.1-1.8.1-ofed-cuda11.1
```

构建过程结束时出现如下构建日志说明镜像构建成功。  
Successfully tagged horovod-pytorch:0.22.1-1.8.1-ofed-cuda11.1

## Step5 上传镜像至 SWR 服务

1. 登录容器镜像服务控制台，选择区域。

图 10-49 容器镜像服务控制台



2. 单击右上角“创建组织”，输入组织名称完成组织创建。请自定义组织名称，本示例使用“deep-learning”，下面的命令中涉及到组织名称“deep-learning”也请替换为自定义的值。

图 10-50 创建组织

### 创建组织



- 单击右上角“登录指令”，获取登录访问指令。

图 10-51 登录指令



- 以root用户登录本地环境，输入登录访问指令。
- 上传镜像至容器镜像服务镜像仓库。
  - 使用docker tag命令给上传镜像打标签。  
#region和domain信息请替换为实际值，组织名称deep-learning也请替换为自定义的值。  
sudo docker tag horovod-pytorch:0.22.1-1.8.1-ofed-cuda11.1 swr.{region-id}.{domain}/deep-learning/horovod-pytorch:0.22.1-1.8.1-ofed-cuda11.1  
#此处以华为云cn-north-4为例  
sudo docker tag horovod-pytorch:0.22.1-1.8.1-ofed-cuda11.1 swr.cn-north-4.myhuaweicloud.com/deep-learning/horovod-pytorch:0.22.1-1.8.1-ofed-cuda11.1
  - 使用docker push命令上传镜像。  
#region和domain信息请替换为实际值，组织名称deep-learning也请替换为自定义的值。  
sudo docker push swr.{region-id}.{domain}/deep-learning/horovod-pytorch:0.22.1-1.8.1-ofed-cuda11.1  
#此处以华为云cn-north-4为例  
sudo docker push swr.cn-north-4.myhuaweicloud.com/deep-learning/horovod-pytorch:0.22.1-1.8.1-ofed-cuda11.1
- 完成镜像上传后，在“容器镜像服务控制台>我的镜像”页面可查看已上传的自定义镜像。  
“swr.cn-north-4.myhuaweicloud.com/deep-learning/horovod-pytorch:0.22.1-1.8.1-ofed-cuda11.1”即为此自定义镜像的“SWR\_URL”。



## Step6 在 ModelArts 上创建训练作业

1. 登录ModelArts管理控制台，检查当前账号是否已完成访问授权的配置。如未完成，请参考[使用委托授权](#)。针对之前使用访问密钥授权的用户，建议清空授权，然后使用委托进行授权。
2. 在左侧导航栏中选择“训练管理 > 训练作业”，默认进入“训练作业”列表。
3. 在“创建训练作业”页面，填写相关参数信息，然后单击“下一步”。
  - 创建方式：选择“自定义算法”
  - 镜像来源：选择“自定义”
  - 镜像地址：[Step5 上传镜像至SWR服务](#)中创建的镜像。“swr.cn-north-4.myhuaweicloud.com/deep-learning/horovod-pytorch:0.22.1-1.8.1-ofed-cuda11.1”
  - 代码目录：设置为OBS中存放启动脚本文件的目录，例如：“obs://test-modelarts/pytorch/demo-code/”，训练代码会被自动下载至训练容器的“\${MA\_JOB\_DIR}/demo-code”目录中，“demo-code”为OBS存放代码路径的最后一级目录，可以根据实际修改。
  - 启动命令：“bash \${MA\_JOB\_DIR}/demo-code/run\_mpi.sh python \${MA\_JOB\_DIR}/demo-code/pytorch\_synthetic\_benchmark.py”，此处的“demo-code”为用户自定义的OBS存放代码路径的最后一级目录，可以根据实际修改。
  - 环境变量：单击“增加环境变量”，增加环境变量：MY\_SSHD\_PORT=38888。
  - 资源池：选择公共资源池。
  - 资源类型：选择GPU规格。
  - 计算节点个数：1个或者2个。
  - 永久保存日志：打开。
  - 作业日志路径：设置为OBS中存放训练日志的路径。例如：“obs://test-modelarts/pytorch/log/”
4. 在“规格确认”页面，确认训练作业的参数信息，确认无误后单击“提交”。
5. 训练作业创建完成后，后台将自动完成容器镜像下载、代码目录下载、执行启动命令等动作。

训练作业一般需要运行一段时间，根据您的训练业务逻辑和选择的资源不同，训练时长将持续几十分钟到几小时不等。训练作业执行成功后，日志信息如下所示。

图 10-52 GPU 规格运行日志信息（1 个计算节点）

```
58 Iter #0: 342.4 img/sec per GPU
59 Iter #1: 342.7 img/sec per GPU
60 Iter #2: 342.8 img/sec per GPU
61 Iter #3: 342.5 img/sec per GPU
62 Iter #4: 342.9 img/sec per GPU
63 Iter #5: 342.8 img/sec per GPU
64 Iter #6: 342.9 img/sec per GPU
65 Iter #7: 343.0 img/sec per GPU
66 Iter #8: 342.6 img/sec per GPU
67 Iter #9: 342.7 img/sec per GPU
68 Img/sec per GPU: 342.7 +-0.3
69 Total img/sec on 1 GPU(s): 342.7 +-0.3
```

图 10-53 GPU 规格运行日志信息（2 个计算节点）

```
84 Iter #0: 115.1 img/sec per GPU
85 Iter #1: 123.5 img/sec per GPU
86 Iter #2: 115.7 img/sec per GPU
87 Iter #3: 117.4 img/sec per GPU
88 Iter #4: 120.6 img/sec per GPU
89 Iter #5: 126.9 img/sec per GPU
90 Iter #6: 119.4 img/sec per GPU
91 Iter #7: 118.4 img/sec per GPU
92 Iter #8: 122.0 img/sec per GPU
93 Iter #9: 118.2 img/sec per GPU
94 Img/sec per GPU: 119.7 +-6.8
95 Total img/sec on 2 GPU(s): 239.4 +-13.5
```

## 10.6 示例：从 0 到 1 制作自定义镜像并用于训练 ( MindSpore+GPU )

本章节介绍如何从0到1制作镜像，并使用该镜像在ModelArts平台上进行训练。镜像中使用的AI引擎是MindSpore，训练使用的资源是GPU。

### 📖 说明

本实践教程仅适用于新版训练作业。

### 场景描述

本示例使用 Linux x86\_64 架构的主机，操作系统ubuntu-18.04，通过编写 Dockerfile 文件制作自定义镜像。

目标：构建安装如下软件的容器镜像，并在ModelArts平台上使用GPU规格资源运行训练任务。

- ubuntu-18.04
- cuda-11.1
- python-3.7.13
- mlnx ofed-5.4
- mindspore gpu-1.8.1

## 操作流程

使用自定义镜像创建训练作业时，需要您熟悉 docker 软件的使用，并具备一定的开发经验。详细步骤如下所示：

- [前提条件](#)
- [Step1 创建OBS桶和文件夹](#)
- [Step2 创建数据集并上传至OBS](#)
- [Step3 准备训练脚本并上传至OBS](#)
- [Step4 准备镜像主机](#)
- [Step5 制作自定义镜像](#)
- [Step6 上传镜像至SWR服务](#)
- [Step7 在ModelArts上创建训练作业](#)

## 前提条件

已注册华为账号并开通华为云，且在使用ModelArts前检查账号状态，账号不能处于欠费或冻结状态。

### Step1 创建 OBS 桶和文件夹

在 OBS 服务中创建桶和文件夹，用于存放样例数据集以及训练代码。需要创建的文件列表如[表10-4](#)所示，示例中的桶名称“test-modelarts”和文件夹名称均为举例，请替换为用户自定义的名称。

创建 OBS 桶和文件夹的操作指导请参见[创建桶](#)和[新建文件夹](#)。

请确保您使用的 OBS 与 ModelArts 在同一区域。

表 10-4 OBS 桶文件夹列表

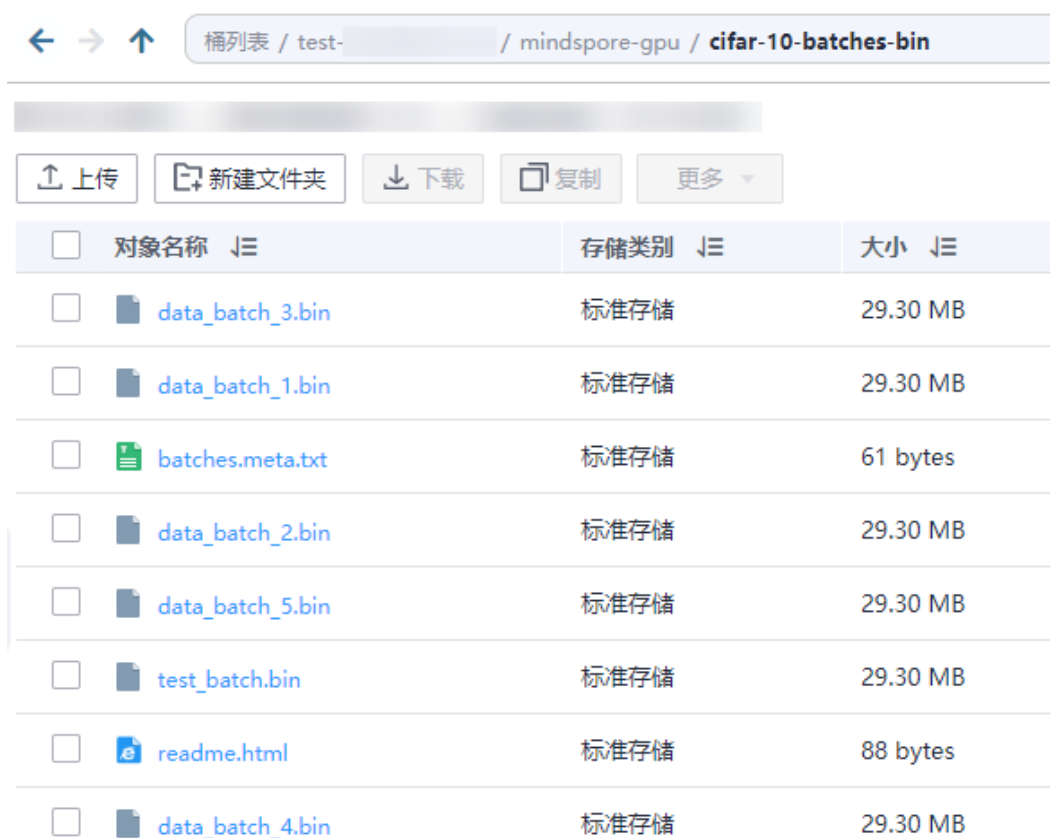
| 文件夹名称                                                      | 用途          |
|------------------------------------------------------------|-------------|
| “obs://test-modelarts/mindspore-gpu/resnet/”               | 用于存储训练脚本文件。 |
| “obs://test-modelarts/mindspore-gpu/cifar-10-batches-bin/” | 用于存储数据集文件。  |
| “obs://test-modelarts/mindspore-gpu/output/”               | 用于存储训练输出文件。 |

| 文件夹名称                                     | 用途          |
|-------------------------------------------|-------------|
| “obs://test-modelarts/mindspore-gpu/log/” | 用于存储训练日志文件。 |

## Step2 创建数据集并上传至 OBS

进入网站<http://www.cs.toronto.edu/~kriz/cifar.html>，下载“CIFAR-10 binary version (suitable for C programs)”，解压后将数据上传至OBS桶的“obs://test-modelarts/mindspore-gpu/cifar-10-batches-bin/”文件夹下。OBS桶中数据集如下所示：

图 10-54 数据集



## Step3 准备训练脚本并上传至 OBS

准备本案例所需的resnet文件和脚本run\_mpi.sh，并上传至OBS桶的“obs://test-modelarts/mindspore-gpu/resnet/”文件夹下。

resnet文件下载地址：<https://gitee.com/mindspore/models/tree/r1.8/official/cv/resnet>

run\_mpi.sh文件内容如下：

```
#!/bin/bash
MY_HOME=/home/ma-user
```

```
MY_SSHD_PORT=${MY_SSHD_PORT:-"36666"}

MY_MPI_BTL_TCP_IF=${MY_MPI_BTL_TCP_IF:-"eth0,bond0"}

MY_TASK_INDEX=${MA_TASK_INDEX:-${VC_TASK_INDEX:-${VK_TASK_INDEX}}}

MY_MPI_SLOTS=${MY_MPI_SLOTS:-"${MA_NUM_GPUS}"}

MY_MPI_TUNE_FILE="${MY_HOME}/env_for_user_process"

if [-z ${MY_MPI_SLOTS}]; then
 echo "[run_mpi] MY_MPI_SLOTS is empty, set it be 1"
 MY_MPI_SLOTS="1"
fi

printf "MY_HOME: ${MY_HOME}\nMY_SSHD_PORT: ${MY_SSHD_PORT}\nMY_MPI_BTL_TCP_IF: ${MY_MPI_BTL_TCP_IF}\nMY_TASK_INDEX: ${MY_TASK_INDEX}\nMY_MPI_SLOTS: ${MY_MPI_SLOTS}\n"

env | grep -E '^MA_|^SHARED_|^S3_|^PATH|^VC_WORKER_|^SCC|^CRED' | grep -v '=' > ${MY_MPI_TUNE_FILE}
add -x to each line
sed -i 's/^-x /' ${MY_MPI_TUNE_FILE}

sed -i 's|{{MY_SSHD_PORT}}|${MY_SSHD_PORT}|g' ${MY_HOME}/etc/ssh/sshd_config

start sshd service
bash -c "$(which sshd) -f ${MY_HOME}/etc/ssh/sshd_config"

confirm the sshd is up
netstat -anp | grep LIS | grep ${MY_SSHD_PORT}

if [$MY_TASK_INDEX -eq 0]; then
 # generate the hostfile of mpi
 for ((i=0; i<${MA_NUM_HOSTS}; i++))
 do
 eval hostname=${MA_VJ_NAME}-${MA_TASK_NAME}-${i}.${MA_VJ_NAME}
 echo "[run_mpi] hostname: ${hostname}"

 ip=""
 while [-z "$ip"]; do
 ip=$(ping -c 1 ${hostname} | grep "PING" | sed -E 's/PING .*([0-9.]+). */1/g')
 sleep 1
 done
 echo "[run_mpi] resolved ip: ${ip}"

 # test the sshd is up
 while :
 do
 if [cat < /dev/null >/dev/tcp/${ip}/${MY_SSHD_PORT}]; then
 break
 fi
 sleep 1
 done

 echo "[run_mpi] the sshd of ip ${ip} is up"

 echo "${ip} slots=${MY_MPI_SLOTS}" >> ${MY_HOME}/hostfile
 done

 printf "[run_mpi] hostfile:\n`cat ${MY_HOME}/hostfile`\n"
fi

RET_CODE=0

if [$MY_TASK_INDEX -eq 0]; then

 echo "[run_mpi] start exec command time: "$(date +%Y-%m-%d-%H:%M:%S")
```

```
np=$((${MA_NUM_HOSTS} * ${MY_MPI_SLOTS}))

echo "[run_mpi] command: mpirun -np ${np} -hostfile ${MY_HOME}/hostfile -mca plm_rsh_args \"-p $
${MY_SSHD_PORT}\" -tune ${MY_MPI_TUNE_FILE} ... @$@"

execute mpirun at worker-0
mpirun
mpirun \
 -np ${np} \
 -hostfile ${MY_HOME}/hostfile \
 -mca plm_rsh_args "-p ${MY_SSHD_PORT}" \
 -tune ${MY_MPI_TUNE_FILE} \
 -bind-to none -map-by slot \
 -x NCCL_DEBUG=INFO -x NCCL_SOCKET_IFNAME=${MY_MPI_BTL_TCP_IF} -x
NCCL_SOCKET_FAMILY=AF_INET \
 -x HOROVOD_MPI_THREADS_DISABLE=1 \
 -x LD_LIBRARY_PATH \
 -mca pml ob1 -mca btl ^openib -mca plm_rsh_no_tree_spawn true \
 "$@"

RET_CODE=$?

if [$RET_CODE -ne 0]; then
 echo "[run_mpi] exec command failed, exited with $RET_CODE"
else
 echo "[run_mpi] exec command successfully, exited with $RET_CODE"
fi

stop 1..N worker by killing the sleep proc
sed -i '1d' ${MY_HOME}/hostfile
if [`cat ${MY_HOME}/hostfile | wc -l` -ne 0]; then
 echo "[run_mpi] stop 1 to (N - 1) worker by killing the sleep proc"

 sed -i 's/${MY_MPI_SLOTS}/1/g' ${MY_HOME}/hostfile
 printf "[run_mpi] hostfile:\n`cat ${MY_HOME}/hostfile`\n"

 mpirun \
 --hostfile ${MY_HOME}/hostfile \
 --mca btl_tcp_if_include ${MY_MPI_BTL_TCP_IF} \
 --mca plm_rsh_args "-p ${MY_SSHD_PORT}" \
 -x PATH -x LD_LIBRARY_PATH \
 pkill sleep \
 > /dev/null 2>&1
fi

echo "[run_mpi] exit time: "$(date +"%Y-%m-%d-%H:%M:%S")
else
 echo "[run_mpi] the training log is in worker-0"
 sleep 365d
 echo "[run_mpi] exit time: "$(date +"%Y-%m-%d-%H:%M:%S")
fi

exit $RET_CODE
```

“obs://test-modelarts/mindspore-gpu/resnet/”文件夹下内容如下图，包含resnet文件和run\_mpi.sh:

图 10-55 resnet 文件和 run\_mpi.sh

| 对象名称                         | 存储类别 | 大小       |
|------------------------------|------|----------|
| eval.py                      | 标准存储 | 3.41 KB  |
| export.py                    | 标准存储 | 2.63 KB  |
| create_imagenet2012_label.py | 标准存储 | 1.62 KB  |
| infer.py                     | 标准存储 | 3.91 KB  |
| gpu_resnet_benchmark.py      | 标准存储 | 11.68 KB |
| mindspore_hub_conf.py        | 标准存储 | 1.18 KB  |
| postprocess.py               | 标准存储 | 3.00 KB  |
| preprocess.py                | 标准存储 | 1.68 KB  |
| README_CN.md                 | 标准存储 | 46.02 KB |
| README.md                    | 标准存储 | 56.79 KB |
| run_mpi.sh                   | 标准存储 | 3.69 KB  |
| requirements.txt             | 标准存储 | 24 bytes |
| train.py                     | 标准存储 | 18.40 KB |
| ascend310_infer              | --   | --       |
| config                       | --   | --       |
| golden_stick                 | --   | --       |
| infer                        | --   | --       |
| modelarts                    | --   | --       |
| scripts                      | --   | --       |
| src                          | --   | --       |

## Step4 准备镜像主机

准备一台 Linux x86\_64 架构的主机，操作系统使用ubuntu-18.04。您可以准备相同规格的 弹性云服务器ECS 或者应用本地已有的主机进行自定义镜像的制作。

购买ECS服务器的具体操作请参考[购买并登录Linux弹性云服务器](#)。镜像选择公共镜像，推荐使用ubuntu18.04的镜像。

图 10-56 创建 ECS 服务器-选择 X86 架构的公共镜像



## Step5 制作自定义镜像

目标：构建安装好如下软件的容器镜像，并使用 ModelArts 训练服务运行。

- ubuntu-18.04
- cuda-11.1
- python-3.7.13
- mlnx ofed-5.4
- mindspore gpu-1.8.1

此处介绍如何通过编写 Dockerfile 文件制作自定义镜像的操作步骤。

### 1. 安装 Docker。

以 Linux x86\_64 架构的操作系统为例，获取 Docker 安装包。您可以使用以下指令安装 Docker。关于安装 Docker 的更多指导内容参见 [Docker 官方文档](#)。

```
curl -fsSL get.docker.com -o get-docker.sh
sh get-docker.sh
```

如果 `docker images` 命令可以执行成功，表示 Docker 已安装，此步骤可跳过。

### 2. 确认 Docker Engine 版本。执行如下命令。

```
docker version | grep -A 1 Engine
```

命令回显如下。

```
Engine:
Version: 18.09.0
```

#### 📖 说明

推荐使用大于等于该版本的 Docker Engine 来制作自定义镜像。

### 3. 准备名为 context 的文件夹。

```
mkdir -p context
```

### 4. 准备可用的pip源文件 pip.conf。本示例使用华为开源镜像站提供的pip源，其 pip.conf 文件内容如下。

```
[global]
index-url = https://repo.huaweicloud.com/repository/pypi/simple
trusted-host = repo.huaweicloud.com
timeout = 120
```



 说明

在华为开源镜像站 <https://mirrors.huaweicloud.com/home> 中，搜索 pypi，也可以查看 pip.conf 文件内容。

5. 下载mindspore\_gpu-1.8.1-cp37-cp37m-linux\_x86\_64.whl文件。

使用网站[https://ms-release.obs.cn-north-4.myhuaweicloud.com/1.8.1/MindSpore/gpu/x86\\_64/cuda-11.1/mindspore\\_gpu-1.8.1-cp37-cp37m-linux\\_x86\\_64.whl](https://ms-release.obs.cn-north-4.myhuaweicloud.com/1.8.1/MindSpore/gpu/x86_64/cuda-11.1/mindspore_gpu-1.8.1-cp37-cp37m-linux_x86_64.whl)，mindspore\_gpu-1.8.1-cp37-cp37m-linux\_x86\_64.whl文件。

6. 下载 Miniconda3 安装文件。

使用地址 [https://repo.anaconda.com/miniconda/Miniconda3-py37\\_4.12.0-Linux-x86\\_64.sh](https://repo.anaconda.com/miniconda/Miniconda3-py37_4.12.0-Linux-x86_64.sh)，下载 Miniconda3 py37 4.12.0 安装文件（对应 python 3.7.13）。

7. 编写容器镜像Dockerfile文件。

在 context 文件夹内新建名为Dockerfile的空文件，并将下述内容写入其中。

```
容器镜像构建主机需要连通公网

基础容器镜像, https://github.com/NVIDIA/nvidia-docker/wiki/CUDA
#
https://docs.docker.com/develop/develop-images/multistage-build/#use-multi-stage-builds
require Docker Engine >= 17.05
#
builder stage
FROM nvidia/cuda:11.1.1-devel-ubuntu18.04 AS builder

基础容器镜像的默认用户已经是 root
USER root

使用华为开源镜像站提供的 pypi 配置
RUN mkdir -p /root/.pip/
COPY pip.conf /root/.pip/pip.conf

复制待安装文件到基础容器镜像中的 /tmp 目录
COPY Miniconda3-py37_4.12.0-Linux-x86_64.sh /tmp
COPY mindspore_gpu-1.8.1-cp37-cp37m-linux_x86_64.whl /tmp

https://conda.io/projects/conda/en/latest/user-guide/install/linux.html#installing-on-linux
安装 Miniconda3 到基础容器镜像的 /home/ma-user/miniconda3 目录中
RUN bash /tmp/Miniconda3-py37_4.12.0-Linux-x86_64.sh -b -p /home/ma-user/miniconda3

使用 Miniconda3 默认 python 环境 (即 /home/ma-user/miniconda3/bin/pip) 安装 mindspore whl
RUN cd /tmp && \
/home/ma-user/miniconda3/bin/pip install --no-cache-dir \
/tmp/mindspore_gpu-1.8.1-cp37-cp37m-linux_x86_64.whl \
easydict PyYAML

构建最终容器镜像
FROM nvidia/cuda:11.1.1-cudnn8-runtime-ubuntu18.04

COPY MLNX_OFED_LINUX-5.4-3.5.8.0-ubuntu18.04-x86_64.tgz /tmp

安装 vim / curl / net-tools / mlnx ofed / ssh 工具 (依然使用华为开源镜像站)
RUN cp -a /etc/apt/sources.list /etc/apt/sources.list.bak && \
sed -i "s@http://.*archive.ubuntu.com@http://repo.huaweicloud.com@g" /etc/apt/sources.list && \
sed -i "s@http://.*security.ubuntu.com@http://repo.huaweicloud.com@g" /etc/apt/sources.list && \
echo > /etc/apt/apt.conf.d/00skip-verify-peer.conf "Acquire { https::Verify-Peer false }" && \
apt-get update && \
apt-get install -y vim curl net-tools iputils-ping libfile-find-rule-perl-perl \
openssh-client openssh-server && \
ssh -V && \
mkdir -p /run/sshd && \
mlnx ofed
apt-get install -y python libfuse2 dpatch libnl-3-dev autoconf libnl-route-3-dev pciutils libnuma1
libpci3 m4 libelf1 debhelper automake graphviz bison lsof kmod libusb-1.0-0 swig libmnl0 autotools-
```

```
dev flex chrpath libltdl-dev && \
 cd /tmp && \
 tar -xvf MLNX_OFED_LINUX-5.4-3.5.8.0-ubuntu18.04-x86_64.tgz && \
 MLNX_OFED_LINUX-5.4-3.5.8.0-ubuntu18.04-x86_64/mlnxofedinstall --user-space-only --basic --
without-fw-update -q && \
 cd - && \
 rm -rf /tmp/* && \
 apt-get clean && \
 mv /etc/apt/sources.list.bak /etc/apt/sources.list && \
 rm /etc/apt/apt.conf.d/00skip-verify-peer.conf

安装 horovod v0.22.1 已经编译好的 openmpi 3.0.0 文件
https://github.com/horovod/horovod/blob/v0.22.1/docker/horovod/Dockerfile
https://github.com/horovod/horovod/files/1596799/openmpi-3.0.0-bin.tar.gz
COPY openmpi-3.0.0-bin.tar.gz /tmp
RUN cd /usr/local && \
 tar -zxf /tmp/openmpi-3.0.0-bin.tar.gz && \
 ldconfig && \
 mpirun --version

增加 ma-user 用户 (uid = 1000, gid = 100)
注意到基础容器镜像已存在 gid = 100 的组, 因此 ma-user 用户可直接使用
RUN useradd -m -d /home/ma-user -s /bin/bash -g 100 -u 1000 ma-user

从上述 builder stage 中复制 /home/ma-user/miniconda3 目录到当前容器镜像的同名目录
COPY --chown=ma-user:100 --from=builder /home/ma-user/miniconda3 /home/ma-user/miniconda3

设置容器镜像默认用户与工作目录
USER ma-user
WORKDIR /home/ma-user

配置 sshd, 使得 ssh 可以免密登录
RUN MA_HOME=/home/ma-user && \
 # setup sshd dir
 mkdir -p ${MA_HOME}/etc && \
 ssh-keygen -f ${MA_HOME}/etc/ssh_host_rsa_key -N "" -t rsa && \
 mkdir -p ${MA_HOME}/etc/ssh ${MA_HOME}/var/run && \
 # setup sshd config (listen at ${MY_SSHD_PORT} port)
 echo "Port ${MY_SSHD_PORT}"\
HostKey ${MA_HOME}/etc/ssh_host_rsa_key\
AuthorizedKeysFile ${MA_HOME}/.ssh/authorized_keys\
PidFile ${MA_HOME}/var/run/sshd.pid\
StrictModes no\
UsePAM no" > ${MA_HOME}/etc/ssh/sshd_config && \
 # generate ssh key
 ssh-keygen -t rsa -f ${MA_HOME}/.ssh/id_rsa -P "" && \
 cat ${MA_HOME}/.ssh/id_rsa.pub >> ${MA_HOME}/.ssh/authorized_keys && \
 # disable ssh host key checking for all hosts
 echo "Host *"\
StrictHostKeyChecking no" > ${MA_HOME}/.ssh/config

设置容器镜像预置环境变量
请务必设置 PYTHONUNBUFFERED=1, 以免日志丢失
ENV PATH=/home/ma-user/miniconda3/bin:$PATH \
 LD_LIBRARY_PATH=/usr/local/cuda/lib64:/usr/lib/x86_64-linux-gnu:$LD_LIBRARY_PATH \
 PYTHONUNBUFFERED=1
```

关于 Dockerfile 文件编写的更多指导内容参见 [Docker 官方文档](#)。

#### 8. 下载MLNX\_OFED\_LINUX-5.4-3.5.8.0-ubuntu18.04-x86\_64.tgz。

进入地址[https://network.nvidia.com/products/infiniband-drivers/linux/mlnx\\_ofed/](https://network.nvidia.com/products/infiniband-drivers/linux/mlnx_ofed/), 单击“Download”, “Version”选择“5.4-3.5.8.0-LTS”, “OSDistributionVersion”选择“Ubuntu 18.04”, “Architecture”选择“x86\_64”, 下载MLNX\_OFED\_LINUX-5.4-3.5.8.0-ubuntu18.04-x86\_64.tgz。

#### 9. 下载openmpi-3.0.0-bin.tar.gz。

使用地址<https://github.com/horovod/horovod/files/1596799/openmpi-3.0.0-bin.tar.gz>, 下载openmpi-3.0.0-bin.tar.gz文件。

- 将上述 Dockerfile 文件、Miniconda3 安装文件等放置在 context 文件夹内，context 文件夹内容如下。

```
context
├── Dockerfile
├── MLNX_OFED_LINUX-5.4-3.5.8.0-ubuntu18.04-x86_64.tgz
├── Miniconda3-py37_4.12.0-Linux-x86_64.sh
├── mindspore_gpu-1.8.1-cp37-cp37m-linux_x86_64.whl
├── openmpi-3.0.0-bin.tar.gz
└── pip.conf
```

- 构建容器镜像。在 Dockerfile 文件所在的目录执行如下命令构建容器镜像 mindspore:1.8.1-ofed-cuda11.1。

```
docker build . -t mindspore:1.8.1-ofed-cuda11.1
```

构建过程结束时出现如下构建日志说明镜像构建成功。

```
Successfully tagged mindspore:1.8.1-ofed-cuda11.1
```

## Step6 上传镜像至 SWR 服务

- 登录容器镜像服务控制台，选择区域。

图 10-57 容器镜像服务控制台



- 单击右上角“创建组织”，输入组织名称完成组织创建。请自定义组织名称，本示例使用“deep-learning”，下面的命令中涉及到组织名称“deep-learning”也请替换为自定义的值。

图 10-58 创建组织

### 创建组织

- 组织名称，全局唯一。
- 当前租户最多可创建5个组织。
- 建议一个组织对应一个公司、部门或个人，以便集中高效地管理镜像资源。

示例：

以公司、部门作为组织: cloud-hangzhou、cloud-develop

以个人作为组织: john

组织名称

- 单击右上角“登录指令”，获取登录访问指令。

图 10-59 登录指令



4. 以root用户登录本地环境，输入登录访问指令。
5. 上传镜像至容器镜像服务镜像仓库。
  - a. 使用docker tag命令给上传镜像打标签。  
#region和domain信息请替换为实际值，组织名称deep-learning也请替换为自定义的值。  
sudo docker tag mindspore:1.8.1-ofed-cuda11.1 swr.{region-id}.{domain}/deep-learning/mindspore:1.8.1-ofed-cuda11.1  
#此处以华为云cn-north-4为例  
sudo docker tag mindspore:1.8.1-ofed-cuda11.1 swr.cn-north-4.myhuaweicloud.com/deep-learning/mindspore:1.8.1-ofed-cuda11.1
  - b. 使用docker push命令上传镜像。  
#region和domain信息请替换为实际值，组织名称deep-learning也请替换为自定义的值。  
sudo docker push swr.{region-id}.{domain}/deep-learning/mindspore:1.8.1-ofed-cuda11.1  
#此处以华为云cn-north-4为例  
sudo docker push swr.cn-north-4.myhuaweicloud.com/deep-learning/mindspore:1.8.1-ofed-cuda11.1
6. 完成镜像上传后，在“容器镜像服务控制台>我的镜像”页面可查看已上传的自定义镜像。  
“swr.cn-north-4.myhuaweicloud.com/deep-learning/mindspore:1.8.1-ofed-cuda11.1”即为此自定义镜像的“SWR\_URL”。

## Step7 在 ModelArts 上创建训练作业

1. 登录ModelArts管理控制台，检查当前账号是否已完成访问授权的配置。如未完成，请参考[使用委托授权](#)。针对之前使用访问密钥授权的用户，建议清空授权，然后使用委托进行授权。
2. 在左侧导航栏中选择“训练管理 > 训练作业”，默认进入“训练作业”列表。
3. 在“创建训练作业”页面，填写相关参数信息，然后单击“下一步”。
  - 创建方式：选择“自定义算法”。
  - 镜像来源：选择“自定义”。
  - 镜像地址：[Step6 上传镜像至SWR服务](#)中创建的镜像。“swr.cn-north-4.myhuaweicloud.com/deep-learning/mindspore:1.8.1-ofed-cuda11.1”。
  - 代码目录：设置为OBS中存放启动脚本文件的目录，例如：“obs://test-modelarts/mindspore-gpu/resnet/”，训练代码会被自动下载至训练容器的“\${MA\_JOB\_DIR}/resnet”目录中，“resnet”为OBS存放代码路径的最后一级目录，可以根据实际修改。
  - 启动命令：“bash \${MA\_JOB\_DIR}/resnet/run\_mpi.sh python \${MA\_JOB\_DIR}/resnet/train.py”，此处的“resnet”为用户自定义的OBS存放代码路径的最后一级目录，可以根据实际修改。

- 训练输入：单击“增加训练输入”，参数名称设置为“data\_path”，选择 OBS 中存放数据集的目录，例如“obs://test-modelarts/mindspore-gpu/cifar-10-batches-bin/”，获取方式设置为“超参”。
  - 训练输出：单击“增加训练输出”，参数名称设置为“output\_path”，选择 OBS 存放训练输出的路径，例如：“obs://test-modelarts/mindspore-gpu/output/”，获取方式设置为“超参”，预下载至本地目录设置为“不下载”。
  - 超参：单击“增加超参”，增加如下四个超参：
    - run\_distribute=True
    - device\_num=1（根据规格中的 GPU 卡数设置）
    - device\_target=GPU
    - epoch\_size=2
  - 环境变量：单击“增加环境变量”，增加环境变量：MY\_SSHD\_PORT=38888。
  - 资源池：选择公共资源池。
  - 资源类型：选择 GPU 规格。
  - 计算节点个数：1 个或者 2 个。
  - 永久保存日志：打开。
  - 作业日志路径：设置为 OBS 中存放训练日志的路径。例如：“obs://test-modelarts/mindspore-gpu/log/”。
4. 在“规格确认”页面，确认训练作业的参数信息，确认无误后单击“提交”。
  5. 训练作业创建完成后，后台将自动完成容器镜像下载、代码目录下载、执行启动命令等动作。

训练作业一般需要运行一段时间，根据您的训练业务逻辑和选择的资源不同，训练时长将持续几十分钟到几小时不等。训练作业执行成功后，日志信息如下所示。

图 10-60 GPU 规格运行日志信息（1 个计算节点）

```
127 epoch: 1 step: 1875, loss is 1.4800076
128 Train epoch time: 369422.027 ms, per step time: 197.025 ms
129 epoch: 2 step: 1875, loss is 1.0306032
130 Train epoch time: 66996.087 ms, per step time: 35.731 ms
```

图 10-61 GPU 规格运行日志信息（2 个计算节点）

```
187 epoch: 1 step: 937, loss is 1.8482083
188 epoch: 1 step: 937, loss is 1.342748
189 Train epoch time: 488492.170 ms, per step time: 521.336 ms
190 Train epoch time: 488490.528 ms, per step time: 521.335 ms
191 epoch: 2 step: 937, loss is 0.9150252
192 Train epoch time: 180200.654 ms, per step time: 192.317 ms
193 epoch: 2 step: 937, loss is 0.9933052
194 Train epoch time: 180199.969 ms, per step time: 192.316 ms
195 172.16.0.45 slots=1
```

## 10.7 示例：从 0 到 1 制作自定义镜像并用于训练 (Tensorflow+GPU)

本章节介绍如何从0到1制作镜像，并使用该镜像在ModelArts平台上进行训练。镜像中使用的AI引擎是Tensorflow，训练使用的资源是GPU。

### 📖 说明

本实践教程仅适用于新版训练作业。

### 场景描述

本示例使用 Linux x86\_64 架构的主机，操作系统ubuntu-18.04，通过编写 Dockerfile 文件制作自定义镜像。

目标：构建安装如下软件的容器镜像，并在ModelArts平台上使用GPU规格资源运行训练任务。

- ubuntu-18.04
- cuda-11.2
- python-3.7.13
- mlnx ofed-5.4
- tensorflow gpu-2.10.0

### 操作流程

使用自定义镜像创建训练作业时，需要您熟悉 docker 软件的使用，并具备一定的开发经验。详细步骤如下所示：

1. [前提条件](#)
2. [Step1 创建OBS桶和文件夹](#)
3. [Step2 创建数据集并上传至OBS](#)
4. [Step3 准备训练脚本并上传至OBS](#)
5. [Step4 准备镜像主机](#)
6. [Step5 制作自定义镜像](#)
7. [Step6 上传镜像至SWR服务](#)
8. [Step7 在ModelArts上创建训练作业](#)

### 前提条件

已注册华为账号并开通华为云，且在使用ModelArts前检查账号状态，账号不能处于欠费或冻结状态。

### Step1 创建 OBS 桶和文件夹

在 OBS 服务中创建桶和文件夹，用于存放样例数据集以及训练代码。需要创建的文件列表如[表10-5](#)所示，示例中的桶名称“test-modelarts”和文件夹名称均为举例，请替换为用户自定义的名称。

创建 OBS 桶和文件夹的操作指导请参见[创建桶](#)和[新建文件夹](#)。

请确保您使用的 OBS 与 ModelArts 在同一区域。

表 10-5 OBS 桶文件夹列表

| 文件夹名称                                   | 用途          |
|-----------------------------------------|-------------|
| “obs://test-modelarts/tensorflow/code/” | 用于存储训练脚本文件。 |
| “obs://test-modelarts/tensorflow/data/” | 用于存储数据集文件。  |
| “obs://test-modelarts/tensorflow/log/”  | 用于存储训练日志文件。 |

## Step2 创建数据集并上传至 OBS

使用网站<https://storage.googleapis.com/tensorflow/tf-keras-datasets/mnist.npz>，下载“mnist.npz”文件并上传至OBS桶的“obs://test-modelarts/tensorflow/data/”文件夹下。

## Step3 准备训练脚本并上传至 OBS

准备本案例所需的训练脚本mnist.py，并上传至OBS桶的“obs://test-modelarts/tensorflow/code/”文件夹下。

mnist.py文件内容如下：

```
import argparse
import tensorflow as tf

parser = argparse.ArgumentParser(description='TensorFlow quick start')
parser.add_argument('--data_url', type=str, default='./Data', help='path where the dataset is saved')
args = parser.parse_args()

mnist = tf.keras.datasets.mnist

(x_train, y_train), (x_test, y_test) = mnist.load_data(args.data_url)
x_train, x_test = x_train / 255.0, x_test / 255.0

model = tf.keras.models.Sequential([
 tf.keras.layers.Flatten(input_shape=(28, 28)),
 tf.keras.layers.Dense(128, activation='relu'),
 tf.keras.layers.Dropout(0.2),
 tf.keras.layers.Dense(10)
])

loss_fn = tf.keras.losses.SparseCategoricalCrossentropy(from_logits=True)

model.compile(optimizer='adam',
 loss=loss_fn,
 metrics=['accuracy'])

model.fit(x_train, y_train, epochs=5)
```



## Step4 准备镜像主机

准备一台 Linux x86\_64 架构的主机，操作系统使用ubuntu-18.04。您可以准备相同规格的 弹性云服务器ECS 或者应用本地已有的主机进行自定义镜像的制作。

购买ECS服务器的具体操作请参考[购买并登录Linux弹性云服务器](#)。镜像选择公共镜像，推荐使用ubuntu18.04的镜像。

图 10-62 创建 ECS 服务器-选择 X86 架构的公共镜像



## Step5 制作自定义镜像

目标：构建安装好如下软件的容器镜像，并使用 ModelArts 训练服务运行。

- ubuntu-18.04
- cuda-11.1
- python-3.7.13
- mlnx ofed-5.4
- mindspore gpu-1.8.1

此处介绍如何通过编写 Dockerfile 文件制作自定义镜像的操作步骤。

### 1. 安装 Docker。

以 Linux x86\_64 架构的操作系统为例，获取 Docker 安装包。您可以使用以下指令安装 Docker。关于安装 Docker 的更多指导内容参见 [Docker 官方文档](#)。

```
curl -fsSL get.docker.com -o get-docker.sh
sh get-docker.sh
```

如果 `docker images` 命令可以执行成功，表示 Docker 已安装，此步骤可跳过。

### 2. 确认 Docker Engine 版本。执行如下命令。

```
docker version | grep -A 1 Engine
```

命令回显如下。

```
Engine:
Version: 18.09.0
```

### 📖 说明

推荐使用大于等于该版本的 Docker Engine 来制作自定义镜像。

### 3. 准备名为 context 的文件夹。

```
mkdir -p context
```



4. 准备可用的pip源文件 pip.conf 。本示例使用华为开源镜像站提供的pip源，其 pip.conf 文件内容如下。

```
[global]
index-url = https://repo.huaweicloud.com/repository/pypi/simple
trusted-host = repo.huaweicloud.com
timeout = 120
```

#### 📖 说明

在华为开源镜像站 <https://mirrors.huaweicloud.com/home> 中，搜索 pypi ，也可以查看 pip.conf 文件内容。

5. 下载tensorflow\_gpu-2.10.0-cp37-cp37m-manylinux\_2\_17\_x86\_64.manylinux2014\_x86\_64.whl文件。  
使用网站<https://pypi.org/project/tensorflow-gpu/2.10.0/#files>，下载 tensorflow\_gpu-2.10.0-cp37-cp37m-manylinux\_2\_17\_x86\_64.manylinux2014\_x86\_64.whl文件。
6. 下载 Miniconda3 安装文件。  
使用地址 [https://repo.anaconda.com/miniconda/Miniconda3-py37\\_4.12.0-Linux-x86\\_64.sh](https://repo.anaconda.com/miniconda/Miniconda3-py37_4.12.0-Linux-x86_64.sh)，下载 Miniconda3 py37 4.12.0 安装文件（对应 python 3.7.13）。
7. 编写容器镜像Dockerfile文件。

在 context 文件夹内新建名为Dockerfile的空文件，并将下述内容写入其中。

```
容器镜像构建主机需要连通公网

基础容器镜像, https://github.com/NVIDIA/nvidia-docker/wiki/CUDA
#
https://docs.docker.com/develop/develop-images/multistage-build/#use-multi-stage-builds
require Docker Engine >= 17.05
#
builder stage
FROM nvidia/cuda:11.2.2-cudnn8-runtime-ubuntu18.04 AS builder

基础容器镜像的默认用户已经是 root
USER root

使用华为开源镜像站提供的 pypi 配置
RUN mkdir -p /root/.pip/
COPY pip.conf /root/.pip/pip.conf

复制待安装文件到基础容器镜像中的 /tmp 目录
COPY Miniconda3-py37_4.12.0-Linux-x86_64.sh /tmp
COPY tensorflow_gpu-2.10.0-cp37-cp37m-manylinux_2_17_x86_64.manylinux2014_x86_64.whl /tmp

https://conda.io/projects/conda/en/latest/user-guide/install/linux.html#installing-on-linux
安装 Miniconda3 到基础容器镜像的 /home/ma-user/miniconda3 目录中
RUN bash /tmp/Miniconda3-py37_4.12.0-Linux-x86_64.sh -b -p /home/ma-user/miniconda3

使用 Miniconda3 默认 python 环境 (即 /home/ma-user/miniconda3/bin/pip) 安装 tensorflow whl
RUN cd /tmp && \
 /home/ma-user/miniconda3/bin/pip install --no-cache-dir \
 /tmp/tensorflow_gpu-2.10.0-cp37-cp37m-manylinux_2_17_x86_64.manylinux2014_x86_64.whl

RUN cd /tmp && \
 /home/ma-user/miniconda3/bin/pip install --no-cache-dir keras==2.10.0

构建最终容器镜像
FROM nvidia/cuda:11.2.2-cudnn8-runtime-ubuntu18.04

COPY MLNX_OFED_LINUX-5.4-3.5.8.0-ubuntu18.04-x86_64.tgz /tmp

安装 vim / curl / net-tools / mlnx ofed (依然使用华为开源镜像站)
RUN cp -a /etc/apt/sources.list /etc/apt/sources.list.bak && \
 sed -i "s@http://.*archive.ubuntu.com@http://repo.huaweicloud.com@g" /etc/apt/sources.list && \
```

```

sed -i "s@http://.*security.ubuntu.com@http://repo.huaweicloud.com@g" /etc/apt/sources.list && \
echo > /etc/apt/apt.conf.d/00skip-verify-peer.conf "Acquire { https::Verify-Peer false }" && \
apt-get update && \
apt-get install -y vim curl net-tools iputils-ping && \
mlnx ofed
apt-get install -y python libfuse2 dpatch libnl-3-dev autoconf libnl-route-3-dev pciutils libnuma1
libpci3 m4 libelf1 debhelper automake graphviz bison lsof kmod libusb-1.0-0 swig libmnl0 autotools-
dev flex chrpath libltdl-dev && \
cd /tmp && \
tar -xvf MLNX_OFED_LINUX-5.4-3.5.8.0-ubuntu18.04-x86_64.tgz && \
MLNX_OFED_LINUX-5.4-3.5.8.0-ubuntu18.04-x86_64/mlnxofedinstall --user-space-only --basic --
without-fw-update -q && \
cd - && \
rm -rf /tmp/* && \
apt-get clean && \
mv /etc/apt/sources.list.bak /etc/apt/sources.list && \
rm /etc/apt/apt.conf.d/00skip-verify-peer.conf

增加 ma-user 用户 (uid = 1000, gid = 100)
注意到基础容器镜像已存在 gid = 100 的组, 因此 ma-user 用户可直接使用
RUN useradd -m -d /home/ma-user -s /bin/bash -g 100 -u 1000 ma-user

从上述 builder stage 中复制 /home/ma-user/miniconda3 目录到当前容器镜像的同名目录
COPY --chown=ma-user:100 --from=builder /home/ma-user/miniconda3 /home/ma-user/miniconda3

设置容器镜像默认用户与工作目录
USER ma-user
WORKDIR /home/ma-user

设置容器镜像预置环境变量
请务必设置 PYTHONUNBUFFERED=1, 以免日志丢失
ENV PATH=/home/ma-user/miniconda3/bin:$PATH \
LD_LIBRARY_PATH=/usr/local/cuda/lib64:/usr/lib/x86_64-linux-gnu:$LD_LIBRARY_PATH \
PYTHONUNBUFFERED=1

```

关于 Dockerfile 文件编写的更多指导内容参见 [Docker 官方文档](#)。

8. 下载MLNX\_OFED\_LINUX-5.4-3.5.8.0-ubuntu18.04-x86\_64.tgz。  
进入[地址](#)，单击“Download”，“Version”选择“5.4-3.5.8.0-LTS”，“OSDistributionVersion”选择“Ubuntu 18.04”，“Architecture”选择“x86\_64”，下载MLNX\_OFED\_LINUX-5.4-3.5.8.0-ubuntu18.04-x86\_64.tgz。
9. 将上述 Dockerfile文件、Miniconda3 安装文件等放置在 context 文件夹内，context 文件夹内容如下。

```

context
├── Dockerfile
├── MLNX_OFED_LINUX-5.4-3.5.8.0-ubuntu18.04-x86_64.tgz
├── Miniconda3-py37_4.12.0-Linux-x86_64.sh
├── pip.conf
└── tensorflow_gpu-2.10.0-cp37-cp37m-manylinux_2_17_x86_64.manylinux2014_x86_64.whl

```

10. 构建容器镜像。在Dockerfile文件所在的目录执行如下命令构建容器镜像 tensorflow:2.10.0-ofed-cuda11.2。  
docker build . -t tensorflow:2.10.0-ofed-cuda11.2  
构建过程结束时出现如下构建日志说明镜像构建成功。  
Successfully tagged tensorflow:2.10.0-ofed-cuda11.2

## Step6 上传镜像至 SWR 服务

1. 登录容器镜像服务控制台，选择区域。

图 10-63 容器镜像服务控制台



2. 单击右上角“创建组织”，输入组织名称完成组织创建。请自定义组织名称，本示例使用“deep-learning”，下面的命令中涉及到组织名称“deep-learning”也请替换为自定义的值。

图 10-64 创建组织

### 创建组织

1. 组织名称，全局唯一。
  2. 当前租户最多可创建5个组织。
  3. 建议一个组织对应一个公司、部门或个人，以便集中高效地管理镜像资源。
- 示例：  
以公司、部门作为组织: cloud-hangzhou、cloud-develop  
以个人作为组织: john

组织名称

deep-learning

3. 单击右上角“登录指令”，获取登录访问指令。

图 10-65 登录指令



4. 以root用户登录本地环境，输入登录访问指令。
5. 上传镜像至容器镜像服务镜像仓库。
  - a. 使用docker tag命令给上传镜像打标签。  
#region和domain信息请替换为实际值，组织名称deep-learning也请替换为自定义的值。  
sudo docker tag tensorflow:2.10.0-ofed-cuda11.2 swr.{region-id}.{domain}/deep-learning/tensorflow:2.10.0-ofed-cuda11.2  
#此处以华为云cn-north-4为例  
sudo docker tag tensorflow:2.10.0-ofed-cuda11.2 swr.cn-north-4.myhuaweicloud.com/deep-learning/tensorflow:2.10.0-ofed-cuda11.2
  - b. 使用docker push命令上传镜像。

```
#region和domain信息请替换为实际值，组织名称deep-learning也请替换为自定义的值。
sudo docker push swr.{region-id}.{domain}/deep-learning/tensorflow:2.10.0-oped-cuda11.2
#此处以华为云cn-north-4为例
sudo docker push swr.cn-north-4.myhuaweicloud.com/deep-learning/tensorflow:2.10.0-oped-cuda11.2
```

6. 完成镜像上传后，在“容器镜像服务控制台>我的镜像”页面可查看已上传的自定义镜像。

“swr.cn-north-4.myhuaweicloud.com/deep-learning/tensorflow:2.10.0-oped-cuda11.2”即为此自定义镜像的“SWR\_URL”。

## Step7 在 ModelArts 上创建训练作业

1. 登录ModelArts管理控制台，检查当前账号是否已完成访问授权的配置。如未完成，请参考[使用委托授权](#)。针对之前使用访问密钥授权的用户，建议清空授权，然后使用委托进行授权。
2. 在左侧导航栏中选择“训练管理 > 训练作业”，默认进入“训练作业”列表。
3. 在“创建训练作业”页面，填写相关参数信息，然后单击“下一步”。
  - 创建方式：选择“自定义算法”。
  - 镜像来源：选择“自定义”。
  - 镜像地址：[Step5 制作自定义镜像](#)中创建的镜像。“swr.cn-north-4.myhuaweicloud.com/deep-learning/tensorflow:2.10.0-oped-cuda11.2”。
  - 代码目录：设置为OBS中存放启动脚本文件的目录，例如：“obs://test-modelarts/tensorflow/code/”，训练代码会被自动下载至训练容器的“\${MA\_JOB\_DIR}/code”目录中，“code”为OBS存放代码路径的最后一级目录，可以根据实际修改。
  - 启动命令：“python \${MA\_JOB\_DIR}/code/mnist.py”，此处的“code”为用户自定义的OBS存放代码路径的最后一级目录，可以根据实际修改。
  - 训练输入：单击“增加训练输入”，参数名称设置为“data\_path”，选择OBS中存放“mnist.npz”的目录，例如“obs://test-modelarts/tensorflow/data/mnist.npz”，获取方式设置为“超参”。
  - 资源池：选择公共资源池。
  - 资源类型：选择GPU规格。
  - 计算节点个数：1个。
  - 永久保存日志：打开。
  - 作业日志路径：设置为OBS中存放训练日志的路径。例如：“obs://test-modelarts/mindspore-gpu/log/”。
4. 在“规格确认”页面，确认训练作业的参数信息，确认无误后单击“提交”。
5. 训练作业创建完成后，后台将自动完成容器镜像下载、代码目录下载、执行启动命令等动作。

训练作业一般需要运行一段时间，根据您的训练业务逻辑和选择的资源不同，训练时长将持续几十分钟到几小时不等。训练作业执行成功后，日志信息如下所示。

图 10-66 GPU 规格运行日志信息

```

0.9767.....
323 1503/1875 [=====>.....] - ETA: 0s - loss: 0.0741 - accuracy:
0.9769.....
324 1533/1875 [=====>.....] - ETA: 0s - loss: 0.0743 - accuracy:
0.9769.....
325 1564/1875 [=====>.....] - ETA: 0s - loss: 0.0746 - accuracy:
0.9768.....
326 1595/1875 [=====>.....] - ETA: 0s - loss: 0.0741 - accuracy:
0.9770.....
327 1624/1875 [=====>.....] - ETA: 0s - loss: 0.0742 - accuracy:
0.9770.....
328 1654/1875 [=====>.....] - ETA: 0s - loss: 0.0745 - accuracy:
0.9770.....
329 1685/1875 [=====>.....] - ETA: 0s - loss: 0.0747 - accuracy:
0.9768.....
330 1716/1875 [=====>.....] - ETA: 0s - loss: 0.0752 - accuracy:
0.9767.....
331 1747/1875 [=====>.....] - ETA: 0s - loss: 0.0755 - accuracy:
0.9767.....
332 1778/1875 [=====>.....] - ETA: 0s - loss: 0.0753 - accuracy:
0.9767.....
333 1809/1875 [=====>.....] - ETA: 0s - loss: 0.0751 - accuracy:
0.9768.....
334 1841/1875 [=====>.....] - ETA: 0s - loss: 0.0753 - accuracy:
0.9767.....
335 1872/1875 [=====>.....] - ETA: 0s - loss: 0.0753 - accuracy:
0.9767.....
336 1875/1875 [=====] - 3s 2ms/step - loss: 0.0752 - accuracy: 0.9767

```

## 10.8 示例：从 0 到 1 制作自定义镜像并用于训练 ( MindSpore+Ascend )

### 10.8.1 场景描述

本案例介绍如何从0到1制作Ascend容器镜像，并使用该镜像在ModelArts平台上进行训练。镜像中使用的AI引擎是MindSpore，训练使用的资源是专属资源池的Ascend芯片。

#### 约束限制

- 由于案例中需要下载商用版CANN，因此本案例仅面向有下载权限的渠道用户，非渠道用户建议参考其他自定义镜像制作教程。
- Mindspore版本与CANN版本，CANN版本与Ascend驱动/固件版本均有严格的匹配关系，版本不匹配会导致训练失败。

#### 场景描述

目标：构建安装如下软件的容器镜像，并在ModelArts平台上使用Ascend规格资源运行训练任务。

- ubuntu-18.04
- cann-6.3.RC2 (商用版本)
- python-3.7.13
- mindspore-2.1.1

### 📖 说明

- 本教程以cann-6.3.RC2、mindspore-2.1.1为例介绍。
- 本示例仅用于示意Ascend容器镜像制作流程，且在匹配正确的Ascend驱动/固件版本的专属资源池上运行通过。

## 操作流程

使用自定义镜像创建训练作业时，需要您熟悉 docker 软件的使用，并具备一定的开发经验。详细步骤如下所示：

1. [Step1 创建OBS桶和文件夹](#)
2. [Step2 准备脚本文件并上传至OBS中](#)
3. [Step3 制作自定义镜像](#)
4. [Step4 上传镜像至SWR](#)
5. [Step5 在ModelArts上创建Notebook并调试](#)
6. [Step6 在ModelArts上创建训练作业](#)

### 10.8.2 Step1 创建 OBS 桶和文件夹

#### 前提条件

已注册华为账号并开通华为云，且在使用 ModelArts 前检查账号状态，账号不能处于欠费或冻结状态。

#### Step1 创建 OBS 桶和文件夹

在 OBS 服务中创建桶和文件夹，用于存放样例数据集以及训练代码。如下示例中，请创建命名为“test-modelarts”的桶，并创建如[表10-6](#)所示的文件夹。

创建 OBS 桶和文件夹的操作指导请参见[创建桶](#)和[新建文件夹](#)。

请确保您使用的 OBS 与 ModelArts 在同一区域。

表 10-6 OBS 桶文件夹列表

| 文件夹名称                                             | 用途                     |
|---------------------------------------------------|------------------------|
| obs://test-modelarts/ascend/demo-code/            | 用于存储 Ascend 训练脚本文件。    |
| obs://test-modelarts/ascend/demo-code/run_ascend/ | 用于存储 Ascend 训练脚本的启动脚本。 |
| obs://test-modelarts/ascend/log/                  | 用于存储训练日志文件。            |

### 10.8.3 Step2 准备脚本文件并上传至 OBS 中

1. 准备本案例所需训练脚本 mindspore-verification.py 文件和 Ascend 的启动脚本文件（共5个）。

- 训练脚本文件具体内容请参见[训练脚本 mindspore-verification.py 文件](#)。
- Ascend 的启动脚本文件包括以下5个，具体脚本内容请参见[Ascend 的启动脚本文件](#)。
  - i. run\_ascend.py
  - ii. common.py
  - iii. rank\_table.py
  - iv. manager.py
  - v. fmk.py

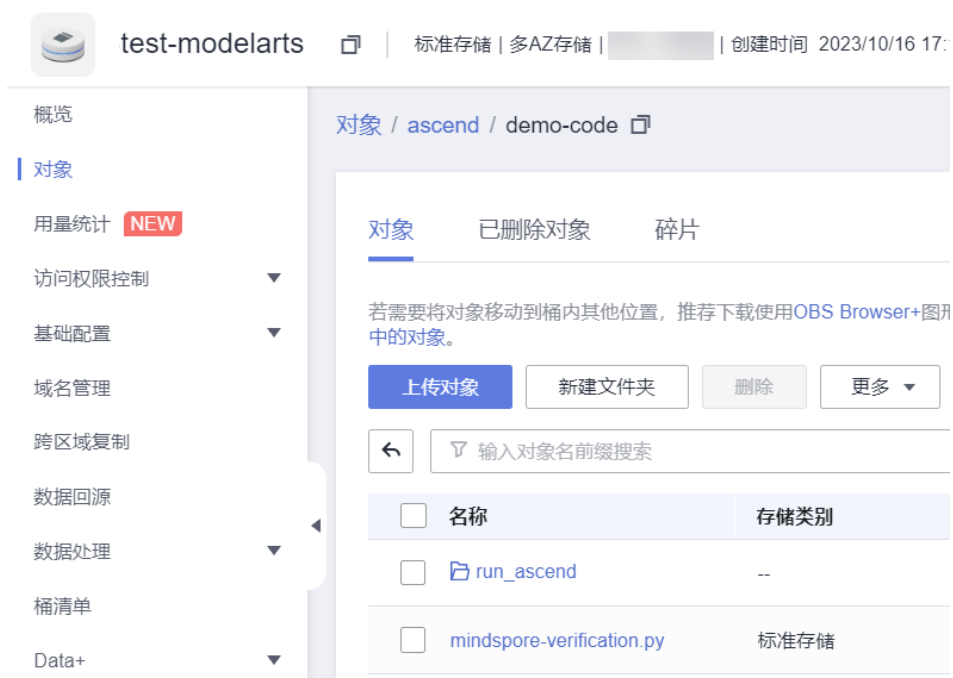
### 📖 说明

mindspore-verification.py 和run\_ascend.py脚本文件在创建训练作业时的“启动命令”参数中调用，具体请参见[启动命令：“python \\${MA\\_JOB\\_D...”](#)。

run\_ascend.py脚本运行时会调用common.py、rank\_table.py、manager.py、fmk.py脚本。

2. 上传训练脚本 mindspore-verification.py 文件至OBS桶的“obs://test-modelarts/ascend/demo-code/”文件夹下。

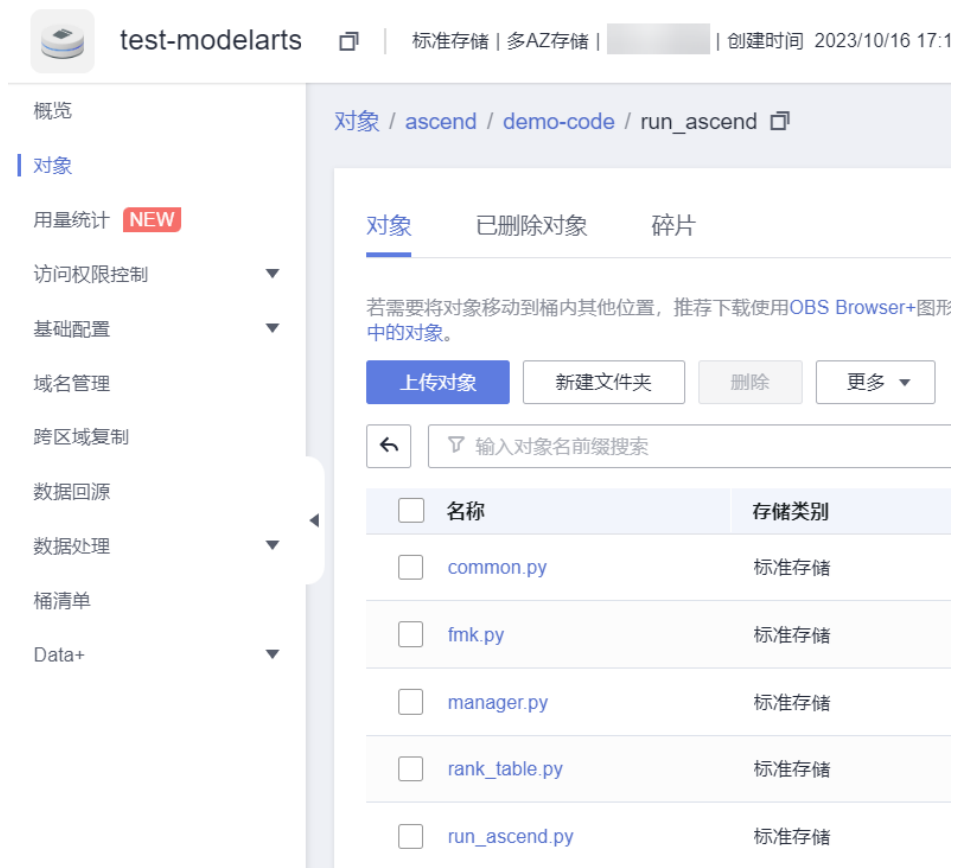
图 10-67 训练脚本文件上传完成后的 OBS 列表



3. 上传Ascend的启动脚本文件（共5个）至OBS桶的“obs://test-modelarts/ascend/demo-code/run\_ascend/”文件夹下。



图 10-68 Ascend 的启动脚本文件上传完成后的 OBS 列表



## 训练脚本 mindspore-verification.py 文件

mindspore-verification.py 文件内容如下：

```
import os
import numpy as np
from mindspore import Tensor
import mindspore.ops as ops
import mindspore.context as context

print('Ascend Envs')
print('-----')
print('JOB_ID: ', os.environ['JOB_ID'])
print('RANK_TABLE_FILE: ', os.environ['RANK_TABLE_FILE'])
print('RANK_SIZE: ', os.environ['RANK_SIZE'])
print('ASCEND_DEVICE_ID: ', os.environ['ASCEND_DEVICE_ID'])
print('DEVICE_ID: ', os.environ['DEVICE_ID'])
print('RANK_ID: ', os.environ['RANK_ID'])
print('-----')

context.set_context(device_target="Ascend")
x = Tensor(np.ones([1,3,3,4]).astype(np.float32))
y = Tensor(np.ones([1,3,3,4]).astype(np.float32))

print(ops.add(x, y))
```

## Ascend 的启动脚本文件

1. run\_ascend.py



```
import sys
import os

from common import RunAscendLog
from common import RankTableEnv

from rank_table import RankTable, RankTableTemplate1, RankTableTemplate2

from manager import FMKManager

if __name__ == '__main__':
 log = RunAscendLog.setup_run_ascend_logger()

 if len(sys.argv) <= 1:
 log.error('there are not enough args')
 sys.exit(1)

 train_command = sys.argv[1:]
 log.info('training command')
 log.info(train_command)

 if os.environ.get(RankTableEnv.RANK_TABLE_FILE_V1) is not None:
 # new format rank table file
 rank_table_path = os.environ.get(RankTableEnv.RANK_TABLE_FILE_V1)
 RankTable.wait_for_available(rank_table_path)
 rank_table = RankTableTemplate1(rank_table_path)
 else:
 # old format rank table file
 rank_table_path_origin = RankTableEnv.get_rank_table_template2_file_path()
 RankTable.wait_for_available(rank_table_path_origin)
 rank_table = RankTableTemplate2(rank_table_path_origin)

 if rank_table.get_device_num() >= 1:
 log.info('set rank table %s env to %s' % (RankTableEnv.RANK_TABLE_FILE,
rank_table.get_rank_table_path()))
 RankTableEnv.set_rank_table_env(rank_table.get_rank_table_path())
 else:
 log.info('device num < 1, unset rank table %s env' % RankTableEnv.RANK_TABLE_FILE)
 RankTableEnv.unset_rank_table_env()

 instance = rank_table.get_current_instance()
 server = rank_table.get_server(instance.server_id)
 current_instance = RankTable.convert_server_to_instance(server)

 fmk_manager = FMKManager(current_instance)
 fmk_manager.run(rank_table.get_device_num(), train_command)
 return_code = fmk_manager.monitor()

 fmk_manager.destroy()

 sys.exit(return_code)
```

## 2. common.py

```
import logging
import os

logo = 'Training'

Rank Table Constants
class RankTableEnv:
 RANK_TABLE_FILE = 'RANK_TABLE_FILE'

 RANK_TABLE_FILE_V1 = 'RANK_TABLE_FILE_V1_0'

 HCCL_CONNECT_TIMEOUT = 'HCCL_CONNECT_TIMEOUT'

 # jobstart_hccl.json is provided by the volcano controller of Cloud-Container-Engine(CCE)
```

```
HCCL_JSON_FILE_NAME = 'jobstart_hccl.json'

RANK_TABLE_FILE_DEFAULT_VALUE = '/user/config/%s' % HCCL_JSON_FILE_NAME

@staticmethod
def get_rank_table_template1_file_dir():
 parent_dir = os.environ[ModelArts.MA_MOUNT_PATH_ENV]
 return os.path.join(parent_dir, 'rank_table')

@staticmethod
def get_rank_table_template2_file_path():
 rank_table_file_path = os.environ.get(RankTableEnv.RANK_TABLE_FILE)
 if rank_table_file_path is None:
 return RankTableEnv.RANK_TABLE_FILE_DEFAULT_VALUE

 return os.path.join(os.path.normpath(rank_table_file_path), RankTableEnv.HCCL_JSON_FILE_NAME)

@staticmethod
def set_rank_table_env(path):
 os.environ[RankTableEnv.RANK_TABLE_FILE] = path

@staticmethod
def unset_rank_table_env():
 del os.environ[RankTableEnv.RANK_TABLE_FILE]

class ModelArts:
 MA_MOUNT_PATH_ENV = 'MA_MOUNT_PATH'
 MA_CURRENT_INSTANCE_NAME_ENV = 'MA_CURRENT_INSTANCE_NAME'
 MA_VJ_NAME = 'MA_VJ_NAME'

 MA_CURRENT_HOST_IP = 'MA_CURRENT_HOST_IP'

 CACHE_DIR = '/cache'

 TMP_LOG_DIR = '/tmp/log/'

 FMK_WORKSPACE = 'workspace'

 @staticmethod
 def get_current_instance_name():
 return os.environ[ModelArts.MA_CURRENT_INSTANCE_NAME_ENV]

 @staticmethod
 def get_current_host_ip():
 return os.environ.get(ModelArts.MA_CURRENT_HOST_IP)

 @staticmethod
 def get_job_id():
 ma_vj_name = os.environ[ModelArts.MA_VJ_NAME]
 return ma_vj_name.replace('ma-job', 'modelarts-job', 1)

 @staticmethod
 def get_parent_working_dir():
 if ModelArts.MA_MOUNT_PATH_ENV in os.environ:
 return os.path.join(os.environ.get(ModelArts.MA_MOUNT_PATH_ENV),
ModelArts.FMK_WORKSPACE)

 return ModelArts.CACHE_DIR

class RunAscendLog:

 @staticmethod
 def setup_run_ascend_logger():
 name = logo
 formatter = logging.Formatter(fmt='[run ascend] %(asctime)s - %(levelname)s - %(message)s')

 handler = logging.StreamHandler()
```

```
handler.setFormatter(formatter)

logger = logging.getLogger(name)
logger.setLevel(logging.INFO)
logger.addHandler(handler)
logger.propagate = False
return logger

@staticmethod
def get_run_ascend_logger():
 return logging.getLogger(logo)
```

### 3. rank\_table.py

```
import json
import time
import os

from common import ModelArts
from common import RunAscendLog
from common import RankTableEnv

log = RunAscendLog.get_run_ascend_logger()

class Device:
 def __init__(self, device_id, device_ip, rank_id):
 self.device_id = device_id
 self.device_ip = device_ip
 self.rank_id = rank_id

class Instance:
 def __init__(self, pod_name, server_id, devices):
 self.pod_name = pod_name
 self.server_id = server_id
 self.devices = self.parse_devices(devices)

 @staticmethod
 def parse_devices(devices):
 if devices is None:
 return []
 device_object_list = []
 for device in devices:
 device_object_list.append(Device(device['device_id'], device['device_ip'], ""))

 return device_object_list

 def set_devices(self, devices):
 self.devices = devices

class Group:
 def __init__(self, group_name, device_count, instance_count, instance_list):
 self.group_name = group_name
 self.device_count = int(device_count)
 self.instance_count = int(instance_count)
 self.instance_list = self.parse_instance_list(instance_list)

 @staticmethod
 def parse_instance_list(instance_list):
 instance_object_list = []
 for instance in instance_list:
 instance_object_list.append(
 Instance(instance['pod_name'], instance['server_id'], instance['devices']))

 return instance_object_list
```

```
class RankTable:
 STATUS_FIELD = 'status'
 COMPLETED_STATUS = 'completed'

 def __init__(self):
 self.rank_table_path = ""
 self.rank_table = {}

 @staticmethod
 def read_from_file(file_path):
 with open(file_path) as json_file:
 return json.load(json_file)

 @staticmethod
 def wait_for_available(rank_table_file, period=1):
 log.info('Wait for Rank table file at %s ready' % rank_table_file)
 complete_flag = False
 while not complete_flag:
 with open(rank_table_file) as json_file:
 data = json.load(json_file)
 if data[RankTable.STATUS_FIELD] == RankTable.COMPLETED_STATUS:
 log.info('Rank table file is ready for read')
 log.info('\n' + json.dumps(data, indent=4))
 return True

 time.sleep(period)

 return False

 @staticmethod
 def convert_server_to_instance(server):
 device_list = []
 for device in server['device']:
 device_list.append(
 Device(device_id=device['device_id'], device_ip=device['device_ip'], rank_id=device['rank_id']))

 ins = Instance(pod_name="", server_id=server['server_id'], devices=[])
 ins.set_devices(device_list)
 return ins

 def get_rank_table_path(self):
 return self.rank_table_path

 def get_server(self, server_id):
 for server in self.rank_table['server_list']:
 if server['server_id'] == server_id:
 log.info('Current server')
 log.info('\n' + json.dumps(server, indent=4))
 return server

 log.error('server [%s] is not found' % server_id)
 return None

class RankTableTemplate2(RankTable):

 def __init__(self, rank_table_template2_path):
 super().__init__()

 json_data = self.read_from_file(file_path=rank_table_template2_path)

 self.status = json_data[RankTableTemplate2.STATUS_FIELD]
 if self.status != RankTableTemplate2.COMPLETED_STATUS:
 return

 # sorted instance list by the index of instance
 # assert there is only one group
 json_data["group_list"][0]["instance_list"] = sorted(json_data["group_list"][0]["instance_list"],
 key=RankTableTemplate2.get_index)
```

```
self.group_count = int(json_data['group_count'])
self.group_list = self.parse_group_list(json_data['group_list'])

self.rank_table_path, self.rank_table = self.convert_template2_to_template1_format_file()

@staticmethod
def parse_group_list(group_list):
 group_object_list = []
 for group in group_list:
 group_object_list.append(
 Group(group['group_name'], group['device_count'], group['instance_count'],
group['instance_list']))

 return group_object_list

@staticmethod
def get_index(instance):
 # pod_name example: job94dc1dbf-job-bj4-yolov4-15
 pod_name = instance["pod_name"]
 return int(pod_name[pod_name.rfind("-") + 1:])

def get_current_instance(self):
 """
 get instance by pod name
 specially, return the first instance when the pod name is None
 :return:
 """
 pod_name = ModelArts.get_current_instance_name()
 if pod_name is None:
 if len(self.group_list) > 0:
 if len(self.group_list[0].instance_list) > 0:
 return self.group_list[0].instance_list[0]

 return None

 for group in self.group_list:
 for instance in group.instance_list:
 if instance.pod_name == pod_name:
 return instance
 return None

def convert_template2_to_template1_format_file(self):
 rank_table_template1_file = {
 'status': 'completed',
 'version': '1.0',
 'server_count': '0',
 'server_list': []
 }

 logic_index = 0
 server_map = {}
 # collect all devices in all groups
 for group in self.group_list:
 if group.device_count == 0:
 continue
 for instance in group.instance_list:
 if instance.server_id not in server_map:
 server_map[instance.server_id] = []

 for device in instance.devices:
 template1_device = {
 'device_id': device.device_id,
 'device_ip': device.device_ip,
 'rank_id': str(logic_index)
 }
 logic_index += 1
 server_map[instance.server_id].append(template1_device)
```

```
server_count = 0
for server_id in server_map:
 rank_table_template1_file['server_list'].append({
 'server_id': server_id,
 'device': server_map[server_id]
 })
 server_count += 1

rank_table_template1_file['server_count'] = str(server_count)

log.info('Rank table file (Template1)')
log.info('\n' + json.dumps(rank_table_template1_file, indent=4))

if not os.path.exists(RankTableEnv.get_rank_table_template1_file_dir()):
 os.makedirs(RankTableEnv.get_rank_table_template1_file_dir())

path = os.path.join(RankTableEnv.get_rank_table_template1_file_dir(),
RankTableEnv.HCCL_JSON_FILE_NAME)
with open(path, 'w') as f:
 f.write(json.dumps(rank_table_template1_file))
 log.info('Rank table file (Template1) is generated at %s', path)

return path, rank_table_template1_file

def get_device_num(self):
 total_device_num = 0
 for group in self.group_list:
 total_device_num += group.device_count
 return total_device_num

class RankTableTemplate1(RankTable):
 def __init__(self, rank_table_template1_path):
 super().__init__()
 self.rank_table_path = rank_table_template1_path
 self.rank_table = self.read_from_file(file_path=rank_table_template1_path)

 def get_current_instance(self):
 current_server = None
 server_list = self.rank_table['server_list']
 if len(server_list) == 1:
 current_server = server_list[0]
 elif len(server_list) > 1:
 host_ip = ModelArts.get_current_host_ip()
 if host_ip is not None:
 for server in server_list:
 if server['server_id'] == host_ip:
 current_server = server
 break
 else:
 current_server = server_list[0]

 if current_server is None:
 log.error('server is not found')
 return None
 return self.convert_server_to_instance(current_server)

 def get_device_num(self):
 server_list = self.rank_table['server_list']
 device_num = 0
 for server in server_list:
 device_num += len(server['device'])
 return device_num
```

#### 4. manager.py

```
import time
import os
import os.path
```

```
import signal

from common import RunAscendLog
from fmk import FMK

log = RunAscendLog.get_run_ascend_logger()

class FMKManager:
 # max destroy time: ~20 (15 + 5)
 # ~ 15 (1 + 2 + 4 + 8)
 MAX_TEST_PROC_CNT = 4

 def __init__(self, instance):
 self.instance = instance
 self.fmk = []
 self.fmk_processes = []
 self.get_sigterm = False
 self.max_test_proc_cnt = FMKManager.MAX_TEST_PROC_CNT

 # break the monitor and destroy processes when get terminate signal
 def term_handle(func):
 def receive_term(signum, stack):
 log.info('Received terminate signal %d, try to destroyed all processes' % signum)
 stack.f_locals['self'].get_sigterm = True

 def handle_func(self, *args, **kwargs):
 origin_handle = signal.getsignal(signal.SIGTERM)
 signal.signal(signal.SIGTERM, receive_term)
 res = func(self, *args, **kwargs)
 signal.signal(signal.SIGTERM, origin_handle)
 return res

 return handle_func

 def run(self, rank_size, command):
 for index, device in enumerate(self.instance.devices):
 fmk_instance = FMK(index, device)
 self.fmk.append(fmk_instance)

 self.fmk_processes.append(fmk_instance.run(rank_size, command))

 @term_handle
 def monitor(self, period=1):
 # busy waiting for all fmk processes exit by zero
 # or there is one process exit by non-zero

 fmk_cnt = len(self.fmk_processes)
 zero_ret_cnt = 0
 while zero_ret_cnt != fmk_cnt:
 zero_ret_cnt = 0
 for index in range(fmk_cnt):
 fmk = self.fmk[index]
 fmk_process = self.fmk_processes[index]
 if fmk_process.poll() is not None:
 if fmk_process.returncode != 0:
 log.error('proc-rank-%s-device-%s (pid: %d) has exited with non-zero code: %d'
 % (fmk.rank_id, fmk.device_id, fmk_process.pid, fmk_process.returncode))
 return fmk_process.returncode

 zero_ret_cnt += 1
 if self.get_sigterm:
 break
 time.sleep(period)

 return 0

 def destroy(self, base_period=1):
```

```
log.info('Begin destroy training processes')
self.send_sigterm_to_fm_k_process()
self.wait_fm_k_process_end(base_period)
log.info('End destroy training processes')

def send_sigterm_to_fm_k_process(self):
 # send SIGTERM to fm_k processes (and process group)
 for r_index in range(len(self.fm_k_processes) - 1, -1, -1):
 fm_k = self.fm_k[r_index]
 fm_k_process = self.fm_k_processes[r_index]
 if fm_k_process.poll() is not None:
 log.info('proc-rank-%s-device-%s (pid: %d) has exited before receiving the term signal',
 fm_k.rank_id, fm_k.device_id, fm_k_process.pid)
 del self.fm_k_processes[r_index]
 del self.fm_k[r_index]

 try:
 os.killpg(fm_k_process.pid, signal.SIGTERM)
 except ProcessLookupError:
 pass

def wait_fm_k_process_end(self, base_period):
 test_cnt = 0
 period = base_period
 while len(self.fm_k_processes) > 0 and test_cnt < self.max_test_proc_cnt:
 for r_index in range(len(self.fm_k_processes) - 1, -1, -1):
 fm_k = self.fm_k[r_index]
 fm_k_process = self.fm_k_processes[r_index]
 if fm_k_process.poll() is not None:
 log.info('proc-rank-%s-device-%s (pid: %d) has exited',
 fm_k.rank_id, fm_k.device_id, fm_k_process.pid)
 del self.fm_k_processes[r_index]
 del self.fm_k[r_index]
 if not self.fm_k_processes:
 break

 time.sleep(period)
 period *= 2
 test_cnt += 1

 if len(self.fm_k_processes) > 0:
 for r_index in range(len(self.fm_k_processes) - 1, -1, -1):
 fm_k = self.fm_k[r_index]
 fm_k_process = self.fm_k_processes[r_index]
 if fm_k_process.poll() is None:
 log.warn('proc-rank-%s-device-%s (pid: %d) has not exited within the max waiting time, '
 'send kill signal',
 fm_k.rank_id, fm_k.device_id, fm_k_process.pid)
 os.killpg(fm_k_process.pid, signal.SIGKILL)
```

## 5. fm\_k.py

```
import os
import subprocess
import pathlib
from contextlib import contextmanager

from common import RunAscendLog
from common import RankTableEnv
from common import ModelArts

log = RunAscendLog.get_run_ascend_logger()

class FMK:

 def __init__(self, index, device):
 self.job_id = ModelArts.get_job_id()
 self.rank_id = device.rank_id
```



```
self.device_id = str(index)

def gen_env_for_fmkl(self, rank_size):
 current_envs = os.environ.copy()

 current_envs['JOB_ID'] = self.job_id

 current_envs['ASCEND_DEVICE_ID'] = self.device_id
 current_envs['DEVICE_ID'] = self.device_id

 current_envs['RANK_ID'] = self.rank_id
 current_envs['RANK_SIZE'] = str(rank_size)

 FMK.set_env_if_not_exist(current_envs, RankTableEnv.HCCL_CONNECT_TIMEOUT, str(1800))

 log_dir = FMK.get_log_dir()
 process_log_path = os.path.join(log_dir, self.job_id, 'ascend', 'process_log', 'rank_' + self.rank_id)
 FMK.set_env_if_not_exist(current_envs, 'ASCEND_PROCESS_LOG_PATH', process_log_path)
 pathlib.Path(current_envs['ASCEND_PROCESS_LOG_PATH']).mkdir(parents=True, exist_ok=True)

 return current_envs

@contextmanager
def switch_directory(self, directory):
 owd = os.getcwd()
 try:
 os.chdir(directory)
 yield directory
 finally:
 os.chdir(owd)

def get_working_dir(self):
 fmk_workspace_prefix = ModelArts.get_parent_working_dir()
 return os.path.join(os.path.normpath(fmk_workspace_prefix), 'device%s' % self.device_id)

@staticmethod
def get_log_dir():
 parent_path = os.getenv(ModelArts.MA_MOUNT_PATH_ENV)
 if parent_path:
 log_path = os.path.join(parent_path, 'log')
 if os.path.exists(log_path):
 return log_path

 return ModelArts.TMP_LOG_DIR

@staticmethod
def set_env_if_not_exist(envs, env_name, env_value):
 if env_name in os.environ:
 log.info('env already exists. env_name: %s, env_value: %s ' % (env_name, env_value))
 return

 envs[env_name] = env_value

def run(self, rank_size, command):
 envs = self.gen_env_for_fmkl(rank_size)
 log.info('bootstrap proc-rank-%s-device-%s' % (self.rank_id, self.device_id))

 log_dir = FMK.get_log_dir()
 if not os.path.exists(log_dir):
 os.makedirs(log_dir)

 log_file = '%s-proc-rank-%s-device-%s.txt' % (self.job_id, self.rank_id, self.device_id)
 log_file_path = os.path.join(log_dir, log_file)

 working_dir = self.get_working_dir()
 if not os.path.exists(working_dir):
 os.makedirs(working_dir)

 with self.switch_directory(working_dir):
```

```
os.setsid: change the process(forked) group id to itself
training_proc = subprocess.Popen(command, env=envs, preexec_fn=os.setsid,
 stdout=subprocess.PIPE, stderr=subprocess.STDOUT)

log.info('proc-rank-%s-device-%s (pid: %d)', self.rank_id, self.device_id, training_proc.pid)

https://docs.python.org/3/library/subprocess.html#subprocess.Popen.wait
subprocess.Popen(['tee', log_file_path], stdin=training_proc.stdout)

return training_proc
```

## 10.8.4 Step3 制作自定义镜像

此处介绍如何通过编写 Dockerfile 文件制作自定义镜像的操作步骤。

目标：构建安装好如下软件的容器镜像，并使用 ModelArts 训练服务运行。

- ubuntu-18.04
- cann-6.3.RC2 (商用版本)
- python-3.7.13
- mindspore-2.1.1

### 📖 说明

Mindspore 版本与 CANN 版本，CANN 版本和Ascend驱动/固件版本均有严格的匹配关系，版本不匹配会导致训练失败。

本示例仅用于示意Ascend容器镜像制作流程，且在匹配正确的Ascend驱动/固件版本的专属资源池上运行通过。

1. 准备一台 Linux **aarch64** 架构的主机，操作系统使用ubuntu-18.04。您可以准备相同规格的 弹性云服务器ECS 或者应用本地已有的主机进行自定义镜像的制作。购买ECS服务器的具体操作请参考[购买并登录Linux弹性云服务器](#)。镜像选择公共镜像，推荐使用ubuntu18.04的镜像。

图 10-69 创建 ECS 服务器-选择 X86 架构的公共镜像



2. 安装 Docker。

以 Linux **aarch64** 架构的操作系统为例，获取 Docker 安装包。您可以使用以下指令安装 Docker。关于安装 Docker 的更多指导内容参见 [Docker 官方文档](#)。

```
curl -fsSL get.docker.com -o get-docker.sh
sh get-docker.sh
```

如果 **docker images** 命令可以执行成功，表示 Docker 已安装，此步骤可跳过。

启动docker。

```
systemctl start docker
```

3. 确认 Docker Engine 版本。执行如下命令。

```
docker version | grep -A 1 Engine
```

命令回显如下。

```
Engine:
Version: 18.09.0
```

#### 说明

推荐使用大于等于该版本的 Docker Engine 来制作自定义镜像。

4. 准备名为 context 的文件夹。

```
mkdir -p context
```

5. 准备可用的 pip 源文件 pip.conf。本示例使用华为开源镜像站提供的 pip 源，其 pip.conf 文件内容如下。

```
[global]
index-url = https://repo.huaweicloud.com/repository/pypi/simple
trusted-host = repo.huaweicloud.com
timeout = 120
```

#### 说明

在华为开源镜像站 <https://mirrors.huaweicloud.com/home> 中，搜索 pypi，可以查看 pip.conf 文件内容。

6. 准备可用的 apt 源文件 Ubuntu-Ports-bionic.list。本示例使用华为开源镜像站提供的 apt 源，执行如下命令获取 apt 源文件。

```
wget -O Ubuntu-Ports-bionic.list https://repo.huaweicloud.com/repository/conf/Ubuntu-Ports-bionic.list
```

#### 说明

在华为开源镜像站 <https://mirrors.huaweicloud.com/home> 中，搜索 Ubuntu-Ports，可以查看获取 apt 源文件的命令。

7. 下载 CANN 6.3.RC2-linux aarch64 与 mindspore-2.1.1-cp37-cp37m-linux\_aarch64.whl 安装文件。

- 下载run文件“Ascend-cann-nnae\_6.3.RC2\_linux-aarch64.run”（[下载链接](#)）。
- 下载whl文件“mindspore-2.1.1-cp37-cp37m-linux\_aarch64.whl”（[下载链接](#)）。

#### 说明

ModelArts当前仅支持CANN商用版本，不支持社区版。

8. 下载 Miniconda3 安装文件。

使用地址 [https://repo.anaconda.com/miniconda/Miniconda3-py37\\_4.10.3-Linux-aarch64.sh](https://repo.anaconda.com/miniconda/Miniconda3-py37_4.10.3-Linux-aarch64.sh)，下载 Miniconda3-py37-4.10.3 安装文件（对应 python 3.7.10）。

9. 将上述 pip 源文件、\*.run 文件、\*.whl 文件、Miniconda3 安装文件放置在 context 文件夹内，context 文件夹内容如下。

```
context
├── Ascend-cann-nnae_6.3.RC2_linux-aarch64.run
├── mindspore-2.1.1-cp37-cp37m-linux_aarch64.whl
├── Miniconda3-py37_4.10.3-Linux-aarch64.sh
├── pip.conf
└── Ubuntu-Ports-bionic.list
```

10. 编写容器镜像 Dockerfile 文件。

在 context 文件夹内新建名为 Dockerfile 的空文件，并将下述内容写入其中。

```
容器镜像构建主机需要连通公网
FROM arm64v8/ubuntu:18.04 AS builder

基础容器镜像的默认用户已经是 root
USER root

安装 OS 依赖（使用华为开源镜像站）
COPY Ubuntu-Ports-bionic.list /tmp
RUN cp -a /etc/apt/sources.list /etc/apt/sources.list.bak && \
 mv /tmp/Ubuntu-Ports-bionic.list /etc/apt/sources.list && \
 echo > /etc/apt/apt.conf.d/00skip-verify-peer.conf "Acquire { https::Verify-Peer false }" && \
 apt-get update && \
 apt-get install -y \
 # utils
 ca-certificates vim curl \
 # CANN 6.3.RC2
 gcc-7 g++ make cmake zlib1g zlib1g-dev openssl libsqlite3-dev libssl-dev libffi-dev unzip pciutils
 net-tools libblas-dev gfortran libblas3 && \
 apt-get clean && \
 mv /etc/apt/sources.list.bak /etc/apt/sources.list && \
 # 修改 CANN 6.3.RC2 安装目录的父目录权限，使得 ma-user 可以写入
 chmod o+w /usr/local

RUN useradd -m -d /home/ma-user -s /bin/bash -g 100 -u 1000 ma-user

设置容器镜像默认用户与工作目录
USER ma-user
WORKDIR /home/ma-user

使用华为开源镜像站提供的 pypi 配置
RUN mkdir -p /home/ma-user/.pip/
COPY --chown=ma-user:100 pip.conf /home/ma-user/.pip/pip.conf

复制待安装文件到基础容器镜像中的 /tmp 目录
COPY --chown=ma-user:100 Miniconda3-py37_4.10.3-Linux-aarch64.sh /tmp

https://conda.io/projects/conda/en/latest/user-guide/install/linux.html#installing-on-linux
安装 Miniconda3 到基础容器镜像的 /home/ma-user/miniconda3 目录中
RUN bash /tmp/Miniconda3-py37_4.10.3-Linux-aarch64.sh -b -p /home/ma-user/miniconda3

ENV PATH=$PATH:/home/ma-user/miniconda3/bin

安装 CANN 6.3.RC2 Python Package 依赖
RUN pip install numpy~=1.14.3 decorator~=4.4.0 sympy~=1.4 cffi~=1.12.3 protobuf~=3.11.3 \
 attrs pyyaml pathlib2 scipy requests psutil absl-py

安装 CANN 6.3.RC2 至 /usr/local/Ascend 目录
COPY --chown=ma-user:100 Ascend-cann-nae_6.3.RC2_linux-aarch64.run /tmp
RUN chmod +x /tmp/Ascend-cann-nae_6.3.RC2_linux-aarch64.run && \
 /tmp/Ascend-cann-nae_6.3.RC2_linux-aarch64.run --install --install-path=/usr/local/Ascend

安装 MindSpore 2.1.1
COPY --chown=ma-user:100 mindspore-2.1.1-cp37-cp37m-linux_aarch64.whl /tmp
RUN chmod +x /tmp/mindspore-2.1.1-cp37-cp37m-linux_aarch64.whl && \
 pip install /tmp/mindspore-2.1.1-cp37-cp37m-linux_aarch64.whl

构建最终容器镜像
FROM arm64v8/ubuntu:18.04

安装 OS 依赖（使用华为开源镜像站）
COPY Ubuntu-Ports-bionic.list /tmp
RUN cp -a /etc/apt/sources.list /etc/apt/sources.list.bak && \
 mv /tmp/Ubuntu-Ports-bionic.list /etc/apt/sources.list && \
 echo > /etc/apt/apt.conf.d/00skip-verify-peer.conf "Acquire { https::Verify-Peer false }" && \
 apt-get update && \
 apt-get install -y \
 # utils
 ca-certificates vim curl \
 # CANN 6.3.RC2
```

```
gcc-7 g++ make cmake zlib1g zlib1g-dev openssl libsqlite3-dev libssl-dev libffi-dev unzip pciutils
net-tools libblas-dev gfortran libblas3 && \
apt-get clean && \
mv /etc/apt/sources.list.bak /etc/apt/sources.list

RUN useradd -m -d /home/ma-user -s /bin/bash -g 100 -u 1000 ma-user

从上述 builder stage 中复制目录到当前容器镜像的同名目录
COPY --chown=ma-user:100 --from=builder /home/ma-user/miniconda3 /home/ma-user/miniconda3
COPY --chown=ma-user:100 --from=builder /home/ma-user/Ascend /home/ma-user/Ascend
COPY --chown=ma-user:100 --from=builder /home/ma-user/var /home/ma-user/var
COPY --chown=ma-user:100 --from=builder /usr/local/Ascend /usr/local/Ascend

设置容器镜像预置环境变量
请务必设置 CANN 相关环境变量
请务必设置 Ascend Driver 相关环境变量
请务必设置 PYTHONUNBUFFERED=1, 以免日志丢失
ENV PATH=$PATH:/usr/local/Ascend/nnae/latest/bin:/usr/local/Ascend/nnae/latest/compiler/
ccec_compiler/bin:/home/ma-user/miniconda3/bin \
LD_LIBRARY_PATH=$LD_LIBRARY_PATH:/usr/local/Ascend/driver/lib64:/usr/local/Ascend/driver/
lib64/common:/usr/local/Ascend/driver/lib64/driver:/usr/local/Ascend/nnae/latest/lib64:/usr/local/
Ascend/nnae/latest/lib64/plugin/opskernel:/usr/local/Ascend/nnae/latest/lib64/plugin/nnengine \
PYTHONPATH=$PYTHONPATH:/usr/local/Ascend/nnae/latest/python/site-packages:/usr/local/
Ascend/nnae/latest/opp/built-in/op_impl/ai_core/tbe \
ASCEND_AICPU_PATH=/usr/local/Ascend/nnae/latest \
ASCEND_OPP_PATH=/usr/local/Ascend/nnae/latest/opp \
ASCEND_HOME_PATH=/usr/local/Ascend/nnae/latest \
PYTHONUNBUFFERED=1

设置容器镜像默认用户与工作目录
USER ma-user
WORKDIR /home/ma-user
```

关于 Dockerfile 文件编写的更多指导内容参见 [Docker 官方文档](#)。

11. 确认已创建完成 Dockerfile 文件。此时 context 文件夹内容如下。

```
context
├── Ascend-cann-nnae_6.3.RC2_linux-aarch64.run
├── Dockerfile
├── mindspore-2.1.1-cp37-cp37m-linux_aarch64.whl
├── Miniconda3-py37_4.10.3-Linux-aarch64.sh
├── pip.conf
└── Ubuntu-Ports-bionic.list
```

12. 构建容器镜像。在 Dockerfile 文件所在的目录执行如下命令构建容器镜像。

```
docker build . -t mindspore:2.1.1-cann6.3.RC2
```

构建过程结束时出现如下构建日志说明镜像构建成功。

```
Successfully tagged mindspore:2.1.1-cann6.3.RC2
```

13. 将制作完成的镜像上传至SWR服务，具体参见[Step4 上传镜像至SWR](#)。

## 10.8.5 Step4 上传镜像至 SWR

本章节介绍如何将制作好的镜像上传至SWR服务，方便后续在ModelArts上创建训练作业时调用。

1. 登录容器镜像服务控制台，选择区域。

图 10-70 容器镜像服务控制台



- 单击右上角“创建组织”，输入组织名称完成组织创建。请自定义组织名称，本示例使用“deep-learning”，下面的命令中涉及到组织名称“deep-learning”也请替换为自定义的值。

图 10-71 创建组织


### 创建组织


1.组织名称，全局唯一。  
2.当前租户最多可创建5个组织。  
3.建议一个组织对应一个公司、部门或个人，以便集中高效地管理镜像资源。  
示例：  
以公司、部门作为组织:cloud-hangzhou、cloud-develop  
以个人作为组织:john

组织名称

- 单击右上角“登录指令”，获取登录访问指令。

图 10-72 登录指令

 **登录指令** ×

```
docker login -u cn-north-4@\[redacted] W9 -p 2f2
[redacted] 9
41374cc204 swr.cn-north-4.myhuaweicloud.com 
```

过期时间：2021/03/16 16:40:45 GMT+08:00

- 以root用户登录本地环境，输入登录访问指令。
- 上传镜像至容器镜像服务镜像仓库。
  - 使用docker tag命令给上传镜像打标签。  
#region和domain信息请替换为实际值，组织名称deep-learning也请替换为自定义的值。  
sudo docker tag mindspore:2.1.1-cann6.3.RC2 swr.{region}.{domain}/deep-learning/  
mindspore:2.1.1-cann6.3.RC2  
#以华为云北京四为例：  
sudo docker tag mindspore:2.1.1-cann6.3.RC2 swr.cn-north-4.myhuaweicloud.com/deep-learning/  
mindspore:2.1.1-cann6.3.RC2
  - 使用docker push命令上传镜像。  
#region和domain信息请替换为实际值，组织名称deep-learning也请替换为自定义的值。  
sudo docker push swr.{region}.{domain}/deep-learning/mindspore:2.1.1-cann6.3.RC2  
#以华为云北京四为例：  
sudo docker push swr.cn-north-4.myhuaweicloud.com/deep-learning/mindspore:2.1.1-cann6.3.RC2
- 完成镜像上传后，在“容器镜像服务控制台>我的镜像”页面可查看已上传的自定义镜像。  
“swr.cn-north-4.myhuaweicloud.com/deep-learning/mindspore:2.1.1-cann6.3.RC2”即为此自定义镜像的“SWR\_URL”。

## 10.8.6 Step5 在 ModelArts 上创建 Notebook 并调试

1. 将[上传到SWR上的镜像](#)注册到ModelArts的镜像管理中。  
登录ModelArts管理控制台，在左侧导航栏中选择“镜像管理”，单击“注册镜像”，根据界面提示注册镜像。注册后的镜像可以用于创建Notebook。
2. 在Notebook中使用自定义镜像创建Notebook并调试，调试成功后，保存镜像。
  - a. 在Notebook中使用自定义镜像创建Notebook操作请参见[基于自定义镜像创建Notebook实例](#)。
  - b. 保存Notebook镜像操作请参见[保存Notebook镜像环境](#)。
3. 已有的镜像调试成功后，再[使用ModelArts训练模块训练作业](#)。

## 10.8.7 Step6 在 ModelArts 上创建训练作业

1. 登录ModelArts管理控制台，在左侧导航栏中选择“训练管理 > 训练作业 New”，默认进入“训练作业”列表。
2. 在“创建训练作业”页面，填写相关参数信息，然后单击“提交”。
  - 创建方式：选择“自定义算法”
  - 启动方式：选择“自定义”
  - 镜像地址：“swr.cn-north-4.myhuaweicloud.com/deep-learning/mindspore:2.1.1-cann6.3.RC2”
  - 代码目录：设置为OBS中存放启动脚本文件的目录，例如：“obs://test-modelarts/ascend/demo-code/”
  - 启动命令：“python \${MA\_JOB\_DIR}/demo-code/run\_ascend/run\_ascend.py python \${MA\_JOB\_DIR}/demo-code/mindspore-verification.py”
  - 资源池：选择专属资源池
  - 类型：选择驱动/固件版本匹配的专属资源池 Ascend 规格。
  - 作业日志路径：设置为OBS中存放训练日志的路径。例如：“obs://test-modelarts/ascend/log/”
3. 在“规格确认”页面，确认训练作业的参数信息，确认无误后单击“提交”。
4. 训练作业创建完成后，后台将自动完成容器镜像下载、代码目录下载、执行启动命令等动作。

训练作业一般需要运行一段时间，根据您的训练业务逻辑和选择的资源不同，训练时长将持续几十分钟到几小时不等。训练作业执行成功后，日志信息如[图10-73](#)所示。

图 10-73 专属资源池 Ascend 规格运行日志信息

```
75 Ascend Envs
76 -----
77 JOB_ID: modelarts-job-2436291a-8543-4ab8-84ad-2dda8f1e4f5c
78 RANK_TABLE_FILE: /home/ma-user/modelarts/rank_table/jobstart_hcc1.json
79 RANK_SIZE: 1
80 ASCEND_DEVICE_ID: 0
81 DEVICE_ID: 0
82 RANK_ID: 0
83 -----
84 [2. 2. 2. 2.]
85 [2. 2. 2. 2.]]
86
87 [[2. 2. 2. 2.]
88 [2. 2. 2. 2.]
89 [2. 2. 2. 2.]]]
90
91 [[2. 2. 2. 2.]
92 [2. 2. 2. 2.]
93 [2. 2. 2. 2.]]]]
```



# 11 推理部署

## 11.1 免费体验：一键完成商超商品识别模型部署

ModelArts的AI Gallery中提供了大量免费的模型供用户一键部署，进行AI体验学习。

本文以“商超商品识别”模型为例，完成从AI Gallery订阅模型，到ModelArts一键部署为在线服务的免费体验过程。

“商超商品识别”模型可以识别81类常见超市商品（包括蔬菜、水果和饮品），并给出置信度最高的5类商品的置信度得分。

### 步骤 1：准备工作

- 已注册华为账号并开通华为云，进行了实名认证，且在使用ModelArts前检查账号状态，账号不能处于欠费或冻结状态。
  - [注册华为账号并开通华为云](#)
  - [进行实名认证](#)
- 配置委托访问授权

ModelArts使用过程中涉及到OBS、SWR、IEF等服务交互，首次使用ModelArts需要用户配置委托授权，允许访问这些依赖服务。

  - a. 使用华为云账号登录[ModelArts管理控制台](#)，在左侧导航栏单击“全局配置”，进入“全局配置”页面，单击“添加授权”。
  - b. 在“访问授权”页面，选择需要授权的“授权对象类型”，选择新增委托及其对应的权限“普通用户”，并勾选“我已经仔细阅读并同意《ModelArts服务声明》”，然后单击“创建”。

图 11-1 配置委托访问授权



- c. 完成配置后，在ModelArts控制台的全局配置列表，可查看到此账号的委托配置信息。

图 11-2 查看委托配置信息



## 步骤 2: 订阅模型

“商超商品识别”的模型共享在AI Gallery中。您可以前往AI Gallery，免费订阅此模型。

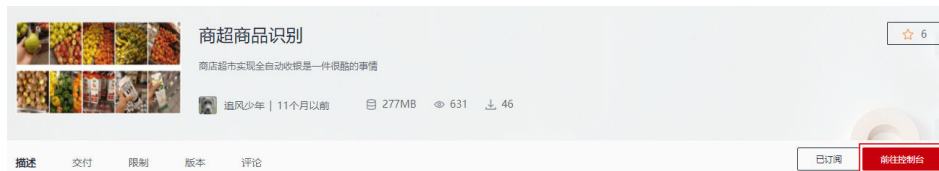
1. 单击案例链接[商超商品识别](#)，进入模型详情页。
2. 完成模型订阅。

在模型详情页，单击“订阅”，阅读并勾选同意《数据安全与隐私风险承担条款》和《华为云AI Gallery服务协议》，单击“继续订阅”。订阅模型完成后，页面的“订阅”按钮显示为“已订阅”。

3. 从模型详情页进入ModelArts控制台的订阅列表。

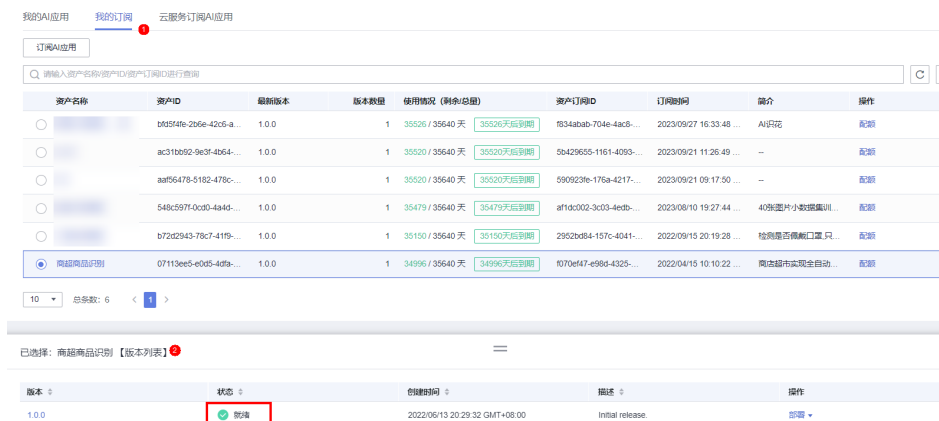
在模型详情页，单击“前往控制台”。在弹出的“选择云服务区域”页面选择ModelArts所在的云服务区域，单击“确定”跳转至ModelArts控制台的“AI应用管理 > AI应用 > 我的订阅”页面。

图 11-3 前往控制台



4. 在“我的订阅”列表，单击资产名称前面的单选按钮，在页面底部展开版本列表，当订阅模型的版本列表的状态显示为“就绪”时表示模型可以使用。

图 11-4 进入“我的订阅”



### 步骤 3: 使用订阅模型部署在线服务

模型订阅成功后，可将此模型部署为在线服务。

- 在“AI应用管理 > AI应用 > 我的订阅”页面，单击资产名称前面的单选按钮，在展开的版本列表中单击“部署 > 在线服务”跳转至部署页面。

图 11-5 部署模型



- 在部署页面，参考如下说明填写关键参数。
  - “名称”：自定义一个在线服务的名称，也可以使用默认值，此处以“商超商品识别服务”为例。
  - “资源池”：选择“公共资源池”。
  - “AI应用来源”和“选择AI应用及版本”：会自动选择订阅模型。
  - “计算节点规格”：在下拉框中选择“限时免费”资源，勾选并阅读免费规格说明。
 其他参数可使用默认值。

#### 📖 说明

如果限时免费资源售罄，建议选择收费CPU资源进行部署。当选择收费CPU资源部署在线服务时会收取少量资源费用，具体费用以界面信息为准。

图 11-6 部署在线服务



3. 参数配置完成后，单击“下一步”，确认规格参数后，单击“提交”启动在线服务的部署。
4. 任务提交成功后，单击“查看任务详情”，等待服务状态变为“运行中”时，表示服务部署成功。预计时长4分钟左右。

图 11-7 等待服务部署成功



## 步骤 4：预测结果

1. 在线服务部署完成后，单击“预测”页签。
2. 在“预测”页签，单击“上传”，上传一个测试图片，单击“预测”查看预测结果。此处提供一个样例图片供预测使用。

### 📖 说明

本案例中使用的订阅模型可以识别**81类**常见超市商品，模型对预测图片有一定范围和要求，不满足条件的图片会影响预测结果的准确性。

图 11-8 预测样例图



图 11-9 预测结果

调用指南 **预测** 配置更新记录 监控信息 事件 日志 标签

请求路径: / 选择预测图片文件 上传 重新预测

上传的预测文件大小不能超过8MB，否则上传文件会失败。详情请参见服务预测请求体大小限制。

预测图片预览



预测结果显示

预测成功

```
1 {
2 "predicted_label": "Orange",
3 "scores": [
4 [
5 "Orange",
6 "0.924"
7],
8 [
9 "Satsumas",
10 "0.035"
11],
12 [
13 "Red-Grapefruit",
14 "0.030"
15],
16 [
17 "Royal-Gala",
18 "0.007"
19],
20 [
21 "Kaiser",
22 "0.001"
23]
24]
25 }
```

## 步骤 5: 清理资源

体验结束后，建议暂停或删除服务，避免占用资源，造成资源浪费。

- 停止在线服务：在“在线服务”列表，单击对应服务操作列的“更多 > 停止”。
- 删除在线服务：在“在线服务”列表，单击对应服务操作列的“更多 > 删除”。

## 常见问题

- [订阅的AI应用一直处于等待同步状态](#)
- [服务预测失败](#)

## 11.2 从 0-1 制作自定义镜像并创建 AI 应用

针对ModelArts目前不支持的AI引擎，您可以针对该引擎构建自定义镜像，并将镜像导入ModelArts，创建为AI应用。本文详细介绍如何使用自定义镜像完成AI应用的创建，并部署成在线服务。

操作流程如下：

1. **本地构建镜像**：在本地制作自定义镜像包，镜像包规范可参考[创建AI应用的自定义镜像规范](#)。
2. **本地验证镜像并上传镜像至SWR服务**：验证自定义镜像的API接口功能，无误后将自定义镜像上传至SWR服务。
3. **将自定义镜像创建为AI应用**：将上传至SWR服务的镜像导入ModelArts的AI应用管理。
4. **将AI应用部署为在线服务**：将导入的模型部署上线。

## 本地构建镜像

以linux x86\_x64架构的主机为例，您可以购买相同规格的ECS或者应用本地已有的主机进行自定义镜像的制作。

购买ECS服务器的具体操作请参考[购买并登录弹性云服务器](#)。镜像选择公共镜像，推荐使用ubuntu18.04的镜像。

图 11-10 创建 ECS 服务器-选择 X86 架构的公共镜像



1. 登录主机后，安装Docker，可参考[Docker官方文档](#)。也可执行以下命令安装docker。

```
curl -fsSL get.docker.com -o get-docker.sh
sh get-docker.sh
```

2. 获取基础镜像。本示例以Ubuntu18.04为例。

```
docker pull ubuntu:18.04
```

3. 新建文件夹“self-define-images”，在该文件夹下编写自定义镜像的“Dockerfile”文件和应用服务代码“test\_app.py”。本样例代码中，应用服务代码采用了flask框架。

文件结构如下所示

```
self-define-images/
```

```
--Dockerfile
```

```
--test_app.py
```

– “Dockerfile”

```
From ubuntu:18.04
配置华为云的源，安装 python、python3-pip 和 Flask
RUN cp -a /etc/apt/sources.list /etc/apt/sources.list.bak && \
 sed -i "s@http://.*security.ubuntu.com@http://repo.huaweicloud.com@g" /etc/apt/sources.list && \
 sed -i "s@http://.*archive.ubuntu.com@http://repo.huaweicloud.com@g" /etc/apt/sources.list && \
 apt-get update && \
 apt-get install -y python3 python3-pip && \
 pip3 install --trusted-host https://repo.huaweicloud.com -i https://repo.huaweicloud.com/
 repository/pypi/simple Flask

复制应用服务代码进镜像里面
COPY test_app.py /opt/test_app.py

指定镜像的启动命令
CMD python3 /opt/test_app.py
```

– “test\_app.py”

```
from flask import Flask, request
import json
app = Flask(__name__)

@app.route('/greet', methods=['POST'])
def say_hello_func():
 print("----- in hello func -----")
 data = json.loads(request.get_data(as_text=True))
 print(data)
 username = data['name']
 rsp_msg = 'Hello, {}'.format(username)
 return json.dumps({"response":rsp_msg}, indent=4)

@app.route('/goodbye', methods=['GET'])
def say_goodbye_func():
 print("----- in goodbye func -----")
 return '\nGoodbye!\n'

@app.route('/', methods=['POST'])
def default_func():
 print("----- in default func -----")
 data = json.loads(request.get_data(as_text=True))
 return '\n called default func !\n {} \n'.format(str(data))

host must be "0.0.0.0", port must be 8080
if __name__ == '__main__':
 app.run(host="0.0.0.0", port=8080)
```

4. 进入“self-define-images”文件夹，执行以下命令构建自定义镜像“test:v1”。  

```
docker build -t test:v1 .
```
5. 您可以使用“docker images”查看您构建的自定义镜像。

## 本地验证镜像并上传镜像至 SWR 服务

1. 在本地环境执行以下命令启动自定义镜像  
docker run -it -p 8080:8080 test:v1

图 11-11 启动自定义镜像

```
:/opt/file# docker run -it -p 8080:8080 test:v1
* Serving Flask app "test_app" (lazy loading)
* Environment: production
 WARNING: This is a development server. Do not use it in a production deployment.
 Use a production WSGI server instead.
* Debug mode: off
* Running on http://0.0.0.0:8080/ (Press CTRL+C to quit)
```

2. 另开一个终端，执行以下命令验证自定义镜像的三个API接口功能。  
curl -X POST -H "Content-Type: application/json" --data '{"name":"Tom"}' 127.0.0.1:8080/  
curl -X POST -H "Content-Type: application/json" --data '{"name":"Tom"}' 127.0.0.1:8080/greet  
curl -X GET 127.0.0.1:8080/goodbye

如果验证自定义镜像功能成功，结果如下图所示。

图 11-12 校验接口

```
root@: ~# curl -X POST -H "Content-Type: application/json" --data '{"name":"Tom"}' 127.0.0.1:8080/
called default func !
{"name": "Tom"}
root@: ~# curl -X POST -H "Content-Type: application/json" --data '{"name":"Tom"}' 127.0.0.1:8080/greet
{
 "response": "Hello, Tom!"
}root@: ~# curl -X GET 127.0.0.1:8080/goodbye
Goodbye!
```

3. 上传自定义镜像至SWR服务。上传镜像的详细操作可参考[如何登录并上传镜像到SWR](#)。
4. 完成自定义镜像上传后，您可以在“容器镜像服务>我的镜像>自有镜像”列表中看到已上传镜像。

图 11-13 上传镜像列表



## 将自定义镜像创建为 AI 应用

参考[从容器镜像中选择元模型](#)导入元模型，您需要特别关注以下参数：

- 元模型来源：选择“从容器镜像中选择”
  - 容器镜像所在的路径：选择已制作好的自有镜像

图 11-14 选择已制作好的自有镜像





- 容器调用接口：指定模型启动的协议和端口号。请确保协议和端口号与自定义镜像中提供的协议和端口号保持一致。
- 镜像复制：选填，选择是否将容器镜像中的模型镜像复制到ModelArts中。
- 健康检查：选填，用于指定模型的健康检查。仅当自定义镜像中配置了健康检查接口，才能配置“健康检查”，否则会导致AI应用创建失败。
- apis定义：选填，用于编辑自定义镜像的apis定义。模型apis定义需要遵循ModelArts的填写规范，参见[模型配置文件说明](#)。

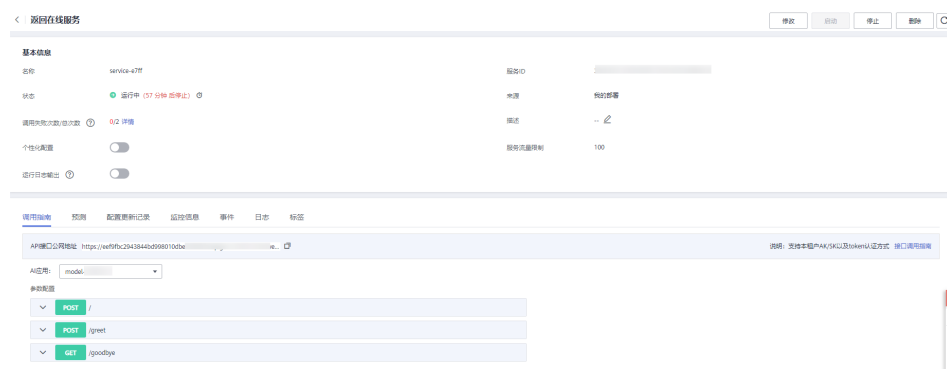
本样例的配置文件如下所示：

```
[{"url": "/", "method": "post", "request": {"Content-type": "application/json"}, "response": {"Content-type": "application/json"}}, {"url": "/greet", "method": "post", "request": {"Content-type": "application/json"}, "response": {"Content-type": "application/json"}}, {"url": "/goodbye", "method": "get", "request": {"Content-type": "application/json"}, "response": {"Content-type": "application/json"}}
```

### 将 AI 应用部署为在线服务

1. 参考[部署为在线服务](#)将AI应用部署为在线服务。
2. 在线服务创建成功后，您可以在服务详情页查看服务详情。

图 11-15 调用指南



3. 您可以通过“预测”页签访问在线服务。

图 11-16 访问在线服务



## 11.3 推理服务访问公网

本章节提供了推理服务访问公网的方法。

### 应用场景

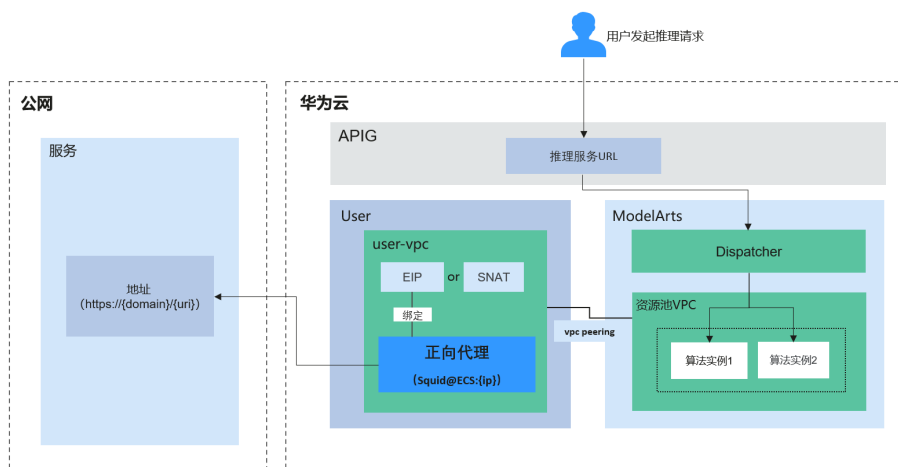
推理服务访问公网地址的场景，如：

- 输入图片，先进行公网OCR服务调用，然后进行NLP处理；
- 进行公网文件下载，然后进行分析；
- 分析结果回调给公网服务终端。

### 方案设计

从推理服务的算法实例内部，访问公网服务地址的方案。如下图所示：

图 11-17 推理服务访问公网



## 操作事项

- **ModelArts：设置资源池的网络**
- **用户VPC：安装和配置正向代理**
- **算法镜像：设置DNS代理和公网地址调用**

### 步骤1 ModelArts：设置资源池的网络

专属资源池的创建作业类型包含推理服务，选择的网络需打通VPC网络，如下图所示：

图 11-18 创建专属资源池

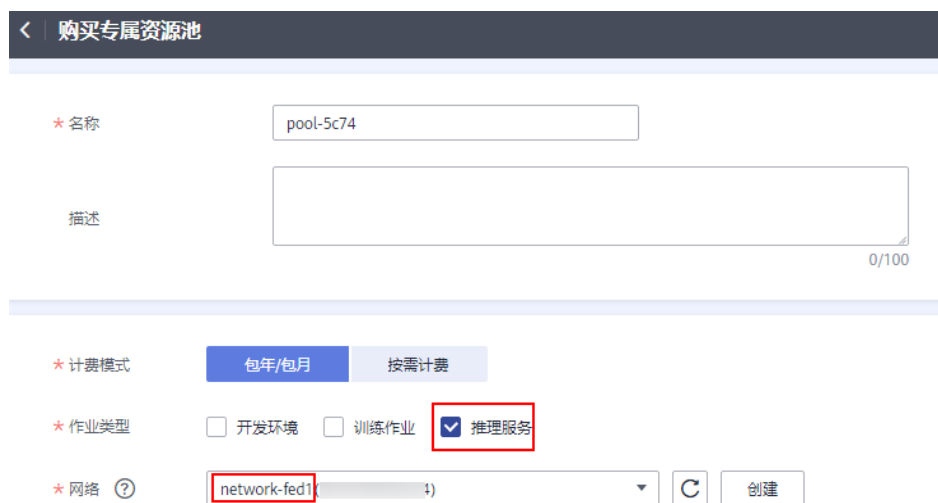


图 11-19 打通 VPC



打通VPC可实现ModelArts资源池和用户VPC的网络打通。打通VPC前需要提前创建好VPC和子网，具体步骤请参考[创建虚拟私有云和子网](#)。

### 步骤2 用户VPC：安装和配置正向代理

在安装正向代理前，需要先购买一台弹性云服务器ECS（镜像可选择Ubuntu最新版本），并配置好弹性EIP，然后登录ECS进行正向代理Squid的安装和配置，步骤如下：

1. 如果没有安装Docker，执行以下命令进行Docker安装  

```
curl -sSL https://get.daocloud.io/docker | sh
```
2. 拉取Squid镜像  

```
docker pull ubuntu/squid
```
3. 创建主机目录，配置whitelist.conf和squid.conf  
 先创建主机目录：  

```
mkdir -p /etc/squid/
```

添加whitelist.conf配置文件，内容为安全控制可访问的地址，如：

```
.apig.cn-east-3.huaweicloudapis.com
```

添加squid.conf配置文件，内容如下：

```
An ACL named 'whitelist'
acl whitelist dstdomain '/etc/squid/whitelist.conf'

Allow whitelisted URLs through
http_access allow whitelist

Block the rest
http_access deny all

Default port
http_port 3128
```

然后设置主机目录和配置文件权限如下：

```
chmod 640 -R /etc/squid
```

#### 4. 启动squid实例

```
docker run -d --name squid -e TZ=UTC -v /etc/squid:/etc/squid -p 3128:3128 ubuntu/squid:latest
```

#### 5. 如果whitelist.conf或squid.conf有更新，则进入容器刷新squid

```
docker exec -it squid bash
root@{container_id}:/# squid -k reconfigure
```

### 步骤3 算法镜像：设置DNS代理和公网地址调用

#### 1. 设置代理

在代码中设置代理指向代理服务器私有IP和端口，如下所示：

```
proxies = {
 "http": "http://{proxy_server_private_ip}:3128",
 "https": "http://{proxy_server_private_ip}:3128"
}
```

服务器私有IP获取如下图所示：

图 11-20 ECS 私有 IP

| 名称ID                                 | 监控 | 可用区  | 状态  | 规格镜像                                                     | IP地址             |
|--------------------------------------|----|------|-----|----------------------------------------------------------|------------------|
| d2199212-15f3-4021-a610-12500d1426fe |    | 可用区2 | 运行中 | 4vCPUs   16GiB   d6.xlrg...<br>Ubuntu 20.04 server 64bit | 92.168.1.12 (私有) |

#### 2. 地址调用

在推理代码中，使用服务URL进行业务请求，如：

```
https://e8a048ce25136adbbac23ce6132a.apig.cn-east-3.huaweicloudapis.com
```

---结束

## 11.4 推理服务端到端运维

ModelArts推理服务的端到端运维覆盖了算法开发、服务运维和业务运行的整个AI流程。

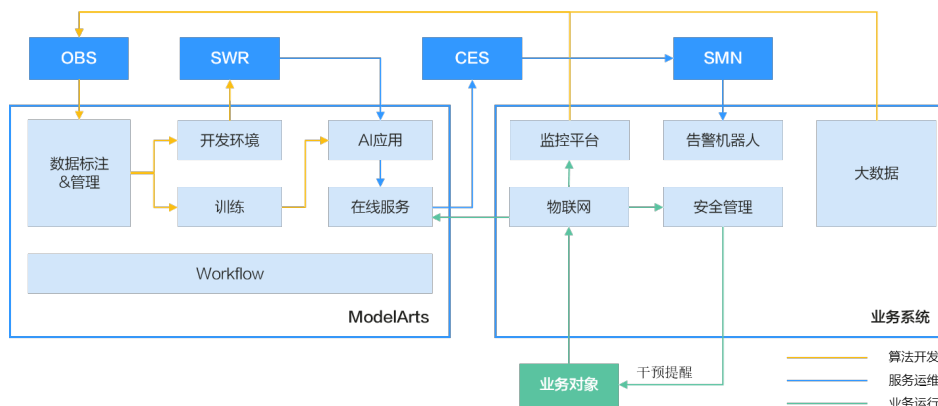
### 方案概述

#### 推理服务的端到端运维流程

- 算法开发阶段，先将业务AI数据存放到对象存储服务（OBS）中，接着通过ModelArts数据管理进行标注和版本管理，然后通过训练获得AI模型结果，最后通过开发环境构建AI应用镜像。

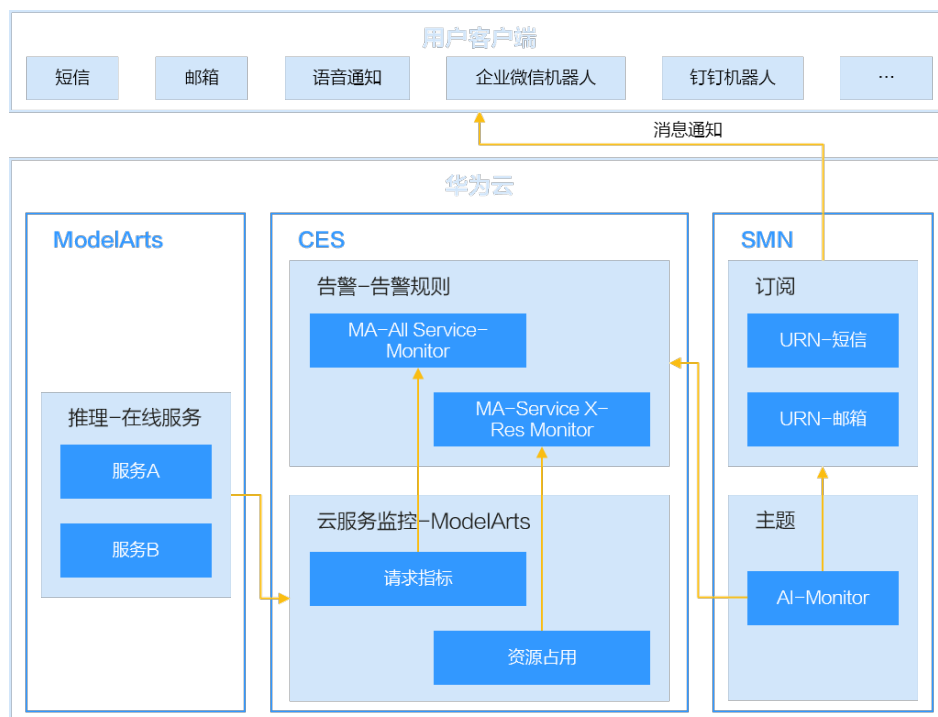
- 服务运维阶段，先利用镜像构建AI应用，接着部署AI应用为在线服务，然后可在云监控服务（CES）中获得ModelArts推理在线服务的监控数据，最后可配置告警规则实现实时告警通知。
- 业务运行阶段，先将业务系统对接在线服务请求，然后进行业务逻辑处理和监控设置。

图 11-21 推理服务的端到端运维流程图



整个运维过程会对服务请求失败和资源占用过高的场景进行监控，当超过阈值时发送告警通知。

图 11-22 监控告警流程图



### 方案优势

通过端到端的服务运维配置，可方便地查看业务运行高低峰情况，并能够实时感知在线服务的健康状态。

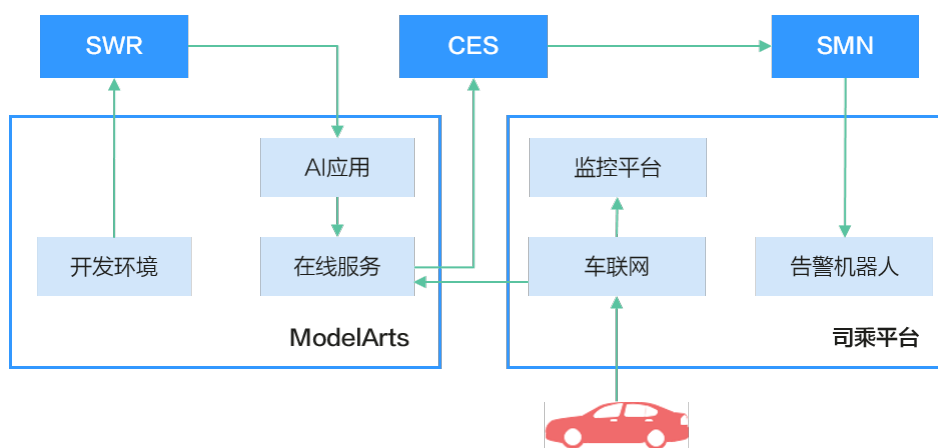
## 约束限制

端到端服务运维只支持在线服务，因为推理的批量服务和边缘服务无CES监控数据，不支持完整的端到端服务运维设置。

## 实施步骤

以出行场景的司乘安全算法为例，介绍使用ModelArts进行流程化服务部署和更新、自动化服务运维和监控的实现步骤。

图 11-23 司乘安全算法



**步骤1** 将用户本地开发完成的模型，使用自定义镜像在ModelArts构建成AI应用。具体操作请参考[从0-1制作自定义镜像并创建AI应用](#)。

**步骤2** 在ModelArts管理控制台，使用创建好的AI应用部署为在线服务。

**步骤3** 登录云监控服务CES管理控制台，设置ModelArts服务的告警规则并配置主题订阅方式发送通知。具体操作请参考[设置告警规则](#)。

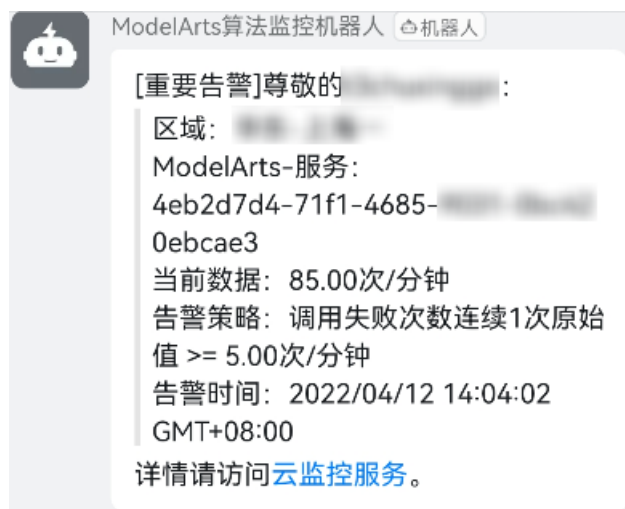
当配置完成后，在左侧导航栏选择“云服务监控 > ModelArts”即可查看在线服务的请求情况和资源占用情况，如下图所示。

图 11-24 查看服务的监控指标



当监控信息触发告警时，主题订阅对象将会收到消息通知。

图 11-25 告警消息通知



----结束

## 11.5 使用自定义引擎创建 AI 应用

使用自定义引擎创建AI应用，用户可以通过选择自己存储在SWR服务中的镜像作为AI应用的引擎，指定预先存储于OBS服务中的文件目录路径作为模型包，来创建AI应用，轻松地应对ModelArts平台预置引擎无法满足个性化诉求的场景。

ModelArts将自定义引擎类型的AI应用部署为服务时，会先将AI应用相关的SWR镜像下载至集群中，用“uid=1000, gid=100”的用户启动SWR镜像为容器，然后将OBS文件下载到容器中的“/home/mind/model”目录下，最后执行SWR镜像中预置的启动命令。ModelArts平台将暴露在容器“8080”端口的服务注册到APIG，用户可以通过提供的APIG（API网关）URL访问到该服务。

### 自定义引擎创建 AI 应用的规范

使用自定义引擎创建AI应用，用户的SWR镜像、OBS模型包和文件大小需要满足以下规范：

- SWR镜像规范：
  - 镜像必须内置一个用户名为“ma-user”，组名为“ma-group”的普通用户，且必须确保该用户的uid=1000、gid=100。内置用户的dockerfile指令如下：
 

```
groupadd -g 100 ma-group && useradd -d /home/ma-user -m -u 1000 -g 100 -s /bin/bash ma-user
```
  - 明确设置镜像的启动命令。在dockerfile文件中指定cmd，dockerfile指令示例如下：
 

```
CMD sh /home/mind/run.sh
```

 启动入口文件run.sh需要自定义。示例如下：
 

```
#!/bin/bash

自定义脚本内容
...

run.sh调用app.py启动服务器，app.py请参考https示例
python app.py
```

- 提供的服务必须使用https协议，且暴露在“8080”端口。请参考[https示例](#)。
- （可选）在“8080”端口，提供URL路径为“/health”的健康检查服务（健康检查的URL路径必须为“/health”）。
- OBS模型包规范  
模型包的名字必须为model。模型包规范请参见[模型包规范介绍](#)。
- 文件大小规范  
当使用公共资源池时，SWR的镜像大小（指下载后的镜像大小，非SWR界面显示的压缩后的镜像大小）和OBS模型包大小总和不大大于30G。

## https 示例

使用Flask启动https，Webserver代码示例如下：

```
from flask import Flask, request
import json

app = Flask(__name__)

@app.route('/greet', methods=['POST'])
def say_hello_func():
 print("----- in hello func -----")
 data = json.loads(request.get_data(as_text=True))
 print(data)
 username = data['name']
 rsp_msg = 'Hello, {}'.format(username)
 return json.dumps({"response":rsp_msg}, indent=4)

@app.route('/goodbye', methods=['GET'])
def say_goodbye_func():
 print("----- in goodbye func -----")
 return '\nGoodbye!\n'

@app.route('/', methods=['POST'])
def default_func():
 print("----- in default func -----")
 data = json.loads(request.get_data(as_text=True))
 return '\n called default func !\n {} \n'.format(str(data))

@app.route('/health', methods=['GET'])
def healthy():
 return "{\"status\": \"OK\"}"

host must be "0.0.0.0", port must be 8080
if __name__ == '__main__':
 app.run(host="0.0.0.0", port=8080, ssl_context='adhoc')
```

## 在本地机器调试

自定义引擎的规范可以在安装有docker的本地机器上通过以下步骤提前验证：

1. 将自定义引擎镜像下载至本地机器，假设镜像名为custom\_engine:v1。
2. 将模型包文件夹复制到本地机器，假设模型包文件夹名字为model。
3. 在模型包文件夹的同级目录下验证如下命令拉起服务：

```
docker run --user 1000:100 -p 8080:8080 -v model:/home/mind/model custom_engine:v1
```

### 📖 说明

该指令无法完全模拟线上，主要是由于-v挂载进去的目录是root权限。在线上，模型文件从OBS下载到/home/mind/model目录之后，文件owner将统一修改为ma-user。



4. 在本地机器上启动另一个终端，执行以下验证指令，得到符合预期的推理结果。  
curl [https://127.0.0.1:8080/\\${推理服务的请求路径}](https://127.0.0.1:8080/${推理服务的请求路径})

## 推理部署示例

本节将详细说明以自定义引擎方式创建AI应用的步骤。

### 1. 创建AI应用并查看AI应用详情

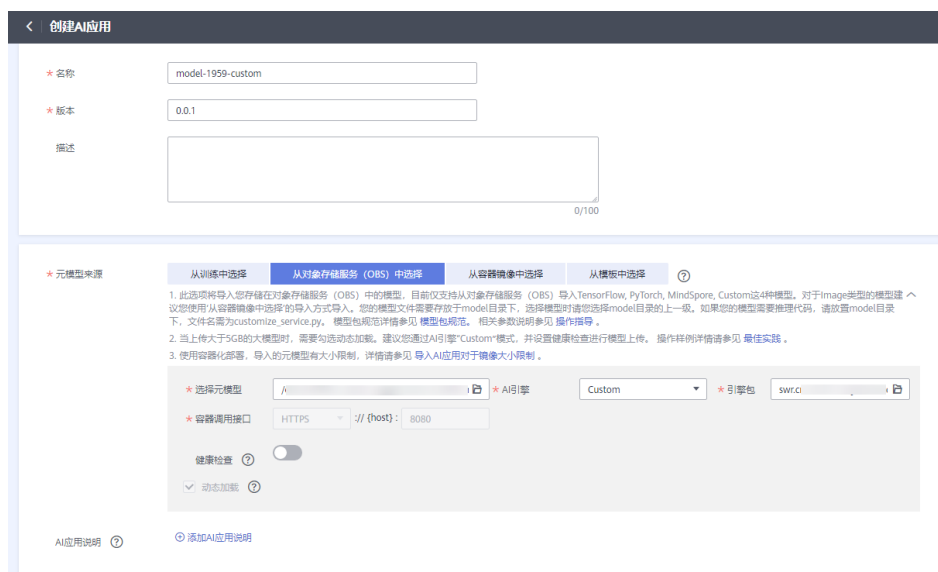
登录ModelArts管理控制台，进入“AI应用管理>AI应用”页面中，单击“创建AI应用”，进入AI应用创建页面，设置相关参数如下：

- 元模型来源：选择“从对象存储服务（OBS）中选择”。
- 选择元模型：从OBS中选择一个模型包。
- AI引擎：选择“Custom”。
- 引擎包：从容器镜像中选择一个镜像。

其他参数保持默认值。

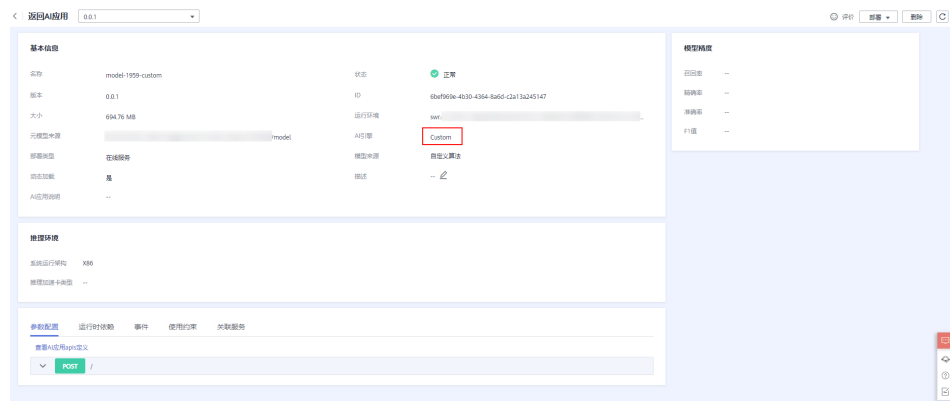
单击“立即创建”，跳转到AI应用列表页，查看AI应用状态，当状态变为“正常”，AI应用创建成功。

图 11-26 创建 AI 应用



单击AI应用名称，进入AI应用详情页面，查看AI应用详情信息。

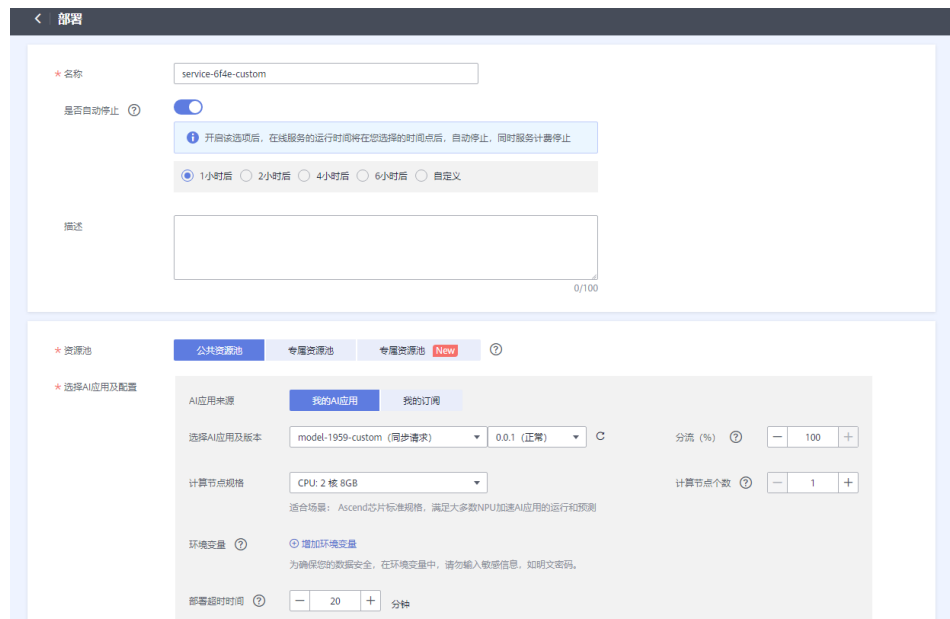
图 11-27 查看 AI 应用详情



2. 部署服务并查看详情

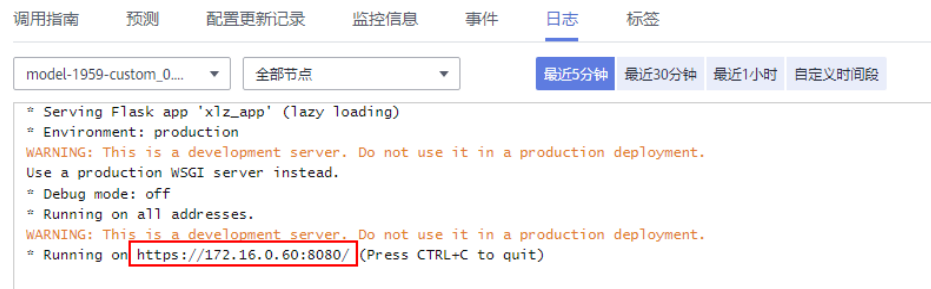
在AI应用详情页面，单击右上角“部署>在线服务”，进入服务部署页面，AI应用和版本默认选中，选择合适的“计算节点规格”，其他参数可保持默认值，单击“下一步”，跳转至服务列表页，当服务状态变为“运行中”，服务部署成功。

图 11-28 部署服务



单击服务名称，进入服务详情页面，查看服务详情信息，单击“日志”页签，查看服务日志信息。

图 11-29 查看服务日志信息



### 3. 服务预测

在服务详情页面，单击“预测”页签，进行服务预测。

图 11-30 服务预测



## 11.6 使用大模型创建 AI 应用部署在线服务

### 背景说明

目前大模型的参数量已经达到千亿甚至万亿，随之大模型的体积也越来越大。千亿参数大模型的体积超过200G，在版本管理、生产部署上对平台系统产生了新的要求。例如：导入AI应用管理时，需要支持动态调整租户存储配额；模型加载、启动慢，部署时需要灵活的超时配置；当负载异常重启，模型需要重新加载，服务恢复时间长的问题亟待解决。

为了应对如上诉求，ModelArts推理平台针对性给出解决方案，用于支持大模型场景下的AI应用管理和部署。

### 约束与限制

- 需要申请单个AI应用大小配额和添加使用节点本地存储缓存的白名单
- 需要使用自定义引擎Custom，配置动态加载
- 需要使用专属资源池部署服务
- 专属资源池磁盘空间需大于1T

## 操作事项

1. [申请扩大AI应用的大小配额和使用节点本地存储缓存白名单](#)
2. [上传模型数据并校验上传对象的一致性](#)
3. [创建专属资源池](#)
4. [创建AI应用](#)
5. [部署在线服务](#)

### 申请扩大 AI 应用的大小配额和使用节点本地存储缓存白名单

服务部署时，默认情况下，动态加载的模型包位于临时磁盘空间，服务停止时已加载的文件会被删除，再次启动时需要重新加载。为了避免反复加载，平台允许使用资源池节点的本地存储空间来加载模型包，并在服务停止和重启时仍有效（通过哈希值保证数据一致性）

使用大模型要求用户采用自定义引擎，并开启动态加载的模式导入模型。基于此，需要执行以下操作：

- 如果模型超过默认配额值，需要提工单申请扩大单个AI应用的大小配额。单个AI应用大小配额默认值为20GB。
- 需要提工单申请添加使用节点本地存储缓存的白名单。

### 上传模型数据并校验上传对象的一致性

为了动态加载时保证数据完整性，需要在上传模型数据至OBS时，进行上传对象的一致性校验。obsutil、OBS Browser+以及OBS SDK都支持在上传对象时进行一致性校验，您可以根据自己的业务选择任意一种方式进行校验。详见[校验上传对象的一致性](#)。

以OBS Browser+为例，如[图11-31](#)。使用OBS Browser+上传数据，开启MD5校验，动态加载并使用节点本地的持久化存储时，检查数据一致性。

图 11-31 OBS Browser+配置 MD5 校验



### 创建专属资源池

使用本地的持久化存储功能，需使用专属资源池，且专属资源池磁盘空间大小必须超过1T。您可以通过专属资源池详情页面，规格页签，查看专属资源池磁盘信息。当服

务部署失败，提示磁盘空间不足时，请参考[服务部署、启动、升级和修改时，资源不足如何处理？](#)

图 11-32 查看专属资源池磁盘信息



## 创建 AI 应用

使用大模型创建AI应用，选择从对象存储服务（OBS）中导入，需满足以下参数配置：

### 1. 采用自定义引擎，开启动态加载

使用大模型要求用户使用自定义引擎，并开启动态加载的模式导入模型。用户可以制作自定义引擎，满足大模型场景下对镜像依赖包、推理框架等的特殊需求。自定义引擎的制作请参考[使用自定义引擎创建AI应用](#)。

当用户使用自定义引擎时，默认开启动态加载，模型包与镜像分离，在服务部署时动态将模型加载到服务负载。

### 2. 配置健康检查

大模型场景下导入的AI应用，要求配置健康检查，避免在部署时服务显示已启动但实际不可用。

图 11-33 采用自定义引擎，开启动态加载并配置健康检查示例图



## 部署在线服务

部署服务时，需满足以下参数配置：

1. 自定义部署超时时间  
大模型加载启动的时间一般大于普通的模型创建的服务，请配置合理的“部署超时时间”，避免尚未启动完成被认为超时而导致部署失败。
2. 添加环境变量  
部署服务时，增加如下环境变量，会将负载均衡的请求亲和策略配置为集群亲和，避免未就绪的服务实例影响预测成功率。  
MODELARTS\_SERVICE\_TRAFFIC\_POLICY: cluster

图 11-34 自定义部署超时时间和添加环境变量示例图



建议部署多实例，增加服务可靠性。

## 11.7 第三方推理框架迁移到推理自定义引擎

### 背景说明

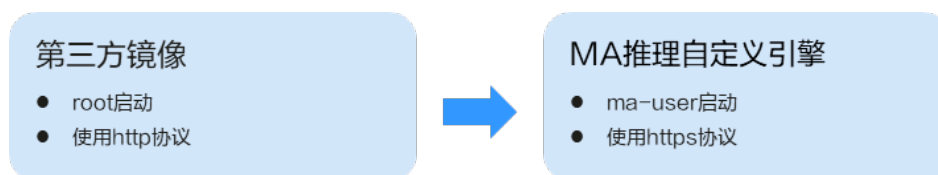
ModelArts支持第三方的推理框架在ModelArts上部署，本文以TF Serving框架、Triton框架为例，介绍如何迁移到推理自定义引擎。

- TensorFlow Serving是一个灵活、高性能的机器学习模型部署系统，提供模型版本管理、服务回滚等能力。通过配置模型路径、模型端口、模型名称等参数，原生TF Serving镜像可以快速启动提供服务，并支持gRPC和HTTP Restful API的访问方式。
- Triton是一个高性能推理服务框架，提供HTTP/gRPC等多种服务协议，支持TensorFlow、TensorRT、PyTorch、ONNXRuntime等多种推理引擎后端，并且支持多模型并发、动态batch等功能，能够提高GPU的使用率，改善推理服务的性能。

当从第三方推理框架迁移到使用ModelArts推理的AI应用管理和服务管理时，需要对原生第三方推理框架镜像的构建方式做一定的改造，以使用ModelArts推理平台的模型版本管理能力和动态加载模型的部署能力。本案例将指导用户完成原生第三方推理框架镜像到ModelArts推理自定义引擎的改造。自定义引擎的镜像制作完成后，即可以通过AI应用导入对模型版本进行管理，并基于AI应用进行部署和管理服务。

适配和改造的主要工作项如下：

图 11-35 改造工作项



针对不同框架的镜像，可能还需要做额外的适配工作，具体差异请见对应框架的操作步骤。

- [TF Serving 框架迁移操作步骤](#)
- [Triton 框架迁移操作步骤](#)

## TF Serving 框架迁移操作步骤

**步骤1** 增加用户ma-user。

基于原生"tensorflow/serving:2.8.0"镜像构建，镜像中100的用户组默认已存在，Dockerfile中执行如下命令增加用户ma-user。

```
RUN useradd -d /home/ma-user -m -u 1000 -g 100 -s /bin/bash ma-user
```

**步骤2** 通过增加nginx代理，支持https协议。

协议转换为https之后，对外暴露的端口从tfserving的8501变为8080。

1. Dockerfile中执行如下命令完成nginx的安装和配置。

```
RUN apt-get update && apt-get -y --no-install-recommends install nginx && apt-get clean
RUN mkdir /home/mind && \
 mkdir -p /etc/nginx/keys && \
 mkfifo /etc/nginx/keys/fifo && \
 chown -R ma-user:100 /home/mind && \
 rm -rf /etc/nginx/conf.d/default.conf && \
 chown -R ma-user:100 /etc/nginx/ && \
 chown -R ma-user:100 /var/log/nginx && \
 chown -R ma-user:100 /var/lib/nginx && \
 sed -i "s#/var/run/nginx.pid#/home/ma-user/nginx.pid#g" /etc/init.d/nginx
ADD nginx /etc/nginx
ADD run.sh /home/mind/
ENTRYPOINT []
CMD /bin/bash /home/mind/run.sh
```

2. 准备nginx目录如下：

```
nginx
├── nginx.conf
├── conf.d
│ └── modelarts-model-server.conf
```

3. 准备nginx.conf文件内容如下：

```
user ma-user 100;
worker_processes 2;
pid /home/ma-user/nginx.pid;
include /etc/nginx/modules-enabled/*.conf;
events {
 worker_connections 768;
}
http {
 ##
 # Basic Settings
 ##
 sendfile on;
 tcp_nopush on;
 tcp_nodelay on;
 types_hash_max_size 2048;
 fastcgi_hide_header X-Powered-By;
 port_in_redirect off;
 server_tokens off;
 client_body_timeout 65s;
 client_header_timeout 65s;
 keepalive_timeout 65s;
 send_timeout 65s;
 # server_names_hash_bucket_size 64;
 # server_name_in_redirect off;
 include /etc/nginx/mime.types;
```

```
default_type application/octet-stream;
##
SSL Settings
##
ssl_protocols TLSv1.2;
ssl_prefer_server_ciphers on;
ssl_ciphers ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES128-GCM-SHA256;
##
Logging Settings
##
access_log /var/log/nginx/access.log;
error_log /var/log/nginx/error.log;
##
Gzip Settings
##
gzip on;
##
Virtual Host Configs
##
include /etc/nginx/conf.d/modelarts-model-server.conf;
}
```

#### 4. 准备modelarts-model-server.conf配置文件内容如下:

```
server {
 client_max_body_size 15M;
 large_client_header_buffers 4 64k;
 client_header_buffer_size 1k;
 client_body_buffer_size 16k;
 ssl_certificate /etc/nginx/ssl/server/server.crt;
 ssl_password_file /etc/nginx/keys/fifo;
 ssl_certificate_key /etc/nginx/ssl/server/server.key;
 # setting for mutual ssl with client
 ##
 # header Settings
 ##
 add_header X-XSS-Protection "1; mode=block";
 add_header X-Frame-Options SAMEORIGIN;
 add_header X-Content-Type-Options nosniff;
 add_header Strict-Transport-Security "max-age=31536000; includeSubdomains;";
 add_header Content-Security-Policy "default-src 'self'";
 add_header Cache-Control "max-age=0, no-cache, no-store, must-revalidate";
 add_header Pragma "no-cache";
 add_header Expires "-1";
 server_tokens off;
 port_in_redirect off;
 fastcgi_hide_header X-Powered-By;
 ssl_session_timeout 2m;
 ##
 # SSL Settings
 ##
 ssl_protocols TLSv1.2;
 ssl_prefer_server_ciphers on;
 ssl_ciphers ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES128-GCM-SHA256;
 listen 0.0.0.0:8080 ssl;
 error_page 502 503 /503.html;
 location /503.html {
 return 503 '{"error_code": "ModelArts.4503","error_msg": "Failed to connect to backend service, please confirm your service is connectable. "}';
 }
 location / {
 # limit_req zone=mylimit;
 # limit_req_status 429;
 proxy_pass http://127.0.0.1:8501;
 }
}
```

#### 5. 准备启动脚本。



## 📖 说明

启动前先创建ssl证书，然后启动TF Serving的启动脚本。

启动脚本run.sh示例代码如下：

```
#!/bin/bash
mkdir -p /etc/nginx/ssl/server && cd /etc/nginx/ssl/server
cipherText=$(openssl rand -base64 32)
openssl genrsa -aes256 -passout pass:"${cipherText}" -out server.key 2048
openssl rsa -in server.key -passin pass:"${cipherText}" -pubout -out rsa_public.key
openssl req -new -key server.key -passin pass:"${cipherText}" -out server.csr -subj "/C=CN/ST=GD/L=SZ/O=Huawei/OU=ops/CN=*.huawei.com"
openssl genrsa -out ca.key 2048
openssl req -new -x509 -days 3650 -key ca.key -out ca.crt.pem -subj "/C=CN/ST=GD/L=SZ/O=Huawei/OU=dev/CN=ca"
openssl x509 -req -days 3650 -in server.csr -CA ca.crt.pem -CAkey ca.key -CAcreateserial -out server.crt
service nginx start &
echo "${cipherText}" > /etc/nginx/keys/fifo
unset cipherText
sh /usr/bin/tf_serving_entrypoint.sh
```

**步骤3** 修改模型默认路径，支持ModelArts推理模型动态加载。

Dockerfile中执行如下命令修改默认的模型路径。

```
ENV MODEL_BASE_PATH /home/mind
ENV MODEL_NAME model
```

----结束

完整的Dockerfile参考：

```
FROM tensorflow/serving:2.8.0
RUN useradd -d /home/ma-user -m -u 1000 -g 100 -s /bin/bash ma-user
RUN apt-get update && apt-get -y --no-install-recommends install nginx && apt-get clean
RUN mkdir /home/mind && \
 mkdir -p /etc/nginx/keys && \
 mkfifo /etc/nginx/keys/fifo && \
 chown -R ma-user:100 /home/mind && \
 rm -rf /etc/nginx/conf.d/default.conf && \
 chown -R ma-user:100 /etc/nginx/ && \
 chown -R ma-user:100 /var/log/nginx && \
 chown -R ma-user:100 /var/lib/nginx && \
 sed -i "s#/var/run/nginx.pid#/home/ma-user/nginx.pid#g" /etc/init.d/nginx
ADD nginx /etc/nginx
ADD run.sh /home/mind/
ENV MODEL_BASE_PATH /home/mind
ENV MODEL_NAME model
ENTRYPOINT []
CMD /bin/bash /home/mind/run.sh
```

## Triton 框架迁移操作步骤

本教程基于nvidia官方提供的nvcr.io/nvidia/tritonserver:23.03-py3镜像进行适配，使用开源大模型llama7b进行推理任务。

**步骤1** 增加用户ma-user。

Triton镜像中默认已存在id为1000的triton-server用户，需先修改triton-server用户名id后再增加用户ma-user，Dockerfile中执行如下命令。

```
RUN usermod -u 1001 triton-server && useradd -d /home/ma-user -m -u 1000 -g 100 -s /bin/bash ma-user
```

**步骤2** 通过增加nginx代理，支持https协议。

1. Dockerfile中执行如下命令完成nginx的安装和配置。

```
RUN apt-get update && apt-get -y --no-install-recommends install nginx && apt-get clean && \
mkdir /home/mind && \
mkdir -p /etc/nginx/keys && \
mkfifo /etc/nginx/keys/fifo && \
chown -R ma-user:100 /home/mind && \
rm -rf /etc/nginx/conf.d/default.conf && \
chown -R ma-user:100 /etc/nginx/ && \
chown -R ma-user:100 /var/log/nginx && \
chown -R ma-user:100 /var/lib/nginx && \
sed -i "s#/var/run/nginx.pid#/home/ma-user/nginx.pid#g" /etc/init.d/nginx
```

2. 准备nginx目录如下:

```
nginx
├── nginx.conf
├── conf.d
│ └── modelarts-model-server.conf
```

3. 准备nginx.conf文件内容如下:

```
user ma-user 100;
worker_processes 2;
pid /home/ma-user/nginx.pid;
include /etc/nginx/modules-enabled/*.conf;
events {
 worker_connections 768;
}
http {
 ##
 # Basic Settings
 ##
 sendfile on;
 tcp_nopush on;
 tcp_nodelay on;
 types_hash_max_size 2048;
 fastcgi_hide_header X-Powered-By;
 port_in_redirect off;
 server_tokens off;
 client_body_timeout 65s;
 client_header_timeout 65s;
 keepalive_timeout 65s;
 send_timeout 65s;
 # server_names_hash_bucket_size 64;
 # server_name_in_redirect off;
 include /etc/nginx/mime.types;
 default_type application/octet-stream;
 ##
 # SSL Settings
 ##
 ssl_protocols TLSv1.2;
 ssl_prefer_server_ciphers on;
 ssl_ciphers ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES128-GCM-SHA256;
 ##
 # Logging Settings
 ##
 access_log /var/log/nginx/access.log;
 error_log /var/log/nginx/error.log;
 ##
 # Gzip Settings
 ##
 gzip on;
 ##
 # Virtual Host Configs
 ##
 include /etc/nginx/conf.d/modelarts-model-server.conf;
}
```

4. 准备modelarts-model-server.conf配置文件内容如下:

```
server {
 client_max_body_size 15M;
 large_client_header_buffers 4 64k;
 client_header_buffer_size 1k;
 client_body_buffer_size 16k;
```

```
ssl_certificate /etc/nginx/ssl/server/server.crt;
ssl_password_file /etc/nginx/keys/fifo;
ssl_certificate_key /etc/nginx/ssl/server/server.key;
setting for mutual ssl with client
##
header Settings
##
add_header X-XSS-Protection "1; mode=block";
add_header X-Frame-Options SAMEORIGIN;
add_header X-Content-Type-Options nosniff;
add_header Strict-Transport-Security "max-age=31536000; includeSubdomains;";
add_header Content-Security-Policy "default-src 'self'";
add_header Cache-Control "max-age=0, no-cache, no-store, must-revalidate";
add_header Pragma "no-cache";
add_header Expires "-1";
server_tokens off;
port_in_redirect off;
fastcgi_hide_header X-Powered-By;
ssl_session_timeout 2m;
##
SSL Settings
##
ssl_protocols TLSv1.2;
ssl_prefer_server_ciphers on;
ssl_ciphers ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES128-GCM-SHA256;
listen 0.0.0.0:8080 ssl;
error_page 502 503 /503.html;
location /503.html {
 return 503 '{"error_code": "ModelArts.4503","error_msg": "Failed to connect to backend service,
please confirm your service is connectable. "};
}
location / {
limit_req zone=mylimit;
limit_req_status 429;
 proxy_pass http://127.0.0.1:8000;
}
}
```

## 5. 准备启动脚本run.sh。

### 说明

启动前先创建ssl证书，然后启动Triton的启动脚本。

```
#!/bin/bash
mkdir -p /etc/nginx/ssl/server && cd /etc/nginx/ssl/server
cipherText=$(openssl rand -base64 32)
openssl genrsa -aes256 -passout pass:"${cipherText}" -out server.key 2048
openssl rsa -in server.key -passin pass:"${cipherText}" -pubout -out rsa_public.key
openssl req -new -key server.key -passin pass:"${cipherText}" -out server.csr -subj "/C=CN/ST=GD/L=SZ/O=Huawei/OU=ops/CN=*.huawei.com"
openssl genrsa -out ca.key 2048
openssl req -new -x509 -days 3650 -key ca.key -out ca-crt.pem -subj "/C=CN/ST=GD/L=SZ/O=Huawei/OU=dev/CN=ca"
openssl x509 -req -days 3650 -in server.csr -CA ca-crt.pem -CAkey ca.key -CAcreateserial -out server.crt
service nginx start &
echo ${cipherText} > /etc/nginx/keys/fifo
unset cipherText

bash /home/mind/model/triton_serving.sh
```

## 步骤3 编译安装tensorrtllm\_backend。

1. Dockerfile中执行如下命令获取tensorrtllm\_backend源码，安装tensorrt、cmake和pytorch等相关依赖，并进行编译安装。

```
get tensorrtllm_backend source code
WORKDIR /opt/tritonserver
RUN apt-get install -y --no-install-recommends rapidjson-dev python-is-python3 git-lfs && \
 git config --global http.sslVerify false && \
 git config --global http.postBuffer 1048576000 && \
```

```
git clone -b v0.5.0 https://github.com/triton-inference-server/tensorrtllm_backend.git --depth 1 && \
cd tensorrtllm_backend && git lfs install && \
git config submodule.tensorrt_llm.url https://github.com/NVIDIA/TensorRT-LLM.git && \
git submodule update --init --recursive --depth 1 && \
pip3 install -r requirements.txt

build tensorrtllm_backend
WORKDIR /opt/tritonserver/tensorrtllm_backend/tensorrt_llm
RUN sed -i "s/wget/wget --no-check-certificate/g" docker/common/install_tensorrt.sh && \
bash docker/common/install_tensorrt.sh && \
export LD_LIBRARY_PATH=/usr/local/tensorrt/lib:${LD_LIBRARY_PATH} && \
sed -i "s/wget/wget --no-check-certificate/g" docker/common/install_cmake.sh && \
bash docker/common/install_cmake.sh && \
export PATH=/usr/local/cmake/bin:$PATH && \
bash docker/common/install_pytorch.sh pypi && \
python3 ./scripts/build_wheel.py --trt_root /usr/local/tensorrt && \
pip install ./build/tensorrt_llm-0.5.0-py3-none-any.whl && \
rm -f ./build/tensorrt_llm-0.5.0-py3-none-any.whl && \
cd ../inflight_batcher_llm && bash scripts/build.sh && \
mkdir /opt/tritonserver/backends/tensorrtllm && \
cp ./build/libtriton_tensorrtllm.so /opt/tritonserver/backends/tensorrtllm/ && \
chown -R ma-user:100 /opt/tritonserver
```

## 2. 准备triton serving的启动脚triton\_serving.sh， llama模型的参考样例如下：

```
MODEL_NAME=llama_7b
MODEL_DIR=/home/mind/model/${MODEL_NAME}
OUTPUT_DIR=/tmp/llama/7B/trt_engines/fp16/1-gpu/
MAX_BATCH_SIZE=1
export LD_LIBRARY_PATH=/usr/local/tensorrt/lib:${LD_LIBRARY_PATH}

build tensorrt_llm engine
cd /opt/tritonserver/tensorrtllm_backend/tensorrt_llm/examples/llama
python build.py --model_dir ${MODEL_DIR} \
 --dtype float16 \
 --remove_input_padding \
 --use_gpt_attention_plugin float16 \
 --enable_context_fmha \
 --use_weight_only \
 --use_gemm_plugin float16 \
 --output_dir ${OUTPUT_DIR} \
 --paged_kv_cache \
 --max_batch_size ${MAX_BATCH_SIZE}

set config parameters
cd /opt/tritonserver/tensorrtllm_backend
mkdir triton_model_repo
cp all_models/inflight_batcher_llm/* triton_model_repo/ -r

python3 tools/fill_template.py -i triton_model_repo/preprocessing/config.pbtxt tokenizer_dir:$
{MODEL_DIR},tokenizer_type:llama,triton_max_batch_size:$
{MAX_BATCH_SIZE},preprocessing_instance_count:1
python3 tools/fill_template.py -i triton_model_repo/postprocessing/config.pbtxt tokenizer_dir:$
{MODEL_DIR},tokenizer_type:llama,triton_max_batch_size:$
{MAX_BATCH_SIZE},postprocessing_instance_count:1
python3 tools/fill_template.py -i triton_model_repo/ensemble/config.pbtxt triton_max_batch_size:$
{MAX_BATCH_SIZE}
python3 tools/fill_template.py -i triton_model_repo/tensorrt_llm/config.pbtxt triton_max_batch_size:$
{MAX_BATCH_SIZE},decoupled_mode:False,max_beam_width:1,engine_dir:$
{OUTPUT_DIR},max_tokens_in_paged_kv_cache:2560,max_attention_window_size:2560,kv_cache_free_
gpu_mem_fraction:0.5,exclude_input_in_output:True,enable_kv_cache_reuse:False,batching_strategy:V1,
max_queue_delay_microseconds:600

launch tritonserver
python3 scripts/launch_triton_server.py --world_size 1 --model_repo=triton_model_repo/
while true; do sleep 10000; done
```

### 部分参数说明：

- MODEL\_NAME: HuggingFace格式模型权重文件所在OBS文件夹名称。
- OUTPUT\_DIR: 通过TensorRT-LLM转换后的模型文件在容器中的路径。

完整的Dockerfile如下:

```
FROM nvcr.io/nvidia/tritonserver:23.03-py3

add ma-user and install nginx
RUN usermod -u 1001 triton-server && useradd -d /home/ma-user -m -u 1000 -g 100 -s /bin/bash ma-user && \
 apt-get update && apt-get -y --no-install-recommends install nginx && apt-get clean && \
 mkdir /home/mind && \
 mkdir -p /etc/nginx/keys && \
 mkfifo /etc/nginx/keys/fifo && \
 chown -R ma-user:100 /home/mind && \
 rm -rf /etc/nginx/conf.d/default.conf && \
 chown -R ma-user:100 /etc/nginx/ && \
 chown -R ma-user:100 /var/log/nginx && \
 chown -R ma-user:100 /var/lib/nginx && \
 sed -i "s#/var/run/nginx.pid#/home/ma-user/nginx.pid#g" /etc/init.d/nginx

get tensorrtllm_backend source code
WORKDIR /opt/tritonserver
RUN apt-get install -y --no-install-recommends rapidjson-dev python-is-python3 git-lfs && \
 git config --global http.sslVerify false && \
 git config --global http.postBuffer 1048576000 && \
 git clone -b v0.5.0 https://github.com/triton-inference-server/tensorrtllm_backend.git --depth 1 && \
 cd tensorrtllm_backend && git lfs install && \
 git config submodule.tensorrt_llm.url https://github.com/NVIDIA/TensorRT-LLM.git && \
 git submodule update --init --recursive --depth 1 && \
 pip3 install -r requirements.txt

build tensorrtllm_backend
WORKDIR /opt/tritonserver/tensorrtllm_backend/tensorrt_llm
RUN sed -i "s/wget/wget --no-check-certificate/g" docker/common/install_tensorrt.sh && \
 bash docker/common/install_tensorrt.sh && \
 export LD_LIBRARY_PATH=/usr/local/tensorrt/lib:${LD_LIBRARY_PATH} && \
 sed -i "s/wget/wget --no-check-certificate/g" docker/common/install_cmake.sh && \
 bash docker/common/install_cmake.sh && \
 export PATH=/usr/local/cmake/bin:$PATH && \
 bash docker/common/install_pytorch.sh pypi && \
 python3 ./scripts/build_wheel.py --trt_root /usr/local/tensorrt && \
 pip install ./build/tensorrt_llm-0.5.0-py3-none-any.whl && \
 rm -f ./build/tensorrt_llm-0.5.0-py3-none-any.whl && \
 cd ../inflight_batcher_llm && bash scripts/build.sh && \
 mkdir /opt/tritonserver/backends/tensorrtllm && \
 cp ./build/libtriton_tensorrtllm.so /opt/tritonserver/backends/tensorrtllm/ && \
 chown -R ma-user:100 /opt/tritonserver

ADD nginx /etc/nginx
ADD run.sh /home/mind/
CMD /bin/bash /home/mind/run.sh
```

完成镜像构建后，将镜像注册至华为云容器镜像服务SWR中，用于后续在ModelArts上部署推理服务。

**步骤4** 使用适配后的镜像在ModelArts部署在线推理服务。

1. 在obs中创建model目录，并将triton\_serving.sh文件和llama\_7b文件夹上传至model目录下，如下图所示。

图 11-36 上传至 model 目录



2. 创建AI应用，源模型来源选择“从对象存储服务（OBS）中选择”，元模型选择至model目录，AI引擎选择Custom，引擎包选择步骤3构建的镜像。

图 11-37 创建 AI 应用



3. 将创建的AI应用部署为在线服务，大模型加载启动的时间一般大于普通的模型创建的服务，请配置合理的“部署超时时间”，避免尚未启动完成被认为超时而导致部署失败。

图 11-38 部署为在线服务



4. 调用在线服务进行大模型推理，请求路径填写/v2/models/ensemble/infer，调用样例如下：

```

{
 "inputs": [
 {
 "name": "text_input",
 "shape": [1, 1],
 "datatype": "BYTES",
 "data": ["what is machine learning"]
 },
 {
 "name": "max_tokens",
 "shape": [1, 1],
 "datatype": "UINT32",
 "data": [64]
 },
 {
 "name": "bad_words",
 "shape": [1, 1],
 "datatype": "BYTES",
 "data": [""]
 },
 {
 "name": "stop_words",
 "shape": [1, 1],
 "datatype": "BYTES",
 "data": [""]
 },
 {
 "name": "pad_id",
 "shape": [1, 1],
 "datatype": "UINT32",
 "data": [2]
 },
 {
 "name": "end_id",
 "shape": [1, 1],
 "datatype": "UINT32",
 "data": [2]
 }
],
 "outputs": [
 {
 "name": "text_output"
 }
]
}

```

**说明**

- "inputs"中"name"为"text\_input"的元素代表输入，"data"为具体输入语句，本示例中为"what is machine learning"。
- "inputs"中"name"为"max\_tokens"的元素代表输出最大tokens数，"data"为具体数值，本示例中为64。

图 11-39 调用在线服务



----结束

## 11.8 推理服务支持虚拟私有云（VPC）直连的高速访问通道

### 背景说明

访问在线服务的实际业务中，用户可能会存在如下需求：

- 高吞吐量、低时延
- TCP或者RPC请求

因此，ModelArts提供了VPC直连的高速访问通道功能以满足用户的需求。

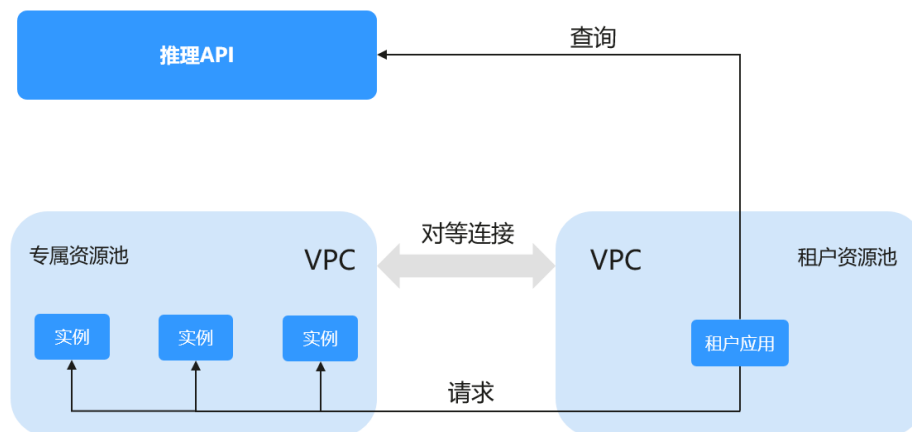
使用VPC直连的高速访问通道，用户的业务请求不需要经过推理平台，而是直接经VPC对等连接发送到实例处理，访问速度更快。

#### 说明

由于请求不经过推理平台，所以会丢失以下功能：

- 认证鉴权
- 流量按配置分发
- 负载均衡
- 告警、监控和统计

图 11-40 VPC 直连的高速访问通道示意图





## 准备工作

使用专属资源池部署在线服务，服务状态为“运行中”。

### 须知

- 需使用新版专属资源池部署服务，详情请参见[ModelArts资源池管理功能全面升级](#)。
- 只有专属资源池部署的服务才支持VPC直连的高速访问通道。
- VPC直连的高速访问通道，目前只支持访问在线服务。
- 因流量限控，获取在线服务的IP和端口号次数有限制，每个主账号租户调用次数不超过2000次/分钟，每个子账号租户不超过20次/分钟。
- 目前仅支持自定义镜像导入模型，部署的服务支持高速访问通道。

## 操作步骤

使用VPC直连的高速访问通道访问在线服务，基本操作步骤如下：

1. [将专属资源池的网络打通VPC](#)
2. [VPC下创建弹性云服务器](#)
3. [获取在线服务的IP和端口号](#)
4. [通过IP和端口号直连应用](#)

### 步骤1 将专属资源池的网络打通VPC

登录ModelArts控制台，进入“专属资源池 > 弹性集群”找到服务部署使用的专属资源池，单击“名称/ID”，进入资源池详情页面，查看网络配置信息。返回专属资源池列表，选择“网络”页签，找到专属资源池关联的网络，打通VPC。打通VPC网络后，网络列表和资源池详情页面将显示VPC名称，单击后可以跳转至VPC详情页面。

图 11-41 查找专属资源池



图 11-42 查看网络配置

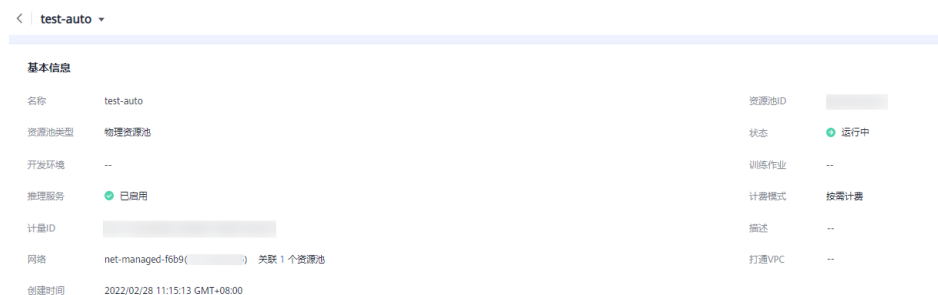
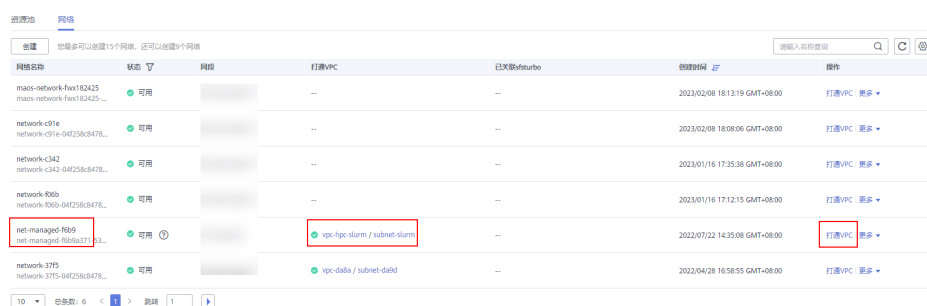


图 11-43 打通 VPC



## 步骤2 VPC下创建弹性云服务器

登录弹性云服务器ECS控制台，单击右上角“购买弹性云服务器”，进入购买弹性云服务器页面，完成基本配置后单击“下一步：网络配置”，进入网络配置页面，选择步骤1中打通的VPC，完成其他参数配置，完成高级配置并确认配置，下发购买弹性云服务器的任务。等待服务器的状态变为“运行中”时，弹性云服务器创建成功。单击“名称/ID”，进入服务器详情页面，查看虚拟私有云配置信息。

图 11-44 购买弹性云服务器时选择 VPC

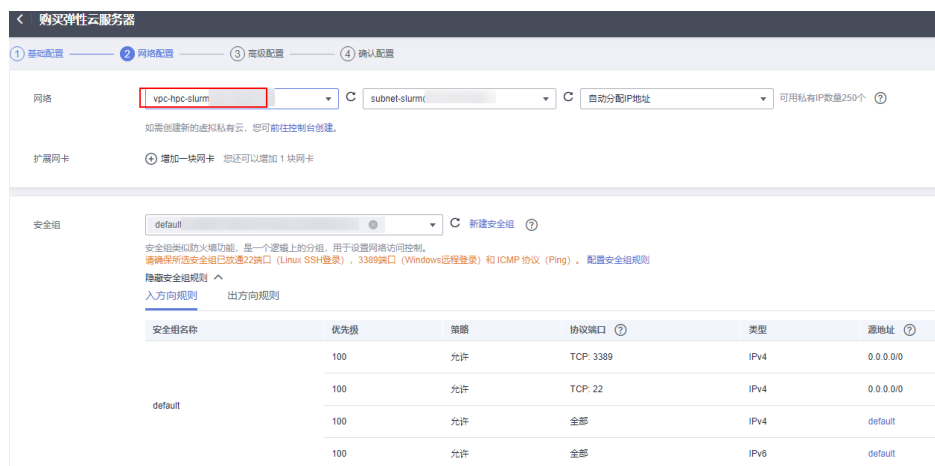


图 11-45 虚拟私有云



**步骤3 获取在线服务的IP和端口号**

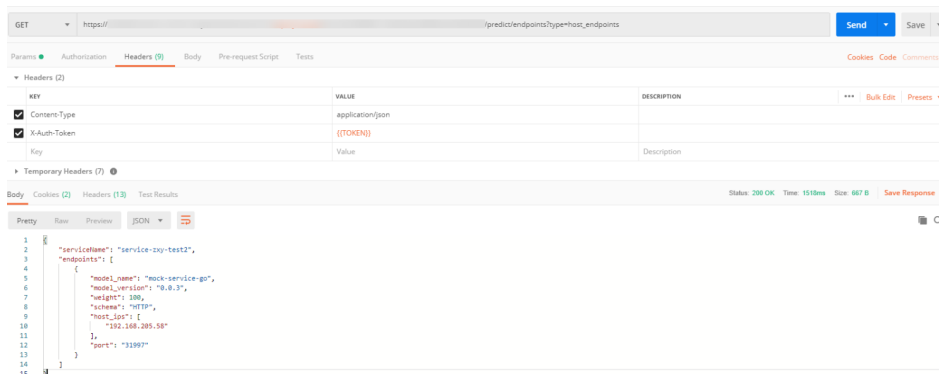
可以通过使用图形界面的软件（以Postman为例）获取服务的IP和端口号，也可以登录弹性云服务器（ECS），创建Python环境运行代码，获取服务IP和端口号。

**API接口：**

GET /v1/{project\_id}/services/{service\_id}/predict/endpoints?type=host\_endpoints

- 方式一：图形界面的软件获取服务的IP和端口号

图 11-46 接口返回示例



- 方式二：Python语言获取IP和端口号

Python代码如下，下述代码中以下参数需要手动修改：

- project\_id: 用户项目ID，获取方法请参见[获取项目ID和名称](#)。
- service\_id: 服务ID，在服务详情页可查看。

- REGION\_ENDPOINT: 服务的终端节点, 查询请参见[终端节点](#)。

```
def get_app_info(project_id, service_id):
 list_host_endpoints_url = "{}v1/{}/services/{}/predict/endpoints?type=host_endpoints"
 url = list_host_endpoints_url.format(REGION_ENDPOINT, project_id, service_id)
 headers = {'X-Auth-Token': X_Auth-Token}
 response = requests.get(url, headers=headers)
 print(response.content)
```

#### 步骤4 通过IP和端口号直连应用

登录弹性云服务器 (ECS), 可以通过Linux命令行访问在线服务, 也可以创建Python环境运行Python代码访问在线服务。schema、ip、port参数值从[步骤3](#)获取。

- 执行命令示例如下, 直接访问在线服务。

```
curl --location --request POST 'http://192.168.205.58:31997' \
--header 'Content-Type: application/json' \
--data-raw '{"a":"a"}
```

图 11-47 访问在线服务

```
[root@ecs-zxy ~]# curl --location --request POST 'http://192.168.205.58:31997' \
> --header 'Content-Type: application/json' \
> --data-raw '{"a":"a"}'
call Post()[root@ecs-zxy ~]# _
```

- 创建Python环境, 运行Python代码访问在线服务。

```
def vpc_infer(schema, ip, port, body):
 infer_url = "{}://{}:{}".format(schema, ip, port)
 url = infer_url.format(schema, ip, port)
 response = requests.post(url, data=body)
 print(response.content)
```

#### 📖 说明

由于高速通道特性会缺失负载均衡的能力, 因此在多实例时需要自主制定负载均衡策略。

----结束

## 11.9 WebSocket 在线服务全流程开发

### 背景说明

WebSocket是一种网络传输协议, 可在单个TCP连接上进行全双工通信, 位于OSI模型的应用层。WebSocket协议在2011年由IETF标准化为RFC 6455, 后由RFC 7936补充规范。Web IDL中的WebSocket API由W3C标准化。

WebSocket使得客户端和服务端之间的数据交换变得更加简单, 允许服务端主动向客户端推送数据。在WebSocket API中, 浏览器和服务端只需要完成一次握手, 两者之间就可以建立持久性的连接, 并进行双向数据传输。

### 前提条件

- 用户需有一定的Java开发经验, 熟悉jar打包流程。
- 用户需了解WebSocket协议的基本概念及调用方法。
- 用户需熟悉Docker制作镜像的方法。

## 约束与限制

- WebSocket协议只支持部署在线服务。
- 只支持自定义镜像导入AI应用部署的在线服务。

## 准备工作

ModelArts使用WebSocket完成推理需要用户自己准备自定义镜像，该自定义镜像需要在单机环境下能够提供完整的WebSocket服务，如完成WebSocket的握手，client向server发送数据，server向client发送数据等。模型的推理过程在自定义镜像中完成，如下载模型，加载模型，执行预处理，完成推理，拼装响应体等。

## 操作步骤

WebSocket在线服务开发操作步骤如下：

- [上传镜像至容器镜像服务](#)
- [使用镜像创建AI应用](#)
- [使用AI应用部署在线服务](#)
- [WebSocket在线服务调用](#)

## 上传镜像至容器镜像服务

将准备好的本地镜像上传到容器镜像服务（SWR）。上传镜像的详细操作可参考[如何登录并上传镜像到SWR](#)。

## 使用镜像创建 AI 应用

1. 登录ModelArts管理控制台，进入“AI应用管理 > AI应用”页面，单击“创建”，跳转至创建AI应用页面。
2. 完成AI应用配置，部分配置如下：
  - 元模型来源：选择“从容器镜像中选择”。
  - 容器镜像所在的路径：选择[上传镜像至容器镜像服务](#)上传的路径。
  - 容器调用接口：根据实际情况配置容器调用接口。
  - 健康检查：保持默认。如果镜像中配置了健康检查则按实际情况配置健康检查。

图 11-48 AI 应用配置参数



- 单击“立即创建”，进入AI应用列表页，等AI应用状态变为“正常”，表示AI应用创建成功。

## 使用 AI 应用部署在线服务

- 登录ModelArts管理控制台，进入“部署上线 > 在线服务”页面，单击“部署”，跳转至在线服务部署页面。
- 完成服务的配置，部分配置如下：
  - 选择AI应用及版本：选择[使用镜像创建AI应用](#)创建完成的AI应用及版本
  - 升级为WebSocket：打开开关

图 11-49 升级为 WebSocket



- 单击“下一步”，确认配置后“提交”，完成在线服务的部署。返回在线服务列表页，查看服务状态变为“运行中”，表示服务部署成功。

## WebSocket 在线服务调用

WebSocket协议本身不提供额外的认证方式。不管自定义镜像里面是ws还是wss，经过ModelArts平台出去的WebSocket协议都是wss的。同时wss只支持客户端对服务端的单向认证，不支持服务端对客户端的双向认证。

可以使用ModelArts提供的以下认证方式：

- [token认证](#)
- [AK/SK](#)
- [APP认证](#)

WebSocket服务调用步骤如下（以图形界面的软件Postman进行预测，token认证为例）：

- [WebSocket连接的建立](#)
- [WebSocket客户端和服务端双向传输数据](#)

### 步骤1 WebSocket连接的建立


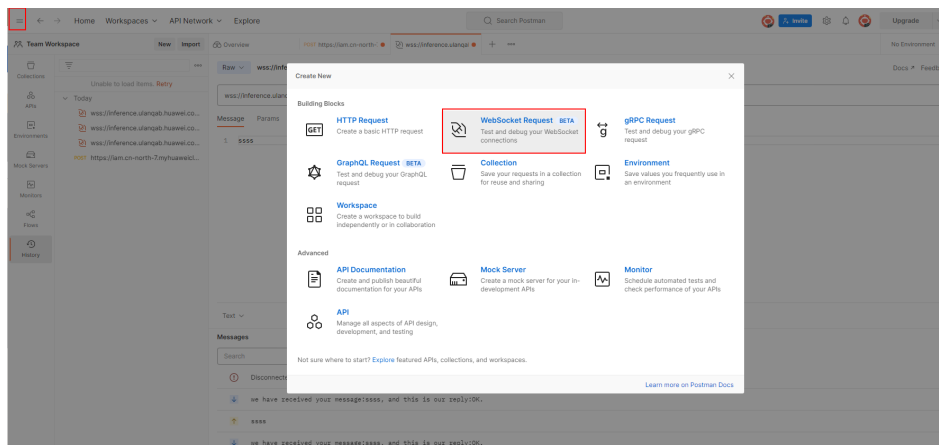
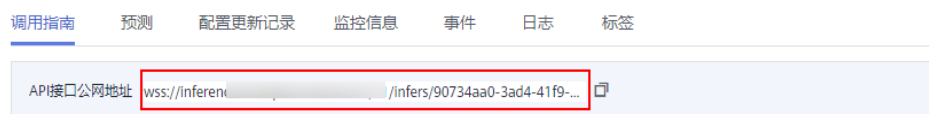
- 打开Postman（需选择8.5以上版本，以10.12.0为例）工具，单击左上角 ，选择“File>New”，弹出新建对话框，选择“WebSocket Request”（当前为beta版本）功能：

图 11-50 选择 WebSocket Request 功能



2. 在新建的窗口中填入WebSocket连接信息：  
左上角选择Raw，不要选择Socket.IO（一种WebSocket实现，要求客户端跟服务端都要基于Socket.IO），地址栏中填入从服务详情页“调用指南”页签中获取“API接口调用公网地址”后面的地址。如果自定义镜像中有更细粒度的地址，则在地址后面追加该URL。如果有queryString，那么在params栏中添加参数。在header中添加认证信息（不同认证方式有不同header，跟https的推理服务相同）。选择单击右上的connect按钮，建立WebSocket连接。

图 11-51 获取 API 接口调用公网地址

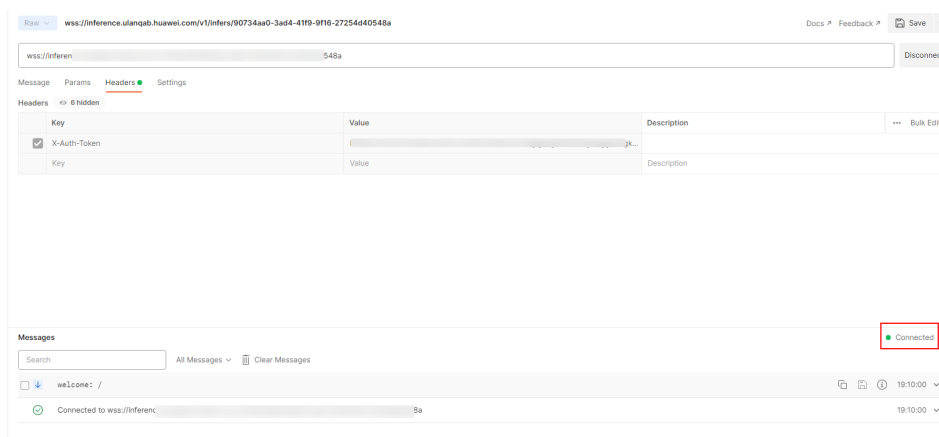


**说明**

- 如果信息正确，右下角连接状态处会显示：CONNECTED；
- 如果无法建立连接，如果是401状态码，检查认证信息；
- 如果显示WRONG\_VERSION\_NUMBER等关键字，检查自定义镜像的端口和ws跟wss的配置是否正确。

连接成功后结果如下：

图 11-52 连接成功



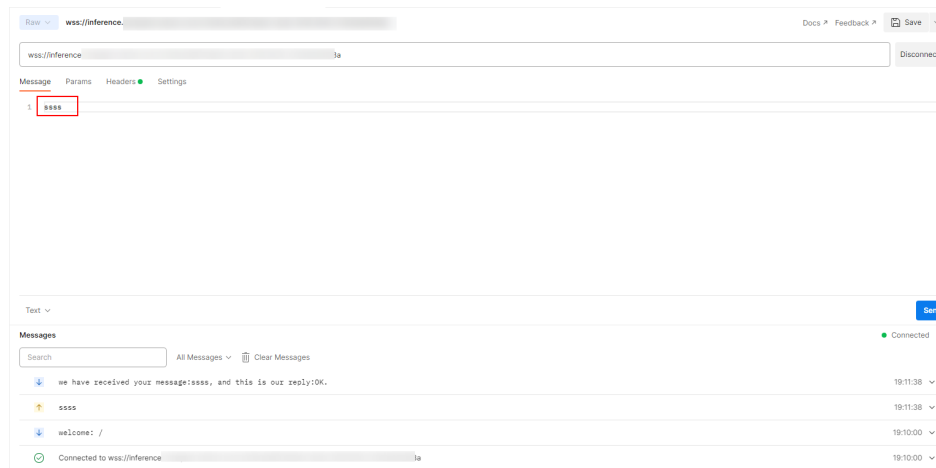
**须知**

优先验证自定义镜像提供的websocket服务的情况，不同的工具实现的websocket服务会有不同，可能出现连接建立后维持不住，可能出现请求一次后连接就中断需要重新连接的情况，ModelArts平台只保证，未上ModelArts前自定义镜像的websocket的形态跟上了ModelArts平台后的websocket形态相同（除了地址跟认证方式不同）。

**步骤2** WebSocket客户端和服务端双向传输数据

连接建立后，WebSocket使用TCP完成全双工通信。WebSocket的客户端可以往服务端发送数据，客户端有不同的实现，同一种语言也存在不同的lib包的实现，这里不考虑实现的不同种类。

客户端发送的内容在协议的角度不限定格式，Postman支持Text/Json/XML/HTML/Binary，以text为例，在输入框中输入要发送的文本，单击右侧中部的Send按钮即可将请求发往服务端，当文本内容过长，可能会导致postman工具卡住。

**图 11-53** 发送数据**----结束**



# 12 专属资源池训练

## 12.1 资源选择推荐

不同AI模型训练所需要的数据量和算力不同，在训练时选择合适存储及训练方案可提升模型训练效率与资源性价比。ModelArts支持单机单卡、单机多卡和多机多卡的训练场景，满足不同AI模型训练的要求。针对第一次使用ModelArts的用户，本文提供端到端案例指导，帮助您快速了解如何在ModelArts上选择合适的训练方案并进行模型训练。

针对不同的数据量和算法情况，推荐以下训练方案：

- 单机单卡：小数据量（1G训练数据）、低算力场景（1卡Vnt1），存储方案使用“OBS的并行文件系统（存放数据和代码）”。
- 单机多卡：中等数据量（50G左右训练数据）、中等算力场景（8卡Vnt1），存储方案使用SFS（存放数据和代码）。
- 多机多卡：大数据量（1T训练数据）、高算力场景（4台8卡Vnt1），存储方案使用“SFS（存放数据）+普通OBS桶（存放代码）”，采用分布式训练。

表 12-1 不同场景所需服务及购买推荐

| 场景   | OBS               | SFS | SWR | DEW | ModelArts | VPC | ECS | EVS   |
|------|-------------------|-----|-----|-----|-----------|-----|-----|-------|
| 单机单卡 | 按需购买。<br>（并行文件系统） | ×   | 免费。 | 免费。 | 包月购买。     | 免费。 | ×   | 按需购买。 |

| 场景   | OBS               | SFS                 | SWR | DEW | ModelArts | VPC | ECS                                                                  | EVS |
|------|-------------------|---------------------|-----|-----|-----------|-----|----------------------------------------------------------------------|-----|
| 单机多卡 | ×                 | 包月购买。<br>(HPC型500G) | 免费。 | 免费。 | 包月购买。     | 免费。 | 包月购买。<br>(Ubuntu 18.04, 建议不小于2U8G, 本地存储空间100G, 带EIP全动态BGP, 按流量10M带宽) | ×   |
| 多机多卡 | 按需购买。<br>(普通OBS桶) | 包月购买。<br>(HPC型500G) | 免费。 | 免费。 | 包月购买。     | 免费。 | 包月购买。<br>(建议不小于2U8G, 本地存储空间100G, 带EIP全动态BGP, 按流量10M带宽)               | ×   |

表 12-2 开源数据集训练效率参考

| 算法及数据                                            | 资源规格     | Epoch数 | 运行时长 (hh:mm:ss) |
|--------------------------------------------------|----------|--------|-----------------|
| 算法: PyTorch官方针对ImageNet的样例<br>数据: ImageNet分类数据子集 | 1机1卡Vnt1 | 10     | 0:05:03         |
| 算法: YOLOX<br>数据: COCO2017                        | 1机1卡Vnt1 | 10     | 03:33:13        |
|                                                  | 1机8卡Vnt1 | 10     | 01:11:48        |
|                                                  | 4机8卡Vnt1 | 10     | 0:36:17         |
| 算法: Swin-Transformer<br>数据: ImageNet21K          | 1机1卡Vnt1 | 10     | 197:25:03       |
|                                                  | 1机8卡Vnt1 | 10     | 26:10:25        |

| 算法及数据 | 资源规格     | Epoch数 | 运行时长 (hh:mm:ss) |
|-------|----------|--------|-----------------|
|       | 4机8卡Vnt1 | 10     | 07:08:44        |

表 12-3 训练各步骤性能参考

| 步骤           | 说明                                                 | 时长   |
|--------------|----------------------------------------------------|------|
| 镜像下载         | 首次下载镜像的时间 (25G)。                                   | 8分钟  |
| 资源调度         | 点创建训练任务开始到变成运行中的时间 (资源充足、镜像已缓存)。                   | 20秒  |
| 训练列表页打开      | 已有50条训练作业, 单击训练模块后的时间。                             | 6秒   |
| 日志加载         | 作业运行中, 已经输出1兆的日志文本, 单击训练详情页面需要多久加载出日志。             | 2.5秒 |
| 训练详情页        | 作业运行中, 没有用户日志情况下, 在ModelArts控制台主页面单击训练详情页面后加载页面内容。 | 2.5秒 |
| JupyterLab页面 | 进入JupyterLab页面后加载页面内容。                             | 0.5秒 |
| Notebook列表页  | 已有50个Notebook实例, 在ModelArts控制台主页面单击开发环境后的时间。       | 4.5秒 |

### 📖 说明

镜像下载时间受节点规格、节点硬盘类型 (高IO/普通IO)、是否SSD等因素影响, 以上数据仅供参考。

## 12.2 步骤总览

### 单机单卡

1. 资源购买:
  - a. [购买对象存储服务OBS](#)
  - b. [购买容器镜像服务SWR](#)
  - c. [创建网络](#)
  - d. [购买ModelArts专属资源池](#)
2. 基本配置:
  - a. [权限配置](#)

- b. [obsutils安装和配置](#)
- c. (可选) [工作空间配置](#)
3. 训练:
  - a. [线下容器镜像构建及调试](#)
  - b. [上传镜像](#)
  - c. [上传数据和算法至OBS \(首次使用时需要\)](#)
  - d. [使用Notebook进行代码调试](#)
  - e. [创建训练任务](#)

## 单机多卡

1. 资源购买:
  - a. [购买虚拟私有云VPC](#)
  - b. [购买弹性文件服务SFS](#)
  - c. [购买容器镜像服务SWR](#)
  - d. [创建网络](#)
  - e. [购买ModelArts专属资源池](#)
  - f. [购买弹性云服务器ECS](#)
2. 基本配置:
  - a. [权限配置](#)
  - b. [专属资源池VPC打通](#)
  - c. [ECS服务器挂载SFS Turbo存储](#)
  - d. (可选) [工作空间配置](#)
3. 训练:
  - a. [线下容器镜像构建及调试](#)
  - b. [上传镜像](#)
  - c. [上传数据和算法至SFS \(首次使用时需要\)](#)
  - d. [使用Notebook进行代码调试](#)
  - e. [创建训练任务](#)

## 多机多卡

1. 资源购买:
  - a. [购买虚拟私有云VPC](#)
  - b. [购买弹性文件服务SFS](#)
  - c. [购买对象存储服务OBS](#)
  - d. [购买容器镜像服务SWR](#)
  - e. [创建网络](#)
  - f. [购买ModelArts专属资源池](#)
  - g. [购买弹性云服务器ECS](#)
2. 基本配置:
  - a. [权限配置](#)

- b. [专属资源池VPC打通](#)
  - c. [ECS服务器挂载SFS Turbo存储](#)
  - d. [在ECS中创建ma-user和ma-group](#)
  - e. [obsutils安装和配置](#)
  - f. (可选) [工作空间配置](#)
3. 训练:
- a. [线下容器镜像构建及调试](#)
  - b. [上传镜像](#)
  - c. [上传数据至OBS \(首次使用时需要\)](#)
  - d. [上传算法至SFS](#)
  - e. [使用Notebook进行代码调试](#)
  - f. [创建训练任务](#)

## 12.3 资源购买

### 购买弹性文件服务 SFS

弹性文件服务默认为按需计费，即按购买的存储容量和时长收费。您也可以购买包年包月套餐，提前规划资源的使用额度和时长。在欠费时，您需要及时（15天之内）续费以避免您的文件系统资源被清空。SFS购买指导请参考[如何购买弹性文件服务？](#)。

### 购买容器镜像服务 SWR

容器镜像服务分为企业版和共享版。

共享版计费项包括存储空间和流量费用，目前均免费提供给您。

企业版当前仅支持按需计费模式，公测期间，可免费使用。

#### 说明

上传镜像前需要创建组织，创建步骤请参考[创建组织](#)。

### 购买对象存储服务 OBS

对象存储服务提供按需计费和包年包月两种计费模式，用户可以根据实际需求购买OBS服务。OBS服务支持以下两种存储方式，单机单卡场景使用文件系统，多机多卡场景使用普通OBS桶。

- [创建普通OBS桶](#)
- [创建并行文件系统](#)

### 购买数据加密服务 DEW

在使用Notebook进行代码调试时，如果要开启“SSH远程开发”功能，需要选择已有密钥对。密钥对可免费创建，您可通过管理控制台创建密钥对，操作指导请参考[如何创建密钥对？](#)。

## 购买虚拟私有云 VPC

虚拟私有云可以为您构建隔离的、用户自主配置和管理的虚拟网络环境，操作指导请参考[创建虚拟私有云和子网](#)。

## 购买弹性云服务器 ECS

如果您需要在服务器上部署相关业务，较之物理服务器，弹性云服务器的创建成本较低，并且可以在几分钟之内快速获得基于云服务平台的弹性云服务器设施，并且这些基础设施是弹性的，可以根据需求伸缩。下面介绍如何在管理控制台购买弹性云服务器。

购买流程：

- [步骤一：基础配置](#)
- [步骤二：网络配置](#)
- [步骤三：高级配置](#)
- [步骤四：确认订单](#)

### 📖 说明

购买时需注意，ECS需要和SFS买到同一个VPC才能挂载SFS存储。

## 购买 ModelArts 专属资源池

提供独享的计算资源，可用于Notebook、训练作业、部署模型。专属资源池不与其他用户共享，更加高效。在使用专属资源池之前，您需要先创建一个专属资源池，操作指导请参考[创建专属资源池](#)。

### 📖 说明

创建一个专属资源池前需要先创建网络，创建网络指导可参考[创建网络](#)。

## 购买 Notebook 存储

使用Notebook代码调试时，需要创建Notebook实例，如果创建时选择“云硬盘EVS”作为存储位置，会创建云硬盘EVS。磁盘规格默认5GB。

从Notebook实例创建成功开始，直至实例删除成功，磁盘每GB按照规定费用收费。

图 12-1 云硬盘 EVS



### 📖 说明

云硬盘EVS会在创建Notebook实例时自动购买，无需用户单独创建。

## 12.4 基本配置

## 12.4.1 权限配置

### 权限列表

为了便于理解权限相关内容，建议先阅读[ModelArts权限管理基本概念](#)。

表 12-4 服务授权列表

| 待授权的服务    | 适用场景                                                                                                                                                                                                                                               |
|-----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ModelArts | <p>授予子用户使用ModelArts服务的权限。</p> <p>ModelArts CommonOperations没有任何专属资源池的创建、更新、删除权限，只有使用权限。推荐给子用户配置此权限。</p> <p>如果需要给予子用户开通专属资源池的创建、更新、删除权限，此处要勾选ModelArts FullAccess，请谨慎配置。</p> <p>ModelArts FullAccess权限和ModelArts CommonOperations权限只能二选一，不能同时选。</p> |
| SFS弹性文件服务 | 弹性文件服务SFS Turbo的所有权限。使用SFS服务时需要配置。                                                                                                                                                                                                                 |
| ECS弹性云服务器 | 弹性云服务器所有权限。使用ECS服务时需要配置。                                                                                                                                                                                                                           |
| SWR容器镜像仓库 | 容器镜像仓库所有权限。使用SWR服务时需要配置。同时，还需开通SWR组织权限。                                                                                                                                                                                                            |
| VPC虚拟私有云  | 子用户在创建ModelArts的专属资源池过程中，如果需要开启自定义网络配置，需要配置VPC权限。                                                                                                                                                                                                  |
| DEW密钥管理服务 | 当子用户使用ModelArts Notebook的SSH远程功能时，需要配置子用户密钥管理服务的使用权限。                                                                                                                                                                                              |
| OBS对象存储服务 | 具有对象存储服务（OBS）查看桶列表、获取桶元数据、列举桶内对象、查询桶位置、上传对象、获取对象、删除对象、获取对象ACL等对象基本操作权限。                                                                                                                                                                            |

#### 12.4.1.1 配置 IAM 权限

1. 使用华为云主帐号创建一个开发者用户组user\_group，将开发者帐号加入用户组user\_group中。具体操作请参见[Step1 创建用户组并加入用户](#)。
2. 创建自定义策略。
  - a. 使用华为云主帐号登录控制台，单击右上角用户名，在下拉框中选择“统一身份认证”，进入IAM服务。

图 12-2 登录控制台



- b. 在统一身份认证服务控制台的左侧菜单栏中，选择“权限管理> 权限”。单击右上角“创建自定义策略”，“策略名称”为“Policy1”，策略配置方式选择JSON视图，输入策略内容，单击“确定”。
- c. 自定义策略“Policy1”的具体内容如下，可以直接复制粘贴。

```
{
 "Version": "1.1",
 "Statement": [
 {
 "Action": [
 "modelarts:*:*"
],
 "Effect": "Allow"
 },
 {
 "Action": [
 "modelarts:pool:create",
 "modelarts:pool:update",
 "modelarts:pool:delete"
],
 "Effect": "Deny"
 },
 {
 "Action": [
 "sfsturbo:*:*",
 "vpc:*:*",
 "dss:*:get",
 "dss:*:list"
],
 "Effect": "Allow"
 },
 {
 "Action": [
 "ecs:*:*",
 "evs:*:get",
 "evs:*:list",
 "evs:volumes:create",
 "evs:volumes:delete",
 "evs:volumes:attach",
 "evs:volumes:detach",
 "evs:volumes:manage",
 "evs:volumes:update",
 "evs:volumes:use",
 "evs:volumes:uploadImage",
 "evs:snapshots:create",
 "vpc:*:get",
 "vpc:*:list",
 "vpc:networks:create",
 "vpc:networks:update",
```



```

"vpc:subnets:update",
"vpc:subnets:create",
"vpc:ports:*",
"vpc:routers:get",
"vpc:routers:update",
"vpc:securityGroups:*",
"vpc:securityGroupRules:*",
"vpc:floatingIps:*",
"vpc:publicIps:*",
"ims:images:create",
"ims:images:delete",
"ims:images:get",
"ims:images:list",
"ims:images:update",
"ims:images:upload"
],
"Effect": "Allow"
},
{
"Action": [
"vpc:*:*",
"ecs:*:get*",
"ecs:*:list*"
],
"Effect": "Allow"
},
{
"Action": [
"kms:cmk:*",
"kms:dek:*",
"kms:grant:*",
"kms:cmkTag:*",
"kms:partition:*"
],
"Effect": "Allow"
}
}
]
}

```

3. 自定义策略“Policy2”的具体内容如下，可以直接复制粘贴。

```

{
"Version": "1.1",
"Statement": [
{
"Action": [
"obs:bucket:ListAllMybuckets",
"obs:bucket:HeadBucket",
"obs:bucket:ListBucket",
"obs:bucket:GetBucketLocation",
"obs:object:GetObject",
"obs:object:GetObjectVersion",
"obs:object:PutObject",
"obs:object:DeleteObject",
"obs:object:DeleteObjectVersion",
"obs:object:ListMultipartUploadParts",
"obs:object:AbortMultipartUpload",
"obs:object:GetObjectAcl",
"obs:object:GetObjectVersionAcl"
],
"Effect": "Allow"
}
]
}

```

### 说明

创建自定义策略时，建议将项目级云服务和全局级云服务拆分为两条策略，便于授权时设置最小授权范围。此处的“Policy1”为项目级云服务、“Policy2”为全局级云服务。[了解更多](#)。

4. 将自定义策略授权给开发者用户组user\_group。
  - a. 在统一身份认证服务控制台的左侧菜单栏中，选择“用户组”。在用户组页面单击对应用户组名称user\_group操作列的“授权”，勾选策略“Policy1”、“Policy2”、“SWR Admin”。单击“下一步”。

#### 说明

SWR的权限有SWR FullAccess、SWR OperateAccess、SWR ReadOnlyAccess。但SWR FullAccess、SWR OperateAccess、SWR ReadOnlyAccess仅限容器镜像服务企业版使用，目前企业版已暂停公测。非企业版用户暂不支持使用此权限。因此需要在此勾选“SWR Admin”策略。

- b. 选择授权范围方案为所有资源，单击“确定”。

图 12-3 选择用户组授权范围



## 精细化授权管理

如果您需要进行精细的权限管理，可参考《ModelArts API参考》中的权限策略和授权项。

- [数据管理权限](#)
- [开发环境权限](#)
- [训练作业权限](#)
- [模型管理权限](#)
- [服务管理权限](#)
- [工作空间管理权限](#)

精细化授权案例可参考[管理员和开发者权限分离](#)。

### 12.4.1.2 配置 ModelArts 委托权限

给用户配置ModelArts委托授权，允许ModelArts服务在运行时访问OBS等依赖服务。

1. 使用华为云主帐号登录ModelArts的管理控制台，在左侧导航栏单击“全局配置”，进入“全局配置”页面。

- 单击“添加授权”。在“访问授权”页面，在“授权对象类型”下面选择“IAM子用户”，“授权对象”选择管理员的帐号，选择“新增委托”，“权限配置”选择“普通用户”。

图 12-4 配置管理员用户委托授权

- 勾选“我已经仔细阅读并同意《 ModelArts服务声明 》”，单击“创建”。

### 12.4.1.3 配置 SWR 组织权限

IAM用户创建后，需要管理员在组织中为用户添加授权，使IAM用户对组织内所有镜像享有读取/编辑/管理的权限。

只有具备“管理”权限的帐号和IAM用户才能添加授权。

- 登录容器镜像服务控制台。
- 在左侧菜单栏选择“组织管理”，单击组织名称。
- 在“用户”页签下单击“添加授权”，在弹出的窗口中为IAM用户选择权限，然后单击“确定”。

SWR授权管理详情可参考[授权管理](#)。

#### 📖 说明

如果给予用户的SWR授权不是SWR Admin权限，则需要继续配置SWR组织权限。

### 12.4.1.4 测试用户权限

由于权限配置需要等待15-30分钟生效，建议在配置完成后，等待30分钟，再执行如下验证操作。

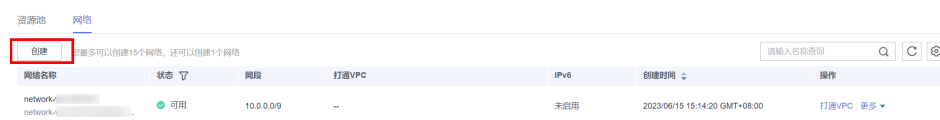
- 使用用户组02中任意一个子用户登录ModelArts管理控制台。在登录页面，请使用“IAM用户登录”方式进行登录。  
首次登录会提示修改密码，请根据界面提示进行修改。
- 验证ModelArts权限。
  - 在左上角的服务列表中，选择ModelArts服务，进入ModelArts管理控制台。
  - 在ModelArts管理控制台，可正常创建Notebook、训练作业、注册镜像。

3. 验证SFS权限。
  - a. 在左上角的服务列表中，选择SFS服务，进入SFS管理控制台。
  - b. 在SFS管理控制台，在SFS Turo中单击右上角的“创建文件系统”，如果能正常打开页面，表示当前用户具备SFS的操作权限。
4. 验证ECS权限。
  - a. 在左上角的服务列表中，选择ECS服务，进入ECS管理控制台。
  - b. 在ECS管理控制台，单击右上角的“购买弹性云服务器”，如果能正常打开页面，表示当前用户具备ECS的操作权限。
5. 验证VPC权限。
  - a. 在左上角的服务列表中，选择VPC服务，进入VPC管理控制台。
  - b. 在VPC管理控制台，单击右上角的“创建虚拟私有云”，如果能正常打开页面，表示当前用户具备VPC的操作权限。
6. 验证DEW权限。
  - a. 在左上角的服务列表中，选择DEW服务，进入DEW管理控制台。
  - b. 在DEW管理控制台，在“密钥对管理”-“私有密钥对”中单击“创建密钥对”，如果能正常打开页面，表示当前用户具备DEW的操作权限。
7. 验证OBS权限。
  - a. 在左上角的服务列表中，选择OBS服务，进入OBS管理控制台。
  - b. 在OBS管理控制台，单击右上角的“创建桶”，如果能正常打开页面，表示当前用户具备OBS的操作权限。
8. 验证SWR权限。
  - a. 在左上角的服务列表中，选择SWR服务，进入SWR管理控制台。
  - b. 在SWR管理控制台，如果能正常打开页面，表示当前用户具备SWR的操作权限。
  - c. 单击右上角的“上传镜像”，如果能看到授权的组织，表示当前用户具备SWR组织权限。

## 12.4.2 创建网络

1. 登录ModelArts管理控制台，在左侧导航栏中选择“专属资源池 > 弹性集群”，默认进入“资源池”页面。
2. 切换到“网络”页签，单击“创建”，弹出“创建网络”页面。

图 12-5 网络列表



3. 在“创建网络”弹窗中填写网络信息。
  - 网络名称：创建网络时默认生成网络名称，也可自行修改。
  - 网段类型：可选“预置”和“自定义”。
  - IPV6：开启IPV6功能后，将自动为子网分配IPV6网段，暂不支持自定义设置IPV6网段，该功能一旦开启，将不能关闭。（若创建网络时未勾选开启IPV6，也可在创建网络后在操作列单击“启动IPV6”）

图 12-6 创建网络

### 创建网络

网络名称

网段类型  预置  自定义

?

用户的VPC网段、容器网段（固定是172.16.0.0/16）、服务网段（固定是10.247.0.0/16）、创建的VPC网段只能在同一个工作空间可见。

IPv6 ?  开启IPv6

### 说明

- 单用户最多可创建15个网络。
  - 网段设置以后不能修改，避免与将要打通的VPC网段冲突。可能冲突的网段包括：
    - 用户的vpc网段
    - 容器网段（固定是172.16.0.0/16）
    - 服务网段（固定是10.247.0.0/16）
4. 确认无误后，单击“确定”。

## 12.4.3 专属资源池 VPC 打通

通过打通VPC，可以方便用户跨VPC使用资源，提升资源利用率。

1. 在“网络”页签，单击网络列表中某个网络操作列的“打通VPC”。

图 12-7 打通 VPC



2. 在打通VPC弹框中，打开“打通VPC”开关，在下拉框中选择可用的VPC和子网。

### 说明

需要打通的对端网络不能和当前网段重叠。

图 12-8 打通 VPC 参数选择



- 如果没有VPC可选，可以单击右侧的“创建虚拟私有云”，跳转到网络控制台，申请创建虚拟私有云。
- 如果没有子网可选，可以单击右侧的“创建子网”，跳转到网络控制台，创建可用的子网。
- 支持1个VPC下多个子网的打通，单击“+”即可添加子网（上限10个）。

## 12.4.4 ECS 服务器挂载 SFS Turbo 存储

本小节介绍如何在ECS服务器挂载SFS Turbo存储，挂载完成后可在后续步骤中，将训练所需的数据通过ECS上传至SFS Turbo。

### 前提条件

- 已创建SFS Turbo，如果未创建，请参考[创建文件系统](#)。
- 数据及算法已经上传至OBS，如果未上传，请参考[上传数据和算法至OBS（首次使用时需要）](#)。
- ECS服务器和SFS的共享硬盘在相同的VPC或者对应VPC能够互联。
- ECS服务器基础镜像需要用Ubuntu 18.04的。
- ECS服务器和SFS Turbo需要在同一子网中。

### 操作步骤

1. 在ECS服务器中设置华为云镜像源。  

```
sudo sed -i "s@http://.*archive.ubuntu.com@http://repo.huaweicloud.com@g" /etc/apt/sources.list
sudo sed -i "s@http://.*security.ubuntu.com@http://repo.huaweicloud.com@g" /etc/apt/sources.list
```
2. 安装NFS客户端，挂载对应盘。  

```
sudo apt-get update
sudo apt-get install nfs-common
```
3. 获取SFS Turbo的挂载命令。
  - a. 进入弹性文件服务SFS管理控制台。
  - b. 选择“SFS Turbo”进入文件系统列表，单击文件系统名称，进入详情页面。
  - c. 在“基本信息”页签获取并记录“Linux挂载命令”。
4. 在ECS服务器中挂载NFS存储。  
首先保证对应目录存在，然后输入对应指令即可。命令参考：

```
mkdir -p /mnt/sfs_turbo
mount -t nfs -o vers=3,nolock 192.168.0.169:/ /mnt/sfs_turbo
```

## 12.4.5 在 ECS 中创建 ma-user 和 ma-group

在ModelArts训练平台使用的自定义镜像时，默认用户为ma-user、默认用户组为ma-group。如果在训练时调用ECS中的文件，需要修改文件权限改为ma-user可读，否则会出现Permission denied错误，因此需要在ECS中提前创建好ma-user和ma-group。

在terminal中执行以下命令：

```
default_user=$(getent passwd 1000 | awk -F ':' '{print $1}') || echo "uid: 1000 does not exist" && \
default_group=$(getent group 100 | awk -F ':' '{print $1}') || echo "gid: 100 does not exist" && \
if [! -z ${default_group}] && [${default_group} != "ma-group"]; then \
 groupdel -f ${default_group}; \
 groupadd -g 100 ma-group; \
fi && \
if [-z ${default_group}]; then \
 groupadd -g 100 ma-group; \
fi && \
if [! -z ${default_user}] && [${default_user} != "ma-user"]; then \
 userdel -r ${default_user}; \
 useradd -d /home/ma-user -m -u 1000 -g 100 -s /bin/bash ma-user; \
 chmod -R 750 /home/ma-user; \
fi && \
if [-z ${default_user}]; then \
 useradd -d /home/ma-user -m -u 1000 -g 100 -s /bin/bash ma-user; \
 chmod -R 750 /home/ma-user; \
fi && \
set bash as default
rm /bin/sh && ln -s /bin/bash /bin/sh
```

查看创建的用户，执行以下命令：

```
id ma-user
```

如果出现以下信息则表示创建成功。

```
uid=1000(ma-user) gid=100(ma-group) groups=100(ma-group)
```

## 12.4.6 obsutil 安装和配置

obsutil是用于访问、管理对象存储服务OBS的命令行工具，使用该工具可以对OBS进行常用的配置管理操作，如创建桶、上传文件/文件夹、下载文件/文件夹、删除文件/文件夹等。

obsutil安装和配置的具体操作指导请参见[obsutils快速入门](#)。

### 须知

操作命令中的AK/SK要换成用户实际获取的AK/SK，Endpoint可以参考[终端节点 \(Endpoint\)](#)和[访问域名](#)获取。

## 12.4.7 (可选) 工作空间配置

ModelArts支持设置子用户的细粒度权限、不同工作空间之间资源隔离。ModelArts工作空间帮您实现项目资源隔离、多项目分开结算等功能。

如果你开通了企业项目管理服务的权限，可以在创建工作空间的时候绑定企业项目ID，并在企业项目下添加用户组，为不同的用户组设置细粒度权限供组里的用户使用。

如果你未开通企业项目管理服务的权限，也可以在ModelArts创建自己独立的工作空间，但是无法使用跟企业项目相关的功能。

### 📖 说明

工作空间为白名单功能，使用该功能需要提工单申请开通。

## 12.5 调试与训练

### 12.5.1 单机单卡

#### 12.5.1.1 线下容器镜像构建及调试

##### 镜像构建

##### 1. 导出conda环境

首先拉起线下的容器镜像：

```
run on terminal
docker run -ti ${your_image:tag}
```

在容器中输入如下命令，得到pytorch.tar.gz：

```
run on container

基于想要迁移的base环境创建一个名为pytorch的conda环境
conda create --name pytorch --clone base

pip install conda-pack

#将pytorch env打包生成pytorch.tar.gz
conda pack -n pytorch -o pytorch.tar.gz
```

将打包好的压缩包传到本地：

```
run on terminal
docker cp ${your_container_id}:/xxx/xxx/pytorch.tar.gz .
```

将pytorch.tar.gz上传到OBS并[设置公共读](#)，并在构建时wget获取、解压、清理。

##### 2. 新镜像构建

基础镜像一般选用ubuntu 18.04的官方镜像，或者nvidia官方提供的带cuda驱动的镜像。相关镜像直接到dockerhub官网查找即可。

构建流程：安装所需的apt包、驱动，配置ma-user用户、导入conda环境、配置Notebook依赖。

### 📖 说明

- 推荐使用Dockerfile的方式构建镜像。这样既满足dockerfile可追溯及构建归档的需求，也保证镜像内容无冗余和残留。
- 每层构建的时候都尽量把tar包等中间态文件删除，保证最终镜像更小，清理缓存的方法可参考：[conda clean](#)。

##### 3. 构建参考样例

Dockerfile样例：

```
FROM nvidia/cuda:11.3.1-cudnn8-devel-ubuntu18.04
```

```
USER root
```

```
section1: add user ma-user whose uid is 1000 and user group ma-group whose gid is 100. If there
```



```
already exists 1000:100 but not ma-user:ma-group, below code will remove it
RUN default_user=$(getent passwd 1000 | awk -F ':' '{print $1}') || echo "uid: 1000 does not exist" && \
default_group=$(getent group 100 | awk -F ':' '{print $1}') || echo "gid: 100 does not exist" && \
if [! -z ${default_group}] && [${default_group} != "ma-group"]; then \
 groupdel -f ${default_group}; \
 groupadd -g 100 ma-group; \
fi && \
if [-z ${default_group}]; then \
 groupadd -g 100 ma-group; \
fi && \
if [! -z ${default_user}] && [${default_user} != "ma-user"]; then \
 userdel -r ${default_user}; \
 useradd -d /home/ma-user -m -u 1000 -g 100 -s /bin/bash ma-user; \
 chmod -R 750 /home/ma-user; \
fi && \
if [-z ${default_user}]; then \
 useradd -d /home/ma-user -m -u 1000 -g 100 -s /bin/bash ma-user; \
 chmod -R 750 /home/ma-user; \
fi && \
set bash as default
rm /bin/sh && ln -s /bin/bash /bin/sh

section2: config apt source and install tools needed.
RUN sed -i "s@http://.*archive.ubuntu.com@http://repo.huaweicloud.com@g" /etc/apt/sources.list && \
sed -i "s@http://.*security.ubuntu.com@http://repo.huaweicloud.com@g" /etc/apt/sources.list && \
apt-get update && \
apt-get install -y ca-certificates curl ffmpeg git libgl1-mesa-glx libglib2.0-0 libibverbs-dev libjpeg-
dev libpng-dev libsm6 libxext6 libxrender-dev ninja-build screen sudo vim wget zip && \
apt-get clean && \
rm -rf /var/lib/apt/lists/*

USER ma-user

section3: install miniconda and rebuild conda env
RUN mkdir -p /home/ma-user/work/ && cd /home/ma-user/work/ && \
wget https://repo.anaconda.com/miniconda/Miniconda3-py37_4.12.0-Linux-x86_64.sh && \
chmod 777 Miniconda3-py37_4.12.0-Linux-x86_64.sh && \
bash Miniconda3-py37_4.12.0-Linux-x86_64.sh -bfp /home/ma-user/anaconda3 && \
wget https://${bucketname}.obs.cn-north-4.myhuaweicloud.com/${folder_name}/pytorch.tar.gz && \
mkdir -p /home/ma-user/anaconda3/envs/pytorch && \
tar -xzf pytorch.tar.gz -C /home/ma-user/anaconda3/envs/pytorch && \
source /home/ma-user/anaconda3/envs/pytorch/bin/activate && conda-unpack && \
/home/ma-user/anaconda3/bin/conda init bash && \
rm -rf /home/ma-user/work/*

ENV PATH=/home/ma-user/anaconda3/envs/pytorch/bin:$PATH

section4: settings of Jupyter Notebook for pytorch env
RUN source /home/ma-user/anaconda3/envs/pytorch/bin/activate && \
pip install ipykernel==6.7.0 --trusted-host https://repo.huaweicloud.com -i https://
repo.huaweicloud.com/repository/pypi/simple && \
ipython kernel install --user --env PATH /home/ma-user/anaconda3/envs/pytorch/bin:$PATH --
name=pytorch && \
rm -rf /home/ma-user/.local/share/jupyter/kernels/pytorch/logo-* && \
rm -rf ~/.cache/pip/* && \
echo 'export PATH=$PATH:/home/ma-user/.local/bin' >> /home/ma-user/.bashrc && \
echo 'export LD_LIBRARY_PATH=$LD_LIBRARY_PATH:/usr/local/nvidia/lib64' >> /home/ma-
user/.bashrc && \
echo 'conda activate pytorch' >> /home/ma-user/.bashrc

ENV DEFAULT_CONDA_ENV_NAME=pytorch
```

### 📖 说明

Dockerfile中的"[https://\\${bucket\\_name}.obs.cn-north-4.myhuaweicloud.com/\\${folder\\_name}/pytorch.tar.gz](https://${bucket_name}.obs.cn-north-4.myhuaweicloud.com/${folder_name}/pytorch.tar.gz)", 需要替换为1中pytorch.tar.gz在OBS上的路径（需将文件设置为公共读）。

进入Dockerfile目录，通过Dockerfile构建镜像命令：

```
cd 到Dockerfile所在目录下，输入构建命令
docker build -t ${image_name}:${image_version} .
例如
docker build -t pytorch-1.13-cuda11.3-cudnn8-ubuntu18.04:v1 .
```

### 📖 说明

- 容器镜像的大小建议小于15G，不能大于25G。否则镜像的迁移、拉起都会存在性能问题。
- 建议通过开源的官方镜像来构建，例如PyTorch的官方镜像。
- 建议容器分层构建，单层容量不要超过1G、文件数不大于10w个。分层时，先构建不常变化的层，例如：先OS，再cuda驱动，再Python，再pytorch，再其他依赖包。
- 不建议把数据、代码放到容器镜像里。因为对应内容应该是经常变动的，会导致频繁的容器镜像构建操作。
- 不建议在容器内再创建多个conda env。因为容器已经能满足隔离需求，没有必要再通过conda env做隔离。
- 本教程通过打包conda env来构建环境，也可以通过pip install、conda install等方式安装conda环境的依赖。
- 更多ModelArts自定义镜像介绍请见[自定义镜像简介](#)。

## 调试要点

1. 确认对应的脚本、代码、流程在linux服务器上运行正常。  
如果在linux服务器上运行就有问题，那么先调通以后再做容器镜像。
2. 确认打入镜像的文件是否在正确的位置、是否有正确的权限。  
训练场景主要查看自研的依赖包是否正常，查看pip list是否包含所需的包，查看容器直接调用的python是否是自己所需要的那个（如果容器镜像装了多个python，需要设置python路径的环境变量）。
3. 测试训练启动脚本
  - a. 优先使用手工进行数据复制的工作并验证  
一般在镜像里不包含训练所用的数据和代码，所以在启动镜像以后需要手工把需要的文件复制进去。建议数据、代码和中间数据都放到"/cache"目录，防止正式运行时磁盘占满（请见[ModelArts环境挂载目录说明](#)）。建议linux服务器申请的时候，有足够大的内存（8G以上）以及足够大的硬盘（100G以上）。  
docker和linux的文件交互命令如下：  

```
docker cp data/ 39c9ceedb1f6:/cache/
```

数据准备完成后，启动训练脚本，查看训练是否能够正常拉起。一般来说，启动脚本为：  

```
cd /cache/code/
python start_train.py
```

如果训练流程不符合预期，可以在容器实例中查看日志、错误等，并进行代码、环境变量的修正。
  - b. 预制脚本测试整体流程  
一般使用run.sh封装训练外的文件复制工作（数据、代码：OBS-->容器，输出结果：容器-->OBS），run.sh的构建方法参考[run.sh脚本测试ModelArts训练整体流程](#)。  
如果预制脚本调用结果不符合预期，可以在容器实例中进行修改和迭代。
  - c. 针对专属池场景  
由于专属池支持SFS挂载，因此代码、数据的导入会更简单，甚至可以不用再关注OBS的相关操作。

可以直接把SFS的目录直接挂载到调试节点的"/mnt/sfs\_turbo"目录，或者保证对应目录的内容和SFS盘匹配。

调试时建议使用接近的方式，即：启动容器实例时使用"-v"参数来指定挂载某个宿主机目录到容器环境。

```
docker run -ti -d -v /mnt/sfs_turbo:/sfs my_deeplearning_image:v1
```

上述命令表示把宿主机的"/mnt/sfs\_turbo"目录挂载到容器的"/sfs"目录，在宿主机和容器对应目录的所有改动都是实时同步的。

4. 分析错误时：训练镜像先看日志，推理镜像先看API的返回。

可以用过命令查看容器输出到stdout的所有日志：

```
docker logs -f 39c9ceedb1f6
```

一般在做推理镜像时，部分日志是直接存储在容器内部的，所以需要进入容器看日志。注意：重点对应日志中是否有ERROR（包括，容器启动时、API执行时）。

5. 牵扯部分文件用户组不一致的情况，可以在宿主机用root权限执行命令进行修改  

```
docker exec -u root:root 39c9ceedb1f6 bash -c "chown -R ma-user:ma-user /cache"
```
6. 针对调试中遇到的错误，可以直接在容器实例里修改，修改结果可以通过commit命令持久化。

### 📖 说明

建议把调试过程中的修改点通过Dockerfile固化到容器构建正式流程，并重新测试。

## 12.5.1.2 上传镜像

### 操作场景

客户端上传镜像，是指在安装了容器引擎客户端的机器上使用docker命令将镜像上传到容器镜像服务的镜像仓库。

如果容器引擎客户端机器为云上的ECS或CCE节点，根据机器所在区域有两种网络链路可以选择：

- 如果机器与容器镜像仓库在同一区域，则上传镜像走内网链路。
- 如果机器与容器镜像仓库不在同一区域，则上传镜像走公网链路，机器需要绑定弹性公网IP。

### 约束与限制

- 使用客户端上传镜像，镜像的每个layer大小不能大于10G。
- 上传镜像的容器引擎客户端版本必须为1.11.2及以上。

### 操作步骤

1. 连接容器镜像服务。
  - a. 登录容器镜像服务控制台。
  - b. 单击右上角“创建组织”，输入组织名称完成组织创建。请自定义组织名称，本示例使用“deep-learning”，下面的命令中涉及到组织名称“deep-learning”也请替换为自定义的值。

图 12-9 创建组织

### 创建组织

- 1.组织名称，全局唯一。
  - 2.当前租户最多可创建5个组织。
  - 3.建议一个组织对应一个公司、部门或个人，以便集中高效地管理镜像资源。
- 示例：  
以公司、部门作为组织:cloud-hangzhou、cloud-develop  
以个人作为组织:john

组织名称

deep-learning


- c. 选择左侧导航栏的“总览”，单击页面右上角的“登录指令”，在弹出的页面中单击  复制登录指令。

图 12-10 登录指令



### 登录指令



如何获取长期有效登录指令。

```
docker login -u cn-east-3@ [redacted] -p [redacted]
```

```
swr.cn-east-3.myhuaweicloud.com 
```

过期时间：2021/09/02 10:04:51 GMT+08:00

### 说明

- 此处生成的登录指令有效期为24小时，如果需要长期有效的登录指令，请参见[获取长期有效登录指令](#)。获取了长期有效的登录指令后，在有效期内的临时登录指令仍然可以使用。
  - 登录指令末尾的域名为镜像仓库地址，请记录该地址，后面会使用到。
- d. 在安装容器引擎的机器中执行上一步复制的登录指令。  
登录成功会显示“Login Succeeded”。
2. 在安装容器引擎的机器上执行如下命令，为镜像打标签。  
**docker tag [镜像名称1:版本名称1] [镜像仓库地址]/[组织名称]/[镜像名称2:版本名称2]**  
其中，
    - [镜像名称1:版本名称1]：\${image\_name}:\${image\_version}请替换为您所要上传的实际镜像的名称和版本名称。
    - [镜像仓库地址]：可在SWR控制台上查询，即1.c中登录指令末尾的域名。

- [组织名称]: `/${organization_name}`请替换为您创建的组织。
- [镜像名称2:版本名称2]: `${image_name}:${image_version}`请替换为您期待的镜像名称和镜像版本。

示例:

```
docker tag ${image_name}:${image_version} swr.cn-north-4.myhuaweicloud.com/${organization_name}/${image_name}:${image_version}
```

3. 上传镜像至镜像仓库。

**docker push** [镜像仓库地址]/[组织名称]/[镜像名称2:版本名称2]

示例:

```
docker push swr.cn-north-4.myhuaweicloud.com/${organization_name}/${image_name}:${image_version}
```

上传镜像完成后, 返回容器镜像服务控制台, 在“我的镜像”页面, 执行刷新操作后可查看到对应的镜像信息。

## 常见问题

### 为什么使用客户端上传镜像失败?

### 12.5.1.3 上传数据和算法至 OBS (首次使用时需要)

#### 前提条件

- 已经在OBS上创建好并行文件系统, 请参见[创建并行文件系统](#)。
- 已经在obsutil安装和配置, 请参见[obsutils安装和配置](#)。

#### 准备数据

1. 单击下载[动物数据集](#)至本地, 并解压。
2. 通过obsutil将数据集上传至OBS桶中。  

```
./obsutil cp ./dog_cat_1w obs://${your_obs_buck}/demo/ -f -r
```

#### 说明

OBS支持多种文件上传方式, 当文件少于100个时, 可以在OBS Console中上传, 当文件大于100个时, 推荐使用工具, 推荐[OBS Browser+](#) (win)、[obsutil](#) (linux)。上述例子为obsutil使用方法。

#### 准备算法

main.py文件内容如下, 并将其上传至OBS桶的demo文件夹中:

```
import argparse
import os
import random
import shutil
import time
import warnings
from enum import Enum
import torch
import torch.nn as nn
import torch.nn.parallel
import torch.backends.cudnn as cudnn
import torch.distributed as dist
import torch.optim
from torch.optim.lr_scheduler import StepLR
import torch.multiprocessing as mp
```

```
import torch.utils.data
import torch.utils.data.distributed
import torchvision.transforms as transforms
import torchvision.datasets as datasets
import torchvision.models as models
model_names = sorted(name for name in models.__dict__
 if name.islower() and not name.startswith("_")
 and callable(models.__dict__[name]))
parser = argparse.ArgumentParser(description='PyTorch ImageNet Training')
parser.add_argument('data', metavar='DIR', default='imagenet',
 help='path to dataset (default: imagenet)')
parser.add_argument('-a', '--arch', metavar='ARCH', default='resnet18',
 choices=model_names,
 help='model architecture: ' +
 ' | '.join(model_names) +
 ' (default: resnet18)')
parser.add_argument('-j', '--workers', default=4, type=int, metavar='N',
 help='number of data loading workers (default: 4)')
parser.add_argument('--epochs', default=90, type=int, metavar='N',
 help='number of total epochs to run')
parser.add_argument('--start-epoch', default=0, type=int, metavar='N',
 help='manual epoch number (useful on restarts)')
parser.add_argument('-b', '--batch-size', default=256, type=int,
 metavar='N',
 help='mini-batch size (default: 256), this is the total '
 'batch size of all GPUs on the current node when '
 'using Data Parallel or Distributed Data Parallel')
parser.add_argument('--lr', '--learning-rate', default=0.1, type=float,
 metavar='LR', help='initial learning rate, dest=lr')
parser.add_argument('--momentum', default=0.9, type=float, metavar='M',
 help='momentum')
parser.add_argument('--wd', '--weight-decay', default=1e-4, type=float,
 metavar='W', help='weight decay (default: 1e-4)',
 dest='weight_decay')
parser.add_argument('-p', '--print-freq', default=10, type=int,
 metavar='N', help='print frequency (default: 10)')
parser.add_argument('--resume', default='', type=str, metavar='PATH',
 help='path to latest checkpoint (default: none)')
parser.add_argument('-e', '--evaluate', dest='evaluate', action='store_true',
 help='evaluate model on validation set')
parser.add_argument('--pretrained', dest='pretrained', action='store_true',
 help='use pre-trained model')
parser.add_argument('--world-size', default=-1, type=int,
 help='number of nodes for distributed training')
parser.add_argument('--rank', default=-1, type=int,
 help='node rank for distributed training')
parser.add_argument('--dist-url', default='tcp://224.66.41.62:23456', type=str,
 help='url used to set up distributed training')
parser.add_argument('--dist-backend', default='nccl', type=str,
 help='distributed backend')
parser.add_argument('--seed', default=None, type=int,
 help='seed for initializing training. ')
parser.add_argument('--gpu', default=None, type=int,
 help='GPU id to use.')
parser.add_argument('--multiprocessing-distributed', action='store_true',
 help='Use multi-processing distributed training to launch '
 'N processes per node, which has N GPUs. This is the '
 'fastest way to use PyTorch for either single node or '
 'multi node data parallel training')
best_acc1 = 0

def main():
 args = parser.parse_args()
 if args.seed is not None:
 random.seed(args.seed)
 torch.manual_seed(args.seed)
 cudnn.deterministic = True
 warnings.warn("You have chosen to seed training. "
```

```
'This will turn on the CUDNN deterministic setting, '
'which can slow down your training considerably! '
'You may see unexpected behavior when restarting '
'from checkpoints.')
```

```
if args.gpu is not None:
 warnings.warn('You have chosen a specific GPU. This will completely '
 'disable data parallelism.')
```

```
if args.dist_url == "env://" and args.world_size == -1:
 args.world_size = int(os.environ["WORLD_SIZE"])
args.distributed = args.world_size > 1 or args.multiprocessing_distributed
ngpus_per_node = torch.cuda.device_count()
if args.multiprocessing_distributed:
 # Since we have ngpus_per_node processes per node, the total world_size
 # needs to be adjusted accordingly
 args.world_size = ngpus_per_node * args.world_size
 # Use torch.multiprocessing.spawn to launch distributed processes: the
 # main_worker process function
 mp.spawn(main_worker, nprocs=ngpus_per_node, args=(ngpus_per_node, args))
else:
 # Simply call main_worker function
 main_worker(args.gpu, ngpus_per_node, args)
```

```
def main_worker(gpu, ngpus_per_node, args):
 global best_acc1
 args.gpu = gpu
 if args.gpu is not None:
 print("Use GPU: {} for training".format(args.gpu))
 if args.distributed:
 if args.dist_url == "env://" and args.rank == -1:
 args.rank = int(os.environ["RANK"])
 if args.multiprocessing_distributed:
 # For multiprocessing distributed training, rank needs to be the
 # global rank among all the processes
 args.rank = args.rank * ngpus_per_node + gpu
 dist.init_process_group(backend=args.dist_backend, init_method=args.dist_url,
 world_size=args.world_size, rank=args.rank)
```

```
create model
if args.pretrained:
 print("=> using pre-trained model '{}".format(args.arch))
 model = models.__dict__[args.arch](pretrained=True)
else:
 print("=> creating model '{}".format(args.arch))
 model = models.__dict__[args.arch]()
```

```
if not torch.cuda.is_available():
 print('using CPU, this will be slow')
```

```
elif args.distributed:
 # For multiprocessing distributed, DistributedDataParallel constructor
 # should always set the single device scope, otherwise,
 # DistributedDataParallel will use all available devices.
 if args.gpu is not None:
 torch.cuda.set_device(args.gpu)
 model.cuda(args.gpu)
 # When using a single GPU per process and per
 # DistributedDataParallel, we need to divide the batch size
 # ourselves based on the total number of GPUs of the current node.
 args.batch_size = int(args.batch_size / ngpus_per_node)
 args.workers = int((args.workers + ngpus_per_node - 1) / ngpus_per_node)
 model = torch.nn.parallel.DistributedDataParallel(model, device_ids=[args.gpu])
 else:
 model.cuda()
 # DistributedDataParallel will divide and allocate batch_size to all
 # available GPUs if device_ids are not set
 model = torch.nn.parallel.DistributedDataParallel(model)
elif args.gpu is not None:
 torch.cuda.set_device(args.gpu)
 model = model.cuda(args.gpu)
else:
 # DataParallel will divide and allocate batch_size to all available GPUs
 if args.arch.startswith('alexnet') or args.arch.startswith('vgg'):
 model.features = torch.nn.DataParallel(model.features)
```

```
 model.cuda()
 else:
 model = torch.nn.DataParallel(model).cuda()
define loss function (criterion), optimizer, and learning rate scheduler
criterion = nn.CrossEntropyLoss().cuda(args.gpu)
optimizer = torch.optim.SGD(model.parameters(), args.lr,
 momentum=args.momentum,
 weight_decay=args.weight_decay)
"""Sets the learning rate to the initial LR decayed by 10 every 30 epochs"""
scheduler = StepLR(optimizer, step_size=30, gamma=0.1)
optionally resume from a checkpoint
if args.resume:
 if os.path.isfile(args.resume):
 print("> loading checkpoint '{}'".format(args.resume))
 if args.gpu is None:
 checkpoint = torch.load(args.resume)
 else:
 # Map model to be loaded to specified single gpu.
 loc = 'cuda:{}'.format(args.gpu)
 checkpoint = torch.load(args.resume, map_location=loc)
 args.start_epoch = checkpoint['epoch']
 best_acc1 = checkpoint['best_acc1']
 if args.gpu is not None:
 # best_acc1 may be from a checkpoint from a different GPU
 best_acc1 = best_acc1.to(args.gpu)
 model.load_state_dict(checkpoint['state_dict'])
 optimizer.load_state_dict(checkpoint['optimizer'])
 scheduler.load_state_dict(checkpoint['scheduler'])
 print("> loaded checkpoint '{}' (epoch {})"
 .format(args.resume, checkpoint['epoch']))
 else:
 print("> no checkpoint found at '{}'".format(args.resume))
cudnn.benchmark = True

Data loading code
traindir = os.path.join(args.data, 'train')
valdir = os.path.join(args.data, 'val')
normalize = transforms.Normalize(mean=[0.485, 0.456, 0.406],
 std=[0.229, 0.224, 0.225])
train_dataset = datasets.ImageFolder(
 traindir,
 transforms.Compose([
 transforms.RandomResizedCrop(224),
 transforms.RandomHorizontalFlip(),
 transforms.ToTensor(),
 normalize,
]))
if args.distributed:
 train_sampler = torch.utils.data.distributed.DistributedSampler(train_dataset)
else:
 train_sampler = None

train_loader = torch.utils.data.DataLoader(
 train_dataset, batch_size=args.batch_size, shuffle=(train_sampler is None),
 num_workers=args.workers, pin_memory=True, sampler=train_sampler)
val_loader = torch.utils.data.DataLoader(
 datasets.ImageFolder(valdir, transforms.Compose([
 transforms.Resize(256),
 transforms.CenterCrop(224),
 transforms.ToTensor(),
 normalize,
])),
 batch_size=args.batch_size, shuffle=False,
 num_workers=args.workers, pin_memory=True)
if args.evaluate:
 validate(val_loader, model, criterion, args)
 return

for epoch in range(args.start_epoch, args.epochs):
```



```
if args.distributed:
 train_sampler.set_epoch(epoch)
train for one epoch
train(train_loader, model, criterion, optimizer, epoch, args)
evaluate on validation set
acc1 = validate(val_loader, model, criterion, args)
scheduler.step()
remember best acc@1 and save checkpoint
is_best = acc1 > best_acc1
best_acc1 = max(acc1, best_acc1)
if not args.multiprocessing_distributed or (args.multiprocessing_distributed
 and args.rank % ngpus_per_node == 0):
 save_checkpoint({
 'epoch': epoch + 1,
 'arch': args.arch,
 'state_dict': model.state_dict(),
 'best_acc1': best_acc1,
 'optimizer': optimizer.state_dict(),
 'scheduler': scheduler.state_dict()
 }, is_best)
def train(train_loader, model, criterion, optimizer, epoch, args):
 batch_time = AverageMeter('Time', ':6.3f')
 data_time = AverageMeter('Data', ':6.3f')
 losses = AverageMeter('Loss', ':.4e')
 top1 = AverageMeter('Acc@1', ':6.2f')
 top5 = AverageMeter('Acc@5', ':6.2f')
 progress = ProgressMeter(
 len(train_loader),
 [batch_time, data_time, losses, top1, top5],
 prefix="Epoch: [{}]" .format(epoch))
 # switch to train mode
 model.train()
 end = time.time()
 for i, (images, target) in enumerate(train_loader):
 # measure data loading time
 data_time.update(time.time() - end)
 if args.gpu is not None:
 images = images.cuda(args.gpu, non_blocking=True)
 if torch.cuda.is_available():
 target = target.cuda(args.gpu, non_blocking=True)
 # compute output
 output = model(images)
 loss = criterion(output, target)
 # measure accuracy and record loss
 acc1, acc5 = accuracy(output, target, topk=(1, 5))
 losses.update(loss.item(), images.size(0))
 top1.update(acc1[0], images.size(0))
 top5.update(acc5[0], images.size(0))
 # compute gradient and do SGD step
 optimizer.zero_grad()
 loss.backward()
 optimizer.step()
 # measure elapsed time
 batch_time.update(time.time() - end)
 end = time.time()
 if i % args.print_freq == 0:
 progress.display(i)
def validate(val_loader, model, criterion, args):
 batch_time = AverageMeter('Time', ':6.3f', Summary.NONE)
 losses = AverageMeter('Loss', ':.4e', Summary.NONE)
 top1 = AverageMeter('Acc@1', ':6.2f', Summary.AVERAGE)
 top5 = AverageMeter('Acc@5', ':6.2f', Summary.AVERAGE)
 progress = ProgressMeter(
 len(val_loader),
 [batch_time, losses, top1, top5],
 prefix='Test: ')
 # switch to evaluate mode
 model.eval()
 with torch.no_grad():
```

```
end = time.time()
for i, (images, target) in enumerate(val_loader):
 if args.gpu is not None:
 images = images.cuda(args.gpu, non_blocking=True)
 if torch.cuda.is_available():
 target = target.cuda(args.gpu, non_blocking=True)
 # compute output
 output = model(images)
 loss = criterion(output, target)
 # measure accuracy and record loss
 acc1, acc5 = accuracy(output, target, topk=(1, 5))
 losses.update(loss.item(), images.size(0))
 top1.update(acc1[0], images.size(0))
 top5.update(acc5[0], images.size(0))
 # measure elapsed time
 batch_time.update(time.time() - end)
 end = time.time()
 if i % args.print_freq == 0:
 progress.display(i)
 progress.display_summary()
return top1.avg

def save_checkpoint(state, is_best, filename='checkpoint.pth.tar'):
 torch.save(state, filename)
 if is_best:
 shutil.copyfile(filename, 'model_best.pth.tar')

class Summary(Enum):
 NONE = 0
 AVERAGE = 1
 SUM = 2
 COUNT = 3

class AverageMeter(object):
 """Computes and stores the average and current value"""

 def __init__(self, name, fmt=':f', summary_type=Summary.AVERAGE):
 self.name = name
 self.fmt = fmt
 self.summary_type = summary_type
 self.reset()

 def reset(self):
 self.val = 0
 self.avg = 0
 self.sum = 0
 self.count = 0

 def update(self, val, n=1):
 self.val = val
 self.sum += val * n
 self.count += n
 self.avg = self.sum / self.count

 def __str__(self):
 fmtstr = '{name} {val} + self.fmt + ' }' (avg' + self.fmt + '})'
 return fmtstr.format(**self.__dict__)

 def summary(self):
 fmtstr = ""
 if self.summary_type is Summary.NONE:
 fmtstr = ""
 elif self.summary_type is Summary.AVERAGE:
 fmtstr = '{name} {avg:.3f}'
 elif self.summary_type is Summary.SUM:
 fmtstr = '{name} {sum:.3f}'
 elif self.summary_type is Summary.COUNT:
 fmtstr = '{name} {count:.3f}'
 else:
 raise ValueError('invalid summary type %r' % self.summary_type)
 return fmtstr.format(**self.__dict__)

class ProgressMeter(object):
 def __init__(self, num_batches, meters, prefix=""):

```

```

self.batch_fmtstr = self._get_batch_fmtstr(num_batches)
self.meters = meters
self.prefix = prefix
def display(self, batch):
 entries = [self.prefix + self.batch_fmtstr.format(batch)]
 entries += [str(meter) for meter in self.meters]
 print('\t'.join(entries))
def display_summary(self):
 entries = [" "]
 entries += [meter.summary() for meter in self.meters]
 print(' '.join(entries))
def _get_batch_fmtstr(self, num_batches):
 num_digits = len(str(num_batches // 1))
 fmt = '{:}' + str(num_digits) + 'd'
 return '[' + fmt + '/' + fmt.format(num_batches) + ']'

def accuracy(output, target, topk=(1,)):
 """Computes the accuracy over the k top predictions for the specified values of k"""
 with torch.no_grad():
 maxk = max(topk)
 batch_size = target.size(0)
 _, pred = output.topk(maxk, 1, True, True)
 pred = pred.t()
 correct = pred.eq(target.view(1, -1).expand_as(pred))
 res = []
 for k in topk:
 correct_k = correct[:k].reshape(-1).float().sum(0, keepdim=True)
 res.append(correct_k.mul_(100.0 / batch_size))
 return res
if __name__ == '__main__':
 main()

```

数据和算法在OBS桶的demo文件夹中，如下图所示。

图 12-11 demo 文件夹中的数据 and 算法



### 12.5.1.4 使用 Notebook 进行代码调试

#### 背景信息

- Notebook使用涉及到计费，具体收费项如下：
  - 处于“运行中”状态的Notebook，会消耗资源，产生费用。根据您选择的资源不同，收费标准不同，价格详情请参见[产品价格详情](#)。当您不需要使用Notebook时，建议停止Notebook，避免产生不必要的费用。

- 创建Notebook时，如果选择使用云硬盘EVS存储配置，云硬盘EVS会一直收费，建议及时停止并删除Notebook，避免产品不必要的费用。
- 在创建Notebook时，默认会开启自动停止功能，在指定时间内停止运行Notebook，避免资源浪费。
- 只有处于“运行中”状态的Notebook，才可以执行打开、停止操作。
- 一个帐户最多创建10个Notebook。

## 创建 Notebook 实例



1. 注册镜像。登录ModelArts控制台，在左侧导航栏选择“镜像管理”，进入镜像管理页面。单击“注册镜像”，镜像源即为推送到SWR中的镜像。请将完整的SWR地址复制到这里即可，或单击可直接从SWR选择自有镜像进行注册，类型勾选“GPU”，如图所示。

图 12-12 注册镜像

\* 镜像源   [查看可选镜像](#)  
 示例: <swr-domain-name>/<namespace>/<repository>/<tag>


描述  0/256


\* 架构  X86\_64  ARM


\* 类型  CPU  GPU

图 12-13 选择自有镜像

从容器镜像中选择

自有镜像 / my-images0012 / swr.c 

自有镜像  

| 镜像版本                                                                                      | 更新时间                          | 模板地址 | 大小         |
|-------------------------------------------------------------------------------------------|-------------------------------|------|------------|
|  0.0.4 | 2022/06/29 19:46:29 GMT+08:00 | ...  | 2349105373 |

10 总条数: 1 < 1 >

2. 登录ModelArts管理控制台，在左侧导航栏中选择“开发环境 > Notebook”，进入“Notebook”新版管理页面。

图 12-14 进入 Notebook



3. 单击“创建”，进入“创建Notebook”页面，请参见如下说明填写参数。
  - a. 填写Notebook基本信息，包含名称、描述、是否自动停止，详细参数请参见表12-5。

图 12-15 Notebook 基本信息

\* 名称

描述  0/256

\* 自动停止

*i* 开启该选项后，该Notebook实例将在运行时长超出您所选择的时长后，自动停止。

1小时  2小时  4小时  6小时  自定义

表 12-5 基本信息的参数描述

| 参数名称 | 说明                                               |
|------|--------------------------------------------------|
| “名称” | Notebook的名称。只能包含数字、大小写字母、下划线和中划线，长度不能大于64位且不能为空。 |
| “描述” | 对Notebook的简要描述。                                  |

| 参数名称   | 说明                                                                                                                                       |
|--------|------------------------------------------------------------------------------------------------------------------------------------------|
| “自动停止” | 默认开启，且默认值为“1小时”，表示该Notebook实例将在运行1小时之后自动停止，即1小时后停止规格资源计费。<br>开启自动停止功能后，可选择“1小时”、“2小时”、“4小时”、“6小时”或“自定义”几种模式。选择“自定义”模式时，可指定1~24小时范围内任意整数。 |

b. 填写Notebook详细参数，如镜像、资源规格等。

图 12-16 Notebook 实例的详细参数

The screenshot shows the configuration page for a Notebook instance. It includes several sections:

- 资源类型 (Resource Type):** Three tabs are visible: "公共资源池" (Public Resource Pool), "专属资源池" (Dedicated Resource Pool), and "专属资源池 New" (Dedicated Resource Pool New).
- 资源池规格 (Resource Pool Specification):** A table with columns: 名称 (Name), 状态 (Status), 节点规格 (Node Specification), and 总节点 (Total Nodes). One entry is shown with status "运行中" (Running) and specification "GPU: 8\*NVIDIA-V100(32GB) | CPU: 65 核 480GB".
- 规格 (Specification):** A dropdown menu showing "vGPU: 1\*v100(32GB)|CPU: 4vCPUs 32GB".
- 存储配置 (Storage Configuration):** Two tabs: "云硬盘EVS" (Cloud Disk EVS) and "弹性文件服务SFS" (Elastic File Service SFS).
- 磁盘规格 (Disk Specification):** A numeric input field set to "5" with "GB" as the unit. A warning icon indicates: "磁盘规格默认为5GB, 从Notebook实例创建成功起, 直至删除成功, 每GB按照规定费用收费。"

- 镜像：选择已上传的自定义镜像。
- 资源池类型：按实际情况选择已创建的专属资源池。
- 规格：选择1 GPU规格。
- 存储配置：选择“云硬盘EVS”作为存储位置。

#### 说明

如果需要通过VS Code连接Notebook方式进行代码调试，则需开启“SSH远程开发”并选择密钥对，请参考[VS Code连接Notebook方式介绍](#)。

- 参数填写完成后，单击“立即创建”进行规格确认。
- 参数确认无误后，单击“提交”，完成Notebook的创建操作。  
进入Notebook列表，正在创建中的Notebook状态为“创建中”，创建过程需要几分钟，请耐心等待。当Notebook状态变为“运行中”时，表示Notebook已创建并启动完成。  
如果创建Notebook启动失败，建议参考[调试要点](#)进行检查。
- 在Notebook列表，单击实例名称，进入实例详情页，查看Notebook实例配置信息。

图 12-17 查看 Notebook 实例详情



7. 挂载OBS并行文件系统：单击“添加数据存储”，设置挂载参数。
  - a. 设置本地挂载目录，在“/data/”目录下输入一个文件夹名称，例如：demo。挂载时，后台自动会在Notebook容器“的/data/”目录下创建该文件夹，用来挂载OBS文件系统。
  - b. 选择存放OBS并行文件系统下的文件夹，单击“确定”。

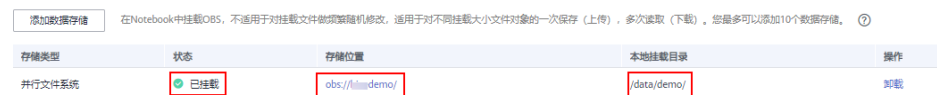
图 12-18 动态挂载 OBS

添加数据存储



8. 挂载成功后，可以在Notebook实例详情页查看到挂载结果。

图 12-19 挂载成功



9. 代码调试。  
打开Notebook，打开Terminal，进入步骤7中挂载的目录。

```
cd /data/demo
执行训练命令：
/home/ma-user/anaconda3/envs/pytorch/bin/python main.py -a resnet50 -b 128 --epochs 5
dog_cat_1w/
```

告警"RequestsDependencyWarning: urllib3 (1.26.8) or chardet (5.0.0)/charset\_normalizer (2.0.12) doesn't match a supported version!"不影响训练，可忽略。

### 📖 说明

Notebook中调试完后，如果镜像有修改，可以保存镜像用于后续训练，具体操作请参见[保存Notebook镜像环境](#)。

## 12.5.1.5 创建训练任务

### 📖 说明

针对专属池场景，应注意挂载的目录设置和调试时一致。

1. 登录ModelArts管理控制台，检查当前帐号是否已完成访问授权的配置。如未完成，请参考[使用委托授权](#)。针对之前使用访问密钥授权的用户，建议清空授权，然后使用委托进行授权。
2. 在左侧导航栏中选择“训练管理 > 训练作业”，默认进入“训练作业”列表。
3. 在“创建训练作业”页面，填写相关参数信息，然后单击“提交”。

图 12-20 训练参数 1

|                       |                                                                                                            |
|-----------------------|------------------------------------------------------------------------------------------------------------|
| * 创建方式                | <span>自定义算法</span> <span>我的算法</span> <span>我的订阅</span> <span>?</span>                                      |
| * 启动方式                | <span>预置框架</span> <span>自定义</span>                                                                         |
| * 镜像                  | <input type="text" value="orch-1.13-cuda11.3-cudnn8-ubuntu18.04:v1"/> <span>选择</span>                      |
| 代码目录                  | <input type="text" value="/demo/"/> <span>选择</span>                                                        |
| * 启动命令 <span>?</span> | <pre>1 cd \${MA_JOB_DIR} /demo &amp;&amp; python main.py -a resnet50 -b 128 -- epochs 10 dog_cat_1w/</pre> |
| 本地代码目录                | /home/ <input type="text" value="ma-user/modelarts/user-job-dir"/>                                         |
| 工作目录                  | <input type="text"/> <span>选择</span>                                                                       |



图 12-21 训练参数 2



- 创建方式：选择“自定义算法”。
  - 启动方式：选择“自定义”。
  - 镜像：选择上传的自定义镜像。
  - 启动命令：  

```
cd ${MA_JOB_DIR}/demo && python main.py -a resnet50 -b 128 --epochs 5 dog_cat_1w/
```

此处的“demo”为用户自定义的OBS存放代码路径的最后一级目录，可以根据实际修改。
  - 资源池：选择专属资源池
  - 规格：选择单GPU规格。
4. 单击“提交”，在“信息确认”页面，确认训练作业的参数信息，确认无误后单击“确定”。
  5. 训练作业创建完成后，后台将自动完成容器镜像下载、代码目录下载、执行启动命令等动作。

训练作业一般需要运行一段时间，根据您的训练业务逻辑和选择的资源不同，训练时长将持续几十分钟到几小时不等。训练作业执行成功后，日志信息如下所示。

### 12.5.1.6 监控资源

用户可以通过资源占用情况窗口查看计算节点的资源使用情况，最多可显示最近三天的数据。在资源占用情况窗口打开时，会定期向后台获取最新的资源使用率数据并刷新。

操作一：如果训练作业使用多个计算节点，可以通过实例名称的下拉框切换节点。

操作二：单击图例“cpuUsage”、“gpuMemUsage”、“gpuUtil”、“memUsage”、“npuMemUsage”、“npuUtil”、可以添加或取消对应参数的使用情况图。

操作三：鼠标悬浮在图片上的时间节点，可查看对应时间节点的占用率情况。

图 12-22 资源占用情况

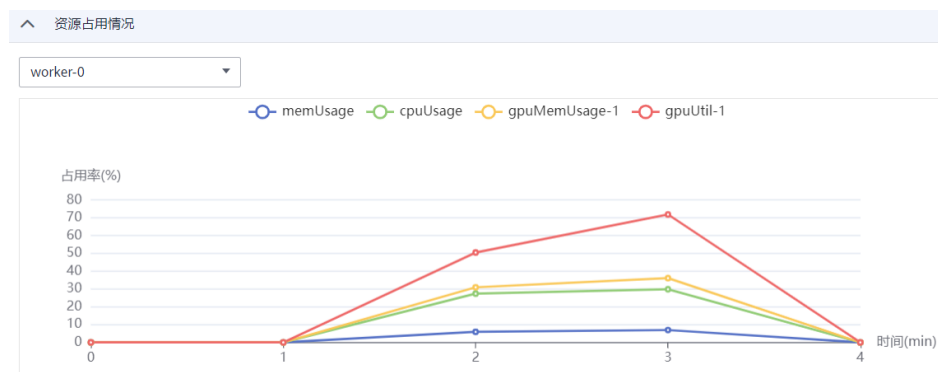


表 12-6 参数说明

| 参数          | 说明        |
|-------------|-----------|
| cpuUsage    | cpu使用率。   |
| gpuMemUsage | gpu内存使用率。 |
| gpuUtil     | gpu使用情况。  |
| memUsage    | 内存使用率。    |
| npuMemUsage | npu内存使用率。 |
| npuUtil     | npu使用情况。  |

## 12.5.2 单机多卡

### 12.5.2.1 线下容器镜像构建及调试

镜像构建及调试与单机单卡相同，请参考[线下容器镜像构建及调试](#)。

### 12.5.2.2 上传镜像

请参考[上传镜像](#)。

### 12.5.2.3 上传数据和算法至 SFS（首次使用时需要）

#### 前提条件

- ECS服务器已挂载SFS，请参考[ECS服务器挂载SFS Turbo存储](#)。
- 已经创建好，请参考[在ECS中创建ma-user和ma-group](#)。
- 已经安装obsutil，请参考[下载和安装obsutil](#)。

## 准备数据类似

1. 登录coco数据集下载官网地址：<https://cocodataset.org/#download>
2. 下载coco2017数据集的Train（18GB）、Val images（1GB）、Train/Val annotations（241MB），分别解压后并放入coco文件夹中。
3. 下载完成后，将数据上传至SFS相应目录中。由于数据集过大，推荐先通过obsutil工具将数据集传到OBS桶后，再将数据集迁移至SFS。
  - a. 在本机机器上运行，通过obsutil工具将本地数据集传到OBS桶。

```
将本地数据传至OBS中
./obsutil cp ${数据集所在的本地文件夹路径} ${存放数据集的obs文件夹路径} -f -r
例如
./obsutil cp ./coco obs://your_bucket/ -f -r
```
  - b. 登录ECS服务器，通过obsutil工具将数据集迁移至SFS，样例代码如下：

```
将OBS数据传至SFS中
./obsutil cp ${数据集所在的obs文件夹路径} ${SFS文件夹路径} -f -r
例如
./obsutil cp obs://your_bucket/coco/ /mnt/sfs_turbo/ -f -r
```

/mnt/sfs\_turbo/coco文件夹内目录结构如下：

```
coco
|--annotations
|--train2017
|--val2017
```

更多obsutil的操作，可参考[obsutil简介](#)。
  - c. 将文件设置归属为ma-user

```
chown -R ma-user:ma-group coco
```

## 代码云上适配

1. 下载YOLOX代码。代码仓地址：<https://github.com/Megvii-BaseDetection/YOLOX.git>。

```
git clone https://github.com/Megvii-BaseDetection/YOLOX.git
cd YOLOX
git checkout 4f8f1d79c8b8e530495b5f183280bab99869e845
```
2. 修改requirements.txt中的onnx版本，改为：onnx>=1.12.0。
3. 修改yolox/data/datasets/coco.py line59: data\_dir = os.path.join(get\_yolox\_datadir(), "COCO") --> data\_dir = '/home/ma-user/coco'。

```
data_dir = os.path.join(get_yolox_datadir(), "COCO")
data_dir = '/home/ma-user/coco'
```
4. 在tools/train.py的第13行前加两句代码：

```
加上这两句代码，防止运行时找不到yolox module
import sys
sys.path.append(os.getcwd())

line13
from yolox.core import launch
from yolox.exp import Exp, get_exp
```
5. yolox/layers/jit\_ops.py 第122行 fast\_cocoeval改为fast\_coco\_eval\_api

```
def __init__(self, name="fast_cocoeval"):
def __init__(self, name="fast_coco_eval_api"):
```
6. yolox\evaluators\coco\_evaluator.py 第294行 from yolox.layers import COCOeval\_opt as COCOeval 改为from pycocotools.cocoeval import COCOeval

```
try:
 # from yolox.layers import COCOeval_opt as COCOeval
 from pycocotools.cocoeval import COCOeval
except ImportError:
 from pycocotools.cocoeval import COCOeval
```

```
logger.warning("Use standard COCOeval.")
```

7. 在tools目录下新建一个run.sh作为启动脚本，run.sh内容可参考：

```
#!/usr/bin/env sh
set -x
set -o pipefail

export NCCL_DEBUG=INFO

DEFAULT_ONE_GPU_BATCH_SIZE=32
BATCH_SIZE=$((${MA_NUM_GPUS:-8} * ${VC_WORKER_NUM:-1} * ${DEFAULT_ONE_GPU_BATCH_SIZE}))
if [${VC_WORKER_HOSTS}];then
 YOLOX_DIST_URL=tcp://$(echo ${VC_WORKER_HOSTS} | cut -d "," -f 1):6666
 /home/ma-user/anaconda3/envs/pytorch/bin/python -u tools/train.py \
 -n yolox-s \
 --devices ${MA_NUM_GPUS:-8} \
 --batch-size ${BATCH_SIZE} \
 --fp16 \
 --occupy \
 --num_machines ${VC_WORKER_NUM:-1} \
 --machine_rank ${VC_TASK_INDEX:-0} \
 --dist-url ${YOLOX_DIST_URL}
else
 /home/ma-user/anaconda3/envs/pytorch/bin/python -u tools/train.py \
 -n yolox-s \
 --devices ${MA_NUM_GPUS:-8} \
 --batch-size ${BATCH_SIZE} \
 --fp16 \
 --occupy \
 --num_machines ${VC_WORKER_NUM:-1} \
 --machine_rank ${VC_TASK_INDEX:-0}
fi
```

### 📖 说明

部分环境变量在Notebook环境中不存在，因此需要提供默认值。

8. 将代码放到OBS上，然后通过OBS将代码传至SFS相应目录中。
- 在本机机器上运行，通过obsutil工具将本地数据集传到OBS桶。  
# 将本地代码传至OBS中  

```
./obsutil cp ./YOLOX obs://your_bucket/ -f -r
```
  - 登录ECS服务器，通过obsutil工具将数据集迁移至SFS，样例代码如下：  
# 将OBS的代码传到SFS中  

```
./obsutil cp obs://your_bucket/YOLOX/ /mnt/sfs_turbo/code/ -f -r
```

### 📖 说明

本案例中以obsutils方式上传文件，除此之外也可通过SCP方式上传文件，具体操作步骤可参考[本地Linux主机使用SCP上传文件到Linux云服务器](#)。

9. 在SFS中将文件设置归属为ma-user  

```
chown -R ma-user:ma-group YOLOX
```
10. 执行以下命令，去除Shell脚本的\r字符。  

```
cd YOLOX
sed -i 's/\r/' run.sh
```

### 📖 说明

Shell脚本在Windows系统编写时，每行结尾是\r\n，而在Linux系统中行每行结尾是\n，所以在Linux系统中运行脚本时，会认为\r是一个字符，导致运行报错“\$'\r': command not found”，因此需要去除Shell脚本的\r字符。

## 12.5.2.4 使用 Notebook 进行代码调试

### 背景信息

- Notebook使用涉及到计费，具体收费项如下：
  - 处于“运行中”状态的Notebook，会消耗资源，产生费用。根据您选择的资源不同，收费标准不同，价格详情请参见[产品价格详情](#)。当您不需要使用Notebook时，建议停止Notebook，避免产生不必要的费用。
  - 创建Notebook时，如果选择使用云硬盘EVS存储配置，云硬盘EVS会一直收费，建议及时停止并删除Notebook，避免产品不必要的费用。
- 在创建Notebook时，默认会开启自动停止功能，在指定时间内停止运行Notebook，避免资源浪费。
- 只有处于“运行中”状态的Notebook，才可以执行打开、停止操作。
- 一个帐户最多创建10个Notebook。

### 创建 Notebook 实例



1. 注册镜像。登录ModelArts控制台，在左侧导航栏选择“镜像管理”，进入镜像管理页面。单击“注册镜像”，镜像源即为推送到SWR中的镜像。请将完整的SWR地址复制到这里即可，或单击可直接从SWR选择自有镜像进行注册，如图所示。

图 12-23 注册镜像

\* 镜像源   [查看可选镜像](#)  
 示例: <swr-domain-name>/<namespace>/<repository>/<tag>


描述


\* 架构  X86\_64  ARM

\* 类型  CPU  GPU

图 12-24 选择自有镜像

从容器镜像中选择

自有镜像 /  

自有镜像  

| 镜像版本                                   | 更新时间                          | 模板地址 | 大小         |
|----------------------------------------|-------------------------------|------|------------|
| <input checked="" type="radio"/> 0.0.4 | 2022/06/29 19:46:29 GMT+08:00 | ...  | 2349105373 |

10 总条数: 1 < 1 >

2. 登录ModelArts管理控制台，在左侧导航栏中选择“开发环境 > Notebook”，进入“Notebook”新版管理页面。

图 12-25 进入 Notebook



3. 单击“创建”，进入“创建Notebook”页面，请参见如下说明填写参数。
  - a. 填写Notebook基本信息，包含名称、描述、是否自动停止，详细参数请参见表12-7。

图 12-26 Notebook 基本信息

\* 名称

描述  0/256

\* 自动停止

*i* 开启该选项后，该Notebook实例将在运行时长超出您所选择的时长后，自动停止。

1小时  2小时  4小时  6小时  自定义

表 12-7 基本信息的参数描述

| 参数名称 | 说明                                               |
|------|--------------------------------------------------|
| “名称” | Notebook的名称。只能包含数字、大小写字母、下划线和中划线，长度不能大于64位且不能为空。 |
| “描述” | 对Notebook的简要描述。                                  |

| 参数名称   | 说明                                                                                                                                       |
|--------|------------------------------------------------------------------------------------------------------------------------------------------|
| “自动停止” | 默认开启，且默认值为“1小时”，表示该Notebook实例将在运行1小时之后自动停止，即1小时后停止规格资源计费。<br>开启自动停止功能后，可选择“1小时”、“2小时”、“4小时”、“6小时”或“自定义”几种模式。选择“自定义”模式时，可指定1~24小时范围内任意整数。 |

b. 填写Notebook详细参数，如镜像、资源规格等。

图 12-27 Notebook 实例的详细参数

The screenshot shows the configuration page for a Notebook instance. It includes sections for:

- 镜像 (Image):** Options for '公共镜像' (Public Image) and '自定义镜像' (Custom Image). A search bar shows 'pytorch-1.13-cuda11.3'.
- 资源池类型 (Resource Pool Type):** Options for '公共资源池' (Public Resource Pool) and '专属资源池' (Dedicated Resource Pool).
- 资源池规格 (Resource Pool Specification):** A table with columns for '名称' (Name), '状态' (Status), '节点规格' (Node Specification), and '总节点' (Total Nodes). One entry is shown with name 'sa', status '运行中' (Running), and specification 'GPU: 8\*NVIDIA-V100(32GB) | CPU: 65 核 480GB'.
- 规格 (Specification):** A dropdown menu showing 'GPU: 8\*V100(256GB)|CPU: 72核 512GB'.
- 存储配置 (Storage Configuration):** Options for '云硬盘EVS' (Cloud Disk EVS) and '弹性文件服务SFS' (Elastic File Service SFS). A sub-section for SFS shows '弹性文件服务' (Elastic File Service) set to 'sfs-tu' and a '子目录挂载' (Subdirectory Mount) field.
- SSH远程开发 (SSH Remote Development):** A toggle switch that is currently turned off.

- 镜像：选择已上传的自定义镜像。
- 资源池类型：按实际情况选择已创建的专属资源池。
- 规格：选择8卡GPU规格。（run.sh文件中默认MA\_NUM\_GPUS为8卡，因此选择notebook规格时需要与MA\_NUM\_GPUS默认值相同）
- 存储配置：选择“弹性文件服务SFS”作为存储位置。子目录挂载可不填写，如果需挂载SFS指定目录，填在子目录挂载出填写具体路径。

### 📖 说明

如果需要通过VS Code连接Notebook方式进行代码调试，则需开启“SSH远程开发”并选择密钥对，请参考[VS Code连接Notebook方式介绍](#)。

4. 参数填写完成后，单击“立即创建”进行规格确认。
5. 参数确认无误后，单击“提交”，完成Notebook的创建操作。

进入Notebook列表，正在创建中的Notebook状态为“创建中”，创建过程需要几分钟，请耐心等待。当Notebook状态变为“运行中”时，表示Notebook已创建并启动完成。

6. 在Notebook列表，单击实例名称，进入实例详情页，查看Notebook实例配置信息。

图 12-28 查看 Notebook 实例详情



7. 在Notebook中打开Terminal，输入启动命令调试代码。

```
建立数据集软链接
ln -s /home/ma-user/work/${coco数据集在SFS上的路径} /home/ma-user/coco
进入到对应目录
cd /home/ma-user/work/${YOLOX在SFS上的路径}
安装环境并执行脚本
/home/ma-user/anaconda3/envs/pytorch/bin/pip install -r requirements.txt && /bin/sh tools/run.sh

例如
ln -s /home/ma-user/work/coco /home/ma-user/coco
cd /home/ma-user/work/code/YOLOX/
/home/ma-user/anaconda3/envs/pytorch/bin/pip install -r requirements.txt && /bin/sh tools/run.sh
```

**说明**

Notebook中调试完后，如果镜像有修改，可以保存镜像用于后续训练，具体操作请参见[保存Notebook镜像环境](#)。

### 12.5.2.5 创建训练任务

1. 登录ModelArts管理控制台，检查当前帐号是否已完成访问授权的配置。如未完成，请参考[使用委托授权](#)针对之前使用访问密钥授权的用户，建议清空授权，然后使用委托进行授权。
2. 在左侧导航栏中选择“训练管理 > 训练作业”，默认进入“训练作业”列表。
3. 在“创建训练作业”页面，填写相关参数信息，然后单击“提交”。



图 12-29 训练参数

图 12-30 资源规格

- 创建方式：选择“自定义算法”。
- 启动方式：选择“自定义”。
- 镜像：选择上传的自定义镜像。
- 启动命令：

```
In -s /home/ma-user/work/coco /home/ma-user/coco && cd /home/ma-user/work/code/
YOLOX/ && /home/ma-user/anaconda3/envs/pytorch/bin/pip install -r requirements.txt
&& /bin/sh tools/run.sh
```

- 资源池：选择专属资源池。
- 规格：选择8卡GPU规格。
- 计算节点：1。
- SFS Turbo：增加挂载配置，选择SFS名称，云上挂载路径为“/home/ma-user/work”。

#### 📖 说明

为了和Notebook调试时代码路径一致，保持相同的启动命令，因此云上挂载路径需要填写为“/home/ma-user/work”。

4. 单击“提交”，在“信息确认”页面，确认训练作业的参数信息，确认无误后单击“确定”。
5. 训练作业创建完成后，后台将自动完成容器镜像下载、代码目录下载、执行启动命令等动作。

训练作业一般需要运行一段时间，根据您的训练业务逻辑和选择的资源不同，训练时长将持续几十分钟到几小时不等。训练作业执行成功后，日志信息如下所示。

## 12.5.3 多机多卡

### 12.5.3.1 线下容器镜像构建及调试

镜像构建及调试与单机单卡相同，请参考[线下容器镜像构建及调试](#)。

### 12.5.3.2 上传镜像

请参考[上传镜像](#)。

### 12.5.3.3 上传数据至 OBS（首次使用时需要）

#### 前提条件

- 已经在OBS上创建好普通OBS桶，请参见[创建普通OBS桶](#)。
- 已经安装obsutil，请参考[下载和安装obsutil](#)。

#### 操作步骤

1. 登录Imagenet数据集下载官网地址，下载Imagenet21k数据集：<http://image-net.org/>
2. 下载格式转换后的annotation文件：  
[ILSVRC2021winner21k\\_whole\\_map\\_train.txt](#) 和  
[ILSVRC2021winner21k\\_whole\\_map\\_val.txt](#)。
3. 下载完成后将上述3个文件数据上传至OBS桶中的imagenet21k\_whole文件夹中。上传方法请参考[上传数据和算法至OBS（首次使用时需要）](#)。

### 12.5.3.4 上传算法至 SFS

1. 下载Swin-Transformer代码。  
git clone --recursive <https://github.com/microsoft/Swin-Transformer.git>
2. 修改lr\_scheduler.py文件，把第27行：t\_mul=1. 注释掉。
3. 修改data文件夹下imagenet22k\_dataset.py，把第28行：print("ERROR IMG LOADED: ", path) 注释掉。
4. 修改data文件夹下的build.py文件，把第112行：prefix = 'ILSVRC2011fall\_whole'，改为prefix = 'ILSVRC2021winner21k\_whole'。
5. 在Swin-Transformer目录下创建requirements.txt指定python依赖库：  
# requirements.txt内容如下  

```
timm==0.4.12
termcolor==1.1.0
yacs==0.1.8
```
6. 准备run.sh文件中所需要的obs文件路径。
  - a. 准备imagenet数据集的分享链接  
勾选要分享的imagenet21k\_whole数据集文件夹，单击分享按钮，选择分享链接有效期，自定义提取码，例如123456，单击“复制链接”，记录该链接。
  - b. 准备obsutil\_linux\_amd64.tar.gz的分享链接  
单击[此处](#)下载obsutil\_linux\_amd64.tar.gz，将其上传至OBS桶中，设置为公共读。单击属性，单击复制链接。  
链接样例如下：  
`https://${bucketname_name}.obs.cn-north-4.myhuaweicloud.com/${folders_name}/pytorch.tar.gz`
7. 在Swin-Transformer目录下，创建运行脚本run.sh。

#### 📖 说明

- 脚本中的"SRC\_DATA\_PATH=\${imagenet数据集在obs中分享链接}"，需要替换为上一步中的imagenet21k\_whole文件夹分享链接。
- 脚本中的"`https://${bucket_name}.obs.cn-north-4.myhuaweicloud.com/${folder_name}/obsutil_linux_amd64.tar.gz`"，需要替换为上一步中obsutil\_linux\_amd64.tar.gz在OBS上的路径（需将文件设置为公共读）。

单机单卡运行脚本：

# 在代码主目录下创建一个run.sh，内容如下

```
#!/bin/bash
```

```
从obs中下载数据到本地SSD盘
```

```
DIS_DATA_PATH=/cache
```

```
SRC_DATA_PATH=${imagenet数据集在obs中分享链接}
```

```
OBSUTIL_PATH=https://${bucket_name}.obs.cn-north-4.myhuaweicloud.com/${folder_name}/
```

```
obsutil_linux_amd64.tar.gz
```

```
mkdir -p $DIS_DATA_PATH && cd $DIS_DATA_PATH && wget $OBSUTIL_PATH && tar -xzf
```

```
obsutil_linux_amd64.tar.gz && $DIS_DATA_PATH/obsutil_linux_amd64*/obsutil share-cp
```

```
$SRC_DATA_PATH $DIS_DATA_PATH/ -ac=123456 -r -f -j 256 && cd -
```

```
IMAGE_DATA_PATH=$DIS_DATA_PATH/imagenet21k_whole
```

```
MASTER_PORT="6061"
```

```
/home/ma-user/anaconda3/envs/pytorch/bin/python -m torch.distributed.launch --nproc_per_node=1
```

```
--master_addr localhost --master_port=$MASTER_PORT main.py --data-path $IMAGE_DATA_PATH --
```

```
cfg ./configs/swin/swin_base_patch4_window7_224_22k.yaml --local_rank 0
```

多机多卡运行脚本：

```
创建run.sh

#!/bin/bash

从obs中下载数据到本地SSD盘
DIS_DATA_PATH=/cache
SRC_DATA_PATH=${imagenet数据集在obs中分享链接}
OBSUTIL_PATH=https://${bucket_name}.obs.cn-north-4.myhuaweicloud.com/${folder_name}/
obsutil_linux_amd64.tar.gz
mkdir -p $DIS_DATA_PATH && cd $DIS_DATA_PATH && wget $OBSUTIL_PATH && tar -xzf
obsutil_linux_amd64.tar.gz && $DIS_DATA_PATH/obsutil_linux_amd64*/obsutil share-cp
$SRC_DATA_PATH $DIS_DATA_PATH/ -ac=123456 -r -f -j 256 && cd -
IMAGE_DATA_PATH=$DIS_DATA_PATH/imagenet21k_whole
MASTER_ADDR=$(echo ${VC_WORKER_HOSTS} | cut -d " " -f 1)

MASTER_PORT="6060"
NNODES="$VC_WORKER_NUM"
NODE_RANK="$VC_TASK_INDEX"
NGPUS_PER_NODE="$MA_NUM_GPUS"

/home/ma-user/anaconda3/envs/pytorch/bin/python -m torch.distributed.launch --nnode=$NNODES
--node_rank=$NODE_RANK --nproc_per_node=$NGPUS_PER_NODE --master_addr $MASTER_ADDR --
master_port=$MASTER_PORT main.py --data-path $IMAGE_DATA_PATH --cfg ./configs/swin/
swin_base_patch4_window7_224_22k.yaml
```

### 📖 说明

- 推荐先使用单机单卡运行脚本，待正常运行后再改用多机多卡运行脚本。
  - 多机多卡run.sh中的“VC\_WORKER\_HOSTS”、“VC\_WORKER\_NUM”、“VC\_TASK\_INDEX”、“MA\_NUM\_GPUS”为ModelArts训练容器中预置的环境变量。训练容器环境变量详细介绍可参考[查看训练容器环境变量](#)。
8. 通过obsutils，将代码文件夹放到OBS上，然后通过OBS将代码传至SFS相应目录中。
  9. 在SFS中将代码文件Swin-Transformer-main设置归属为ma-user。  
chown -R ma-user:ma-group Swin-Transformer
  10. 执行以下命令，去除Shell脚本的\r字符。  
cd Swin-Transformer  
sed -i 's/\r/' run.sh

### 📖 说明

Shell脚本在Windows系统编写时，每行结尾是\r\n，而在Linux系统中行每行结尾是\n，所以在Linux系统中运行脚本时，会认为\r是一个字符，导致运行报错“\$'\r': command not found”，因此需要去除Shell脚本的\r字符。

## 12.5.3.5 使用 Notebook 进行代码调试

由于Notebook的/cache目录只能支持500G的存储，超过后会导致实例重启，ImageNet数据集大小超过该限制，因此建议用线下资源调试、或用小批量数据集在Notebook调试（Notebook调试方法与[使用Notebook进行代码调试](#)、[使用Notebook进行代码调试](#)相同）。

## 12.5.3.6 创建训练任务

1. 登录ModelArts管理控制台，检查当前帐号是否已完成访问授权的配置。如未完成，请参考[使用委托授权](#)。针对之前使用访问密钥授权的用户，建议清空授权，然后使用委托进行授权。
2. 在左侧导航栏中选择“训练管理 > 训练作业”，默认进入“训练作业”列表。
3. 在“创建训练作业”页面，填写相关参数信息，然后单击“提交”。

图 12-31 创建训练作业参数 1

\* 创建方式 自定义算法 我的算法 我的订阅 ?

\* 启动方式 预置框架 自定义

\* 镜像  选择

代码目录  选择

\* 启动命令 ?

```
1 cd /home/ma-user/work/code/Swin-Transformer && /home/ma-user/anaconda3/envs/pytorch/bin/pip install -r requirements.txt && /bin/sh run.sh
```

本地代码目录

工作目录  选择

图 12-32 创建训练作业参数 2

\* 资源池 公共资源池 专属资源池

| 名称  | 状态  | 节点规格                                      | 可用节点/总节点 | 卡数 (可用/总数) |
|-----|-----|-------------------------------------------|----------|------------|
| sa  | 运行中 | GPU: 8*nvidia-v100-nv32   CPU: 72 核 512GB | 3/3      | 16/24      |
| ... |     |                                           |          |            |

\* 规格

\* 计算节点个数

作业优先级 ?

SFS Turbo ?

名称  目录  云上挂载路径  🗑️

增加挂载配置

- 创建方式：选择“自定义算法”。
- 启动方式：选择“自定义”。
- 镜像：选择上传的自定义镜像。
- 启动命令：

```
cd /home/ma-user/work/code/Swin-Transformer && /home/ma-user/anaconda3/envs/pytorch/bin/pip install -r requirements.txt && /bin/sh run.sh
```
- 资源池：在“专属资源池”页签选择GPU规格的专属资源池。
- 规格：选择所需GPU规格。
- 计算节点个数：选择需要的节点个数。
- SFS Turbo：增加挂载配置，选择SFS名称，云上挂载路径为“/home/ma-user/work”。

**说明**

为了和Notebook调试时代码路径一致，保持相同的启动命令，云上挂载路径需要填写为“/home/ma-user/work”。

4. 单击“提交”，在“信息确认”页面，确认训练作业的参数信息，确认无误后单击“确定”。

5. 训练作业创建完成后，后台将自动完成容器镜像下载、代码目录下载、执行启动命令等动作。

训练作业一般需要运行一段时间，根据您的训练业务逻辑和选择的资源不同，训练时长将持续几十分钟到几小时不等。训练作业执行成功后，日志信息如下所示。

## 12.6 FAQ

### 12.6.1 CUDA 和 CUDNN

#### 12.6.1.1 Vnt1 机型软件版本建议

##### gpu driver version : 440.95.01

- gpu driver version : 440.95.01 ( GPU驱动在宿主机中安装，镜像中无需安装 )
- cuda runtime version : 10.2 ( PyTorch自带，无需关心 )
- cudnn version : 7.6.x ( PyTorch自带，无需关心 )
- pytorch version : 1.x.x+cu102

##### gpu driver version : 470.57.02

- gpu driver version : 470.57.02 ( GPU驱动在宿主机中安装，镜像中无需安装 )
- cuda runtime version : 10.2 ( PyTorch自带，无需关心 )
- cudnn version : 7.6 ( PyTorch自带，无需关心 )
- pytorch version : 1.X.X-cu102

##### gpu driver version : 510.65.01

- gpu driver version : 510.65.01
- cuda runtime version : 10.2 ( PyTorch自带，无需关心 )
- cudnn version : 7.6 ( PyTorch自带，无需关心 )
- pytorch version : 1.X.X-cu102

#### 12.6.1.2 CUDA Compatibility 如何使用？

当CUDA 10.2与低版本GPU驱动（440.33以下）配合使用时，可能会出现兼容问题，此时需要使用CUDA Compatibility。在创建训练页面添加以下环境变量：

```
export LD_LIBRARY_PATH=/usr/local/cuda/compat
```

##### 说明

训练时默认不需要加此环节变量，仅当发现驱动版本不够时才使用此方法。

#### 12.6.1.3 专属池驱动版本如何升级？

当专属资源池中的节点含有GPU/Ascend资源时，用户基于自己的业务，可能会有自定义GPU/Ascend驱动的需求，ModelArts面向此类客户提供了自助升级专属资源池GPU/Ascend驱动的能力，具体操作请参见[资源池驱动升级](#)。

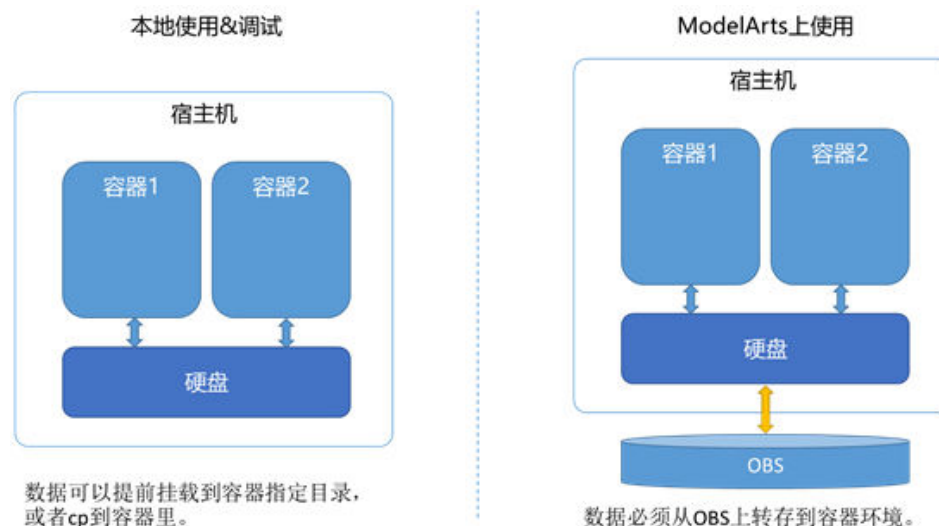
## 12.6.2 CloudShell 调试方法

当使用专属资源池时，允许用户使用ModelArts控制台提供的CloudShell登录运行中的训练容器。CloudShell调试方法请参见[CloudShell使用指导](#)。

## 12.6.3 run.sh 脚本测试 ModelArts 训练整体流程

自定义容器在ModelArts上训练和本地训练的区别如下图：

图 12-33 本地与 ModelArts 上训练对比



ModelArts上进行训练比本地训练多了一步OBS和容器环境的数据迁移工作。

增加了和OBS交互工作的整个训练流程如下：

### 📖 说明

建议使用OBSutil作为和OBS交互的工具，如何在本机安装obsutil可以参考[obsutil安装和配置](#)。

1. 训练数据、代码、模型下载。（本地使用硬盘挂载或者docker cp，在ModelArts上使用OBSutil）
2. 启动脚本。（用法无切换，一般就是到达执行目录，然后python xxx.py）
3. 训练结果、日志、checkpoints上传。（本地使用硬盘挂载或者docker cp，在ModelArts上使用OBSutil）

可以用一个run脚本把整个流程包起来。run.sh脚本的内容可以参考如下示例：

```
#!/bin/bash

##认证用的AK和SK硬编码到代码中或者明文存储都有很大的安全风险，建议在配置文件或者环境变量中密文存放，使用时解密，确保安全。
##本示例以AK和SK保存在环境变量中来实现身份验证为例，运行本示例前请先在本地环境中设置环境变量HUAWEICLOUD_SDK_AK和HUAWEICLOUD_SDK_SK。

##安装obsutil，完成AKSK配置。建议在基础镜像里做好。
#mkdir -p /opt && cd /opt
#wget https://obs-community.obs.cn-north-1.myhuaweicloud.com/obsutil/current/obsutil_linux_amd64.tar.gz
#tar -xzf obsutil_linux_amd64.tar.gz && mv obsutil_linux_amd64_*/ utils
#alias obsutil='/opt/utils/obsutil'
#obsutil config -i=${HUAWEICLOUD_SDK_AK} -k=${HUAWEICLOUD_SDK_SK} -e=obs.cn-north-4.myhuaweicloud.com
```



```
##训练输入复制到容器镜像本地。
#/cache目录的容量较大。

DATA_URL=`echo ${DLS_DATA_URL} | sed /s/s3/obs/`
mkdir -p /cache/data
/opt/utils/obsutil cp -r -f ${DATA_URL} /cache/data

##执行训练任务。
#涉及conda env切换时。
source /xxxx/etc/profile.d/conda.sh
conda activate xxxenv
conda info --envs
#启动训练脚本。
cd xxxx
python xxx.py

##复制输出结果到OBS目录。
TRAIN_URL=`echo ${DLS_TRAIN_URL} | sed /s/s3/obs/`
/opt/utils/obsutil cp -r -f /cache/out ${TRAIN_URL}
```

把run.sh放到/opt目录，在实际启动任务的时候，使用以下命令启动任务即可：

```
bash -x /opt/run.sh
```

把run.sh放到/root目录，可以在原镜像里增加一层，这一层就只是COPY这个run脚本。在基础镜像里可以一起把obsutil安装、配置好。参考如下dockerfile：

```
FROM $your_docker_image_tag

RUN mkdir -p /opt && cd /opt && \
 wget https://obs-community.obs.cn-north-1.myhuaweicloud.com/obsutil/current/obsutil_linux_amd64.tar.gz && \
 tar -xzf obsutil_linux_amd64.tar.gz && mv obsutil_linux_amd64 */utils && \
 /opt/utils/obsutil config -i=${HUAWEICLOUD_SDK_AK} -k=${HUAWEICLOUD_SDK_SK} -e=obs.cn-north-4.myhuaweicloud.com

COPY run.sh /opt/run.sh
```

### 须知

ModelArts的容器会有一个/cache目录，这个目录挂载的硬盘容量最大。建议下载数据和中间数据都存到这个目录中，防止因硬盘占满导致任务失败。

## 12.6.4 ModelArts 环境挂载目录说明

本小节介绍Notebook开发环境、训练任务实例的目录挂载情况（以下挂载点在保存镜像的时候不会保存）。详情如下：

### Notebook

表 12-8 Notebook 挂载点介绍

| 挂载点                 | 是否只读 | 备注          |
|---------------------|------|-------------|
| /home/ma-user/work/ | 否    | 客户数据的持久化目录。 |
| /data               | 否    | 客户PFS的挂载目录。 |



| 挂载点                                                  | 是否只读 | 备注                      |
|------------------------------------------------------|------|-------------------------|
| /cache                                               | 否    | 裸机规格时支持，用于挂载宿主机NVMe的硬盘。 |
| /train-worker1-log                                   | 否    | 兼容训练任务调试过程。             |
| /dev/shm                                             | 否    | 用于PyTorch引擎加速。          |
| /modelarts                                           | 是    | /                       |
| /etc/secret-volume                                   | 是    | /                       |
| /etc/sudoers                                         | 是    | /                       |
| /etc/localtime                                       | 是    | /                       |
| var/run/secrets/<br>kubernetes.io/<br>serviceaccount | 是    | /                       |

## 训练任务

表 12-9 训练任务挂载点介绍

| 挂载点                         | 是否只读 | 备注                        |
|-----------------------------|------|---------------------------|
| /xxx                        | 否    | 专属池使用SFS盘挂载的目录，路由由客户自己指定。 |
| /home/ma-user/<br>modelarts | 否    | 空文件夹，建议用户主要用这个目录。         |
| /cache                      | 否    | 裸机规格支持，挂载宿主机NVMe的硬盘。      |
| /dev/shm                    | 否    | 用于PyTorch引擎加速。            |
| /usr/local/nvidia           | 是    | 宿主机的nvidia库。              |

### 12.6.5 如何查看训练环境变量

在创建训练作业时，“启动命令”输入为“env”，其他参数保持不变。

当训练任务执行完成后，在训练作业详情页面中查看“日志”。日志中即为所有的环境变量信息。

图 12-34 查看日志

```
1 NV_LIBCUBLAS_DEV_VERSION=11.3.1.68-1
2 NV_CUDA_COMPAT_PACKAGE=cuda-compat-11-2
3 NV_CUDNN_PACKAGE_DEV=libcudnn8-dev=8.1.1.33-1+cuda11.2
4 LD_LIBRARY_PATH=/usr/local/nccl/lib:/usr/local/nccl/lib64
5 NV_LIBNCCL_DEV_PACKAGE=libnccl-dev=2.8.4-1+cuda11.2
6 MA_ENGINE_VERSION=
7 MA_NUM_HOSTS=1
8 VC_WORKER_HOSTS=modelarts-job-5f8e4b52-630b-4c15-9bb6-c3f68a48ac47-worker-0.modelarts-job-5f8e4b52-630b-4c15-9bb6-c3f68a48ac47
9 VK_TASK_INDEX=0
10 _=/usr/bin/env
11 MA_SCRIPT_INTERPRETER=
12 NV_LIBNPP_DEV_PACKAGE=libnpp-dev-11-2=11.2.1.68-1
13 MA_MAX_BACKOFF=0
14 HOSTNAME=modelarts-job-5f8e4b52-630b-4c15-9bb6-c3f68a48ac47-worker-0
15 MA_IAM_USER_ID=79098163dd814fd986eca7ef0325d086
16 MA_CURRENT_IP=10.0.0.62
17 NV_LIBNVP_DEV_PACKAGE=11.2.1.68-1
18 NV_NVPROF_DEV_PACKAGE=cuda-nvprof-11-2=11.2.67-1
19 MA_MOUNT_PATH=/home/ma-user/modelarts
20 NVIDIA_VISIBLE_DEVICES=all
21 MA_ENGINE_TYPE=
22 NV_NVPROF_VERSION=11.2.67-1
23 NV_LIBCUSPARSE_VERSION=11.3.1.68-1
24 MODELARTS_SCC_SERVICE_PORT=60687
25 MA_HOME=/home/ma-user
26 KUBERNETES_PORT_443_TCP_PROTO=tcp
27 KUBERNETES_PORT_443_TCP_ADDR=10.247.0.1
28 NV_LIBCUBLAS_DEV_PACKAGE=libcublas-dev-11-2=11.3.1.68-1
29 MA_VJ_NAME=modelarts-job-5f8e4b52-630b-4c15-9bb6-c3f68a48ac47
30 MA_PIP_URL=http://repo.myhuaweicloud.com/repository/pypi/simple/
31 NCCL_VERSION=2.8.4-1
32 KUBERNETES_PORT=tcp://10.247.0.1:443
33 PWD=/
34 NVARCH=x86_64
35 HOME=/home/ma-user
```

## 12.6.6 infiniband 驱动的安装

### infiniband 驱动的安装

如果安装了 libibverbs-dev 库后仍然无法使能 infiniband 网卡，您可以直接安装 infiniband 官方驱动，以使用 infiniband 网卡进行分布式通信，提升训练性能。infiniband 驱动需要在制作镜像时安装。

### 操作步骤

1. 下载 MLNX\_OFED\_LINUX-4.3-1.0.1.0-ubuntu16.04-x86\_64.tgz。

进入[地址](#)，单击“Download”，选择“Archive Versions”，“Version”选择“4.3-1.0.1.0”，“OS Distribution”选择“Ubuntu”，“OS Distribution Version”选择“Ubuntu 16.04”，“Architecture”选择“x86\_64”，下载 MLNX\_OFED\_LINUX-4.3-1.0.1.0-ubuntu16.04-x86\_64.tgz。

#### 说明

宿主机安装的 infiniband 驱动版本为 4.3-1.0.1.0，容器镜像中安装的 infiniband 驱动版本需要与宿主机版本匹配，即同为 4.3-1.0.1.0。

可能部分区域的网卡较新，会出现更高版本的 infiniband 驱动版本，如果您遇到了 infiniband 驱动安装后，仍然无法使能 infiniband 网卡的问题，可以咨询相关运维人员以确认宿主机的实际 infiniband 驱动版本。

图 12-35 下载驱动

| Version (Archive) | OS Distribution | OS Distribution Version | Architecture | Download/Documentation                                                                                              |
|-------------------|-----------------|-------------------------|--------------|---------------------------------------------------------------------------------------------------------------------|
| 4.5-1.0.1.0       | Wind River      | Ubuntu 18.04            | x86_64       | ISO: <a href="#">MLNX_OFED_LINUX-4.3-1.0.1.0-ubuntu16.04-x86_64.iso</a><br>MD5SUM: cf3727ff01a5e8543e65880585ae2edc |
| 4.4-2.0.7.0.3     | Ubuntu          | Ubuntu 17.10            | ppc64le      |                                                                                                                     |
| 4.4-2.0.7.0       | SLES            | Ubuntu 16.04            |              | Size: 157M                                                                                                          |
| 4.4-1.0.0.0       | RHEL/CentOS     |                         |              |                                                                                                                     |
| 4.4-1.0.0.0       | OL              |                         |              |                                                                                                                     |
| 4.3-3.0.2.1       | Fedora          |                         |              | tgz: <a href="#">MLNX_OFED_LINUX-4.3-1.0.1.0-ubuntu16.04-x86_64.tgz</a><br>MD5SUM: 13aa7d177b6a2b15a321d61da9e5754d |
| 4.3-1.0.1.0       | EulerOS         |                         |              | Size: 156M                                                                                                          |
| 4.2-1.2.0.0       | Debian          |                         |              | SOURCES: <a href="#">MLNX_OFED_SRC-debian-4.3-1.0.1.0.tgz</a><br>MD5SUM: c1b13ce821804ca4a16816ec96b7063f           |
| 4.2-1.0.0.0       |                 |                         |              |                                                                                                                     |
| 4.1-1.0.2.0       |                 |                         |              |                                                                                                                     |
| 4.1-0.0.0.5       |                 |                         |              |                                                                                                                     |

2. 参考如下Dockerfile中，以在容器镜像中安装infiniband驱动。

```
USER root

copy MLNX_OFED_LINUX-4.3-1.0.1.0-ubuntu16.04-x86_64.tgz to docker image

RUN tar xzvf MLNX_OFED_LINUX-4.3-1.0.1.0-ubuntu16.04-x86_64.tgz && \
 cd MLNX_OFED_LINUX-4.3-1.0.1.0-ubuntu16.04-x86_64 && \
 chmod +x mlnxofedinstall && \
 ./mlnxofedinstall --user-space-only --without-fw-update --force && \
 cd - && \
 rm MLNX_OFED_LINUX-4.3-1.0.1.0-ubuntu16.04-x86_64.tgz && \
 rm -rf MLNX_OFED_LINUX-4.3-1.0.1.0-ubuntu16.04-x86_64

USER ma-user
```

3. 验证infiniband驱动是否安装成功。

在训练代码中执行以下命令，如果无报错则infiniband驱动安装成功：

```
os.system("ofed_info")
```

## 12.6.7 Tensorboard 的使用

ModelArts支持在开发环境中开启TensorBoard可视化工具。TensorBoard是TensorFlow的可视化工具包，提供机器学习实验所需的可视化功能和工具。

TensorBoard能够有效地展示TensorFlow在运行过程中的计算图、各种指标随着时间的变化趋势以及训练中使用到的数据信息。

### 前提条件

为了保证训练结果中输出Summary文件，在编写训练脚本时，您需要在脚本中添加收集Summary相关代码。

TensorFlow引擎的训练脚本中添加Summary代码，具体方式请参见[TensorFlow官方网站](#)。

### 注意事项

- 运行中的可视化作业不单独计费，当停止Notebook实例时，计费停止。
- Summary文件数据如果存放在OBS中，由OBS单独收费。任务完成后请及时停止Notebook实例，清理OBS数据，避免产生不必要的费用。

## 在开发环境中创建 TensorBoard 可视化作业流程

### Step1 创建开发环境并在线打开

### Step2 上传Summary数据

### Step3 启动TensorBoard

### Step4 查看训练看板中的可视化数据

## Step1 创建开发环境并在线打开

在ModelArts控制台，进入“开发环境 > Notebook”页面，创建TensorFlow或者PyTorch镜像的开发环境实例。创建成功后，单击开发环境实例操作栏右侧的“打开”，在线打开运行中的开发环境。

TensorBoard可视化训练作业，当前仅支持基于TensorFlow2.1、Pytorch1.4/1.8以上版本镜像，CPU/GPU规格的资源类型。请根据实际局点支持的镜像和资源规格选择使用。

## Step2 上传 Summary 数据

在开发环境中使用TensorBoard可视化功能，需要用到Summary数据。

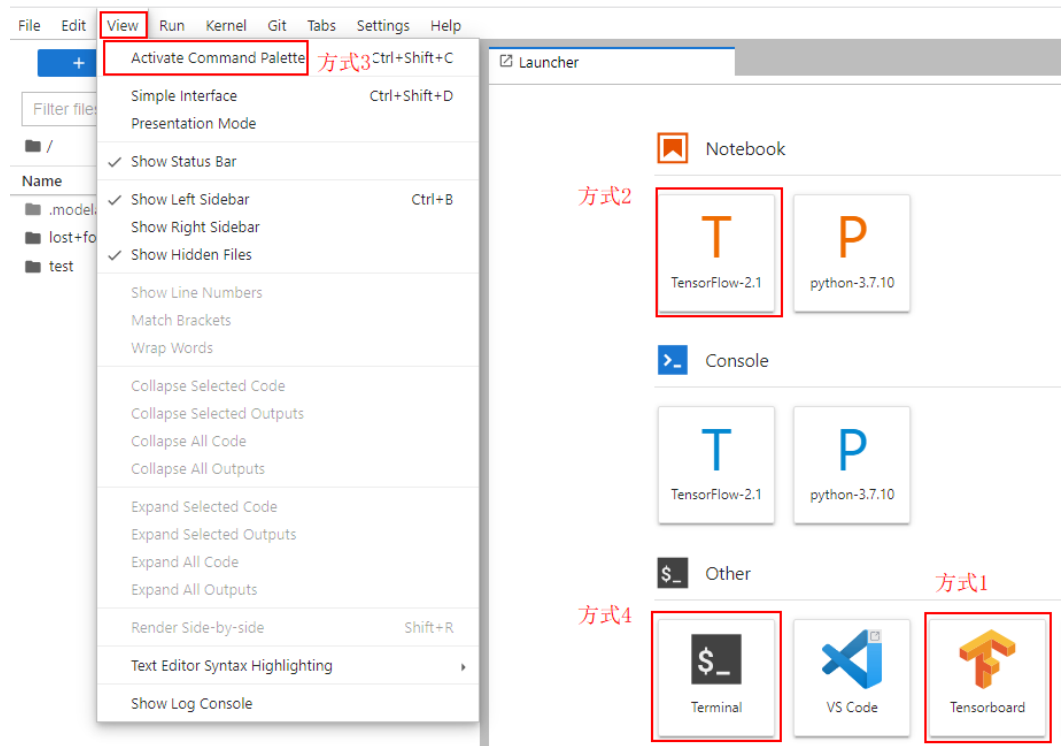
Summary数据可以直接传到开发环境的这个路径下/home/ma-user/work/，也可以放到OBS并行文件系统中。

- Summary数据上传到Notebook路径/home/ma-user/work/下的方式，请参见[上传数据至Notebook](#)。
- Summary数据如果是通过OBS并行文件系统挂载到Notebook中，请将模型训练时产生的Summary文件先上传到OBS并行文件系统，并确保OBS并行文件系统与ModelArts在同一区域。在Notebook中启动TensorBoard时，Notebook会自动从挂载的OBS并行文件系统目录中读取Summary数据。

## Step3 启动 TensorBoard

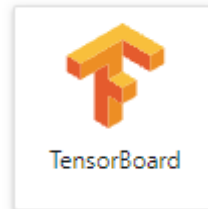
在开发环境的JupyterLab中打开TensorBoard有多种方法。可根据使用习惯选择。

图 12-36 JupyterLab 中打开 TensorBoard 的方法



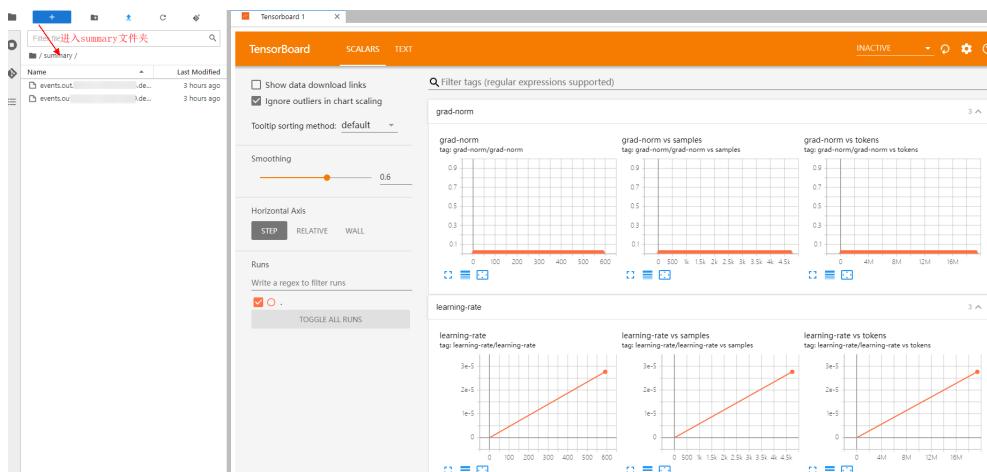
**方式1（推荐）：**

1. 在JupyterLab左侧导航创建名为“summary”的文件夹，将数据上传到“/home/ma-user/work/summary”路径。注：文件夹命名只能为summary否则无法使用。



2. 进入“summary”文件夹，单击方式1，直接进入TensorBoard可视化界面。如图12-37所示。

图 12-37 TensorBoard 界面 (1)



方式2:

须知

用户可以自行升级除2.4.0之外的TensorBoard，但需注意升级后只有方式2使用新的TensorBoard，其余方式保持TensorBoard2.1.1不变。



1. 单击方式2，进入JupyterLab开发环境中，并自动创建“.ipynb”文件。
2. 在对话框中输入TensorBoard相应命令，即可展示界面。

```
%reload_ext ma_tensorboard
%ma_tensorboard --port {PORT} --logdir {BASE_DIR}
```

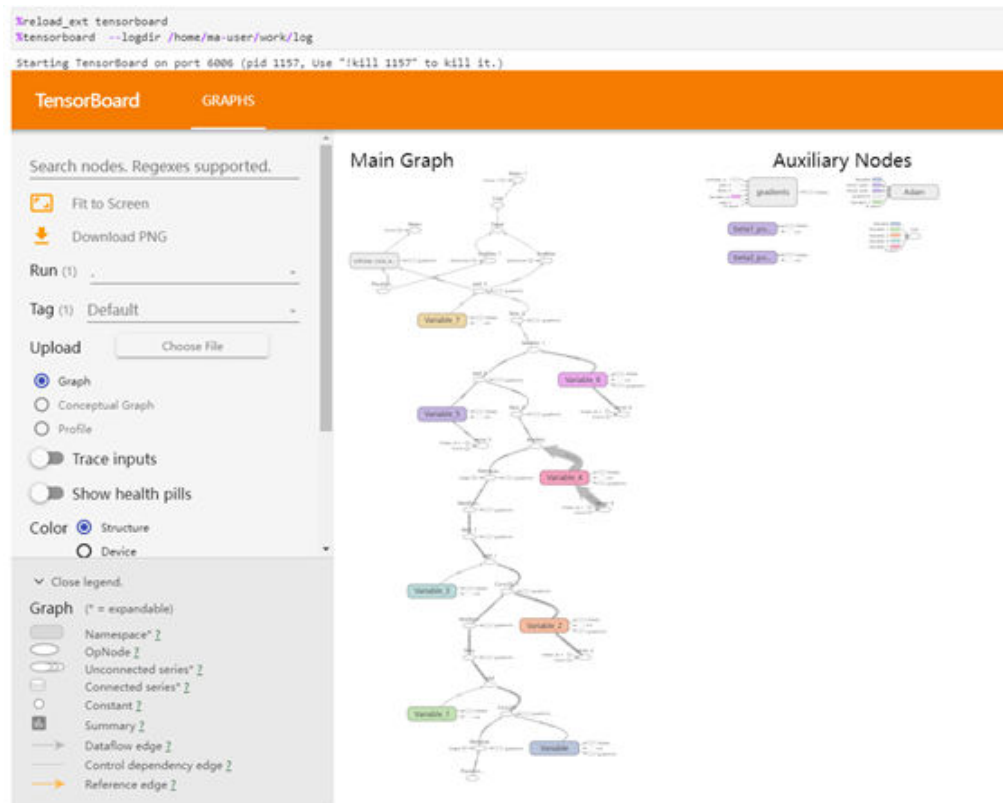
参数解释:

- --port {PORT}: 指定Web可视化服务端口。可以不设置，默认使用8080端口。如果8080端口被占用了，需要在1~65535任意指定一个端口。
- --logdir {BASE\_DIR}: 表示数据在开发环境中的存储路径
  - 开发环境本地路径：“./work/xxx”（相对路径）或/home/ma-user/work/xxx（绝对路径）
  - OBS并行文件系统的路径：obs://xxx/

例如:

```
#Summary数据如果是在开发环境的这个路径下/home/ma-user/work/，执行下面这条命令。
%ma_tensorboard --port {PORT} --logdir /home/ma-user/work/xxx
或者
#Summary数据如果是存在OBS并行文件系统中，执行下面这条命令，开发环境会自动挂载该OBS并行文件系统路径并读取数据。
%ma_tensorboard --port {PORT} --logdir obs://xxx/
```

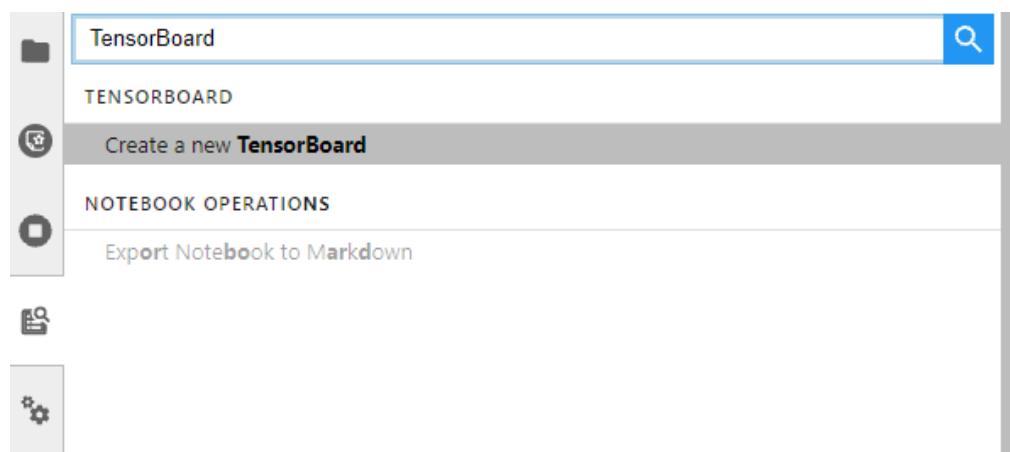
图 12-38 TensorBoard 界面 (2)



方式3:

1. 单击方式3 View -> Activate Command Palette, 在搜索框中输入“TensorBoard”, 再单击“Create a new TensorBoard”。

图 12-39 Create a new TensorBoard



2. 填写需要查看的Summary数据路径, 或者OBS并行文件系统桶的路径。
  - 开发环境本地路径: ./summary (相对路径) 或/home/ma-user/work/summary (绝对路径)
  - OBS并行文件系统桶的路径: obs://xxx/

图 12-40 输入 Summary 数据路径

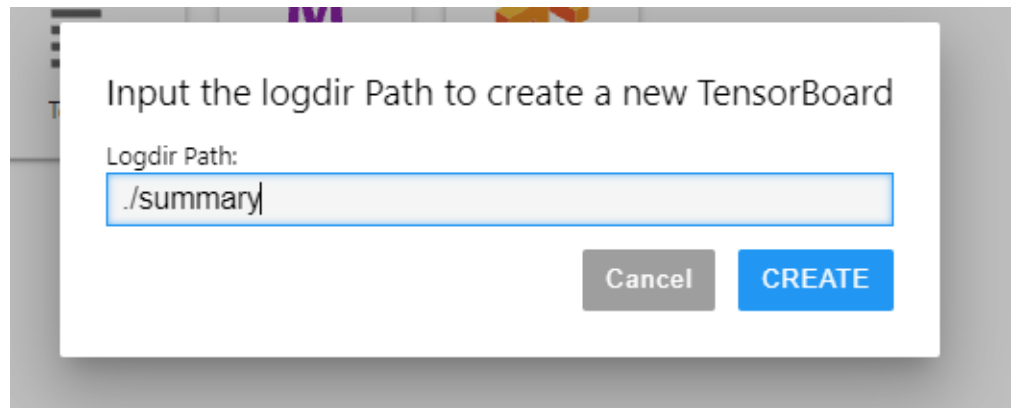
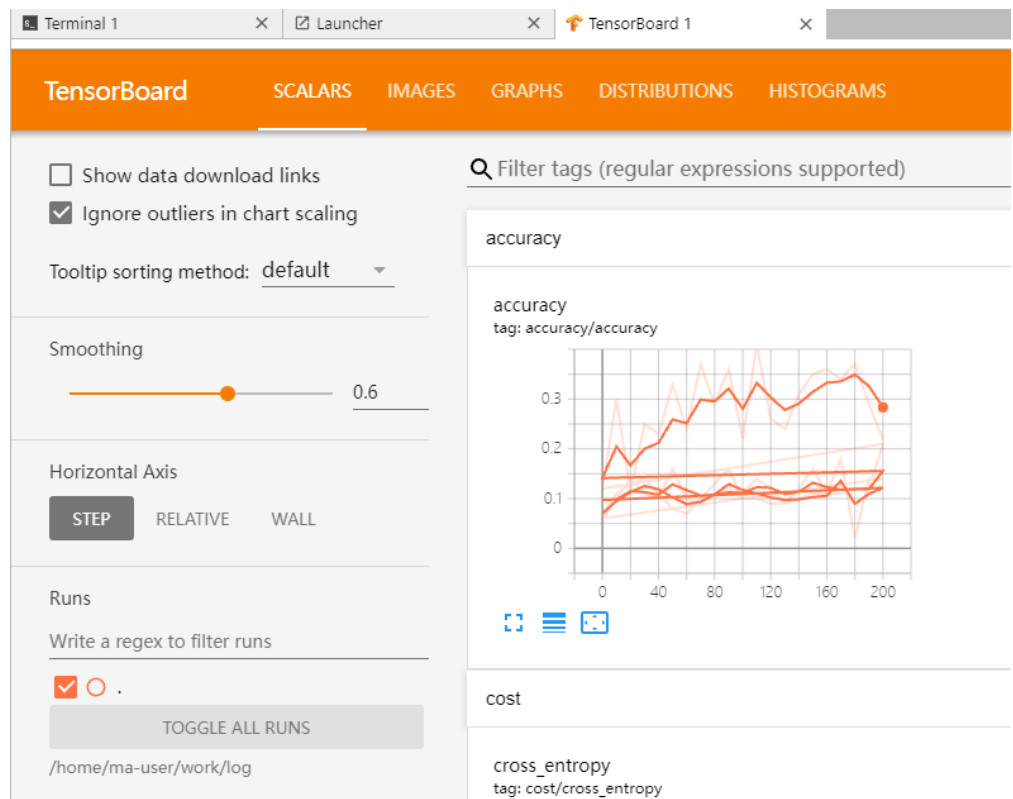


图 12-41 TensorBoard 界面 (3)



方式4:



单击方式4 **Terminal** ，输入命令执行，但启动后不能显示UI界面。

```
tensorboard --logdir ./log
```



图 12-42 Terminal 方式打开 TensorBoard

```
sh-4.4#pwd
/home/sawuser
sh-4.4#tensorboard --logdir ./log
2021-10-18 20:34:53.586976: I tensorflow/stream_executor/platform/default/dso_loader.cc:44] Successfully opened dynamic library libwinfer.so.6
2021-10-18 20:34:53.589272: I tensorflow/stream_executor/platform/default/dso_loader.cc:44] Successfully opened dynamic library libwinfer_plugin.so.6
Serving TensorBoard on localhost; to expose to the network, use a proxy or pass --bind_all
TensorBoard 2.1.1 at http://localhost:6006/ (Press CTRL+C to quit)
```

### Step4 查看训练看板中的可视化数据

训练看板是TensorBoard的可视化组件的重要组成部分，而训练看板的标签包含：标量可视化、图像可视化和计算图可视化等。

更多功能介绍请参见[TensorBoard官网资料](#)。

### 相关操作

关闭TensorBoard方式如下：


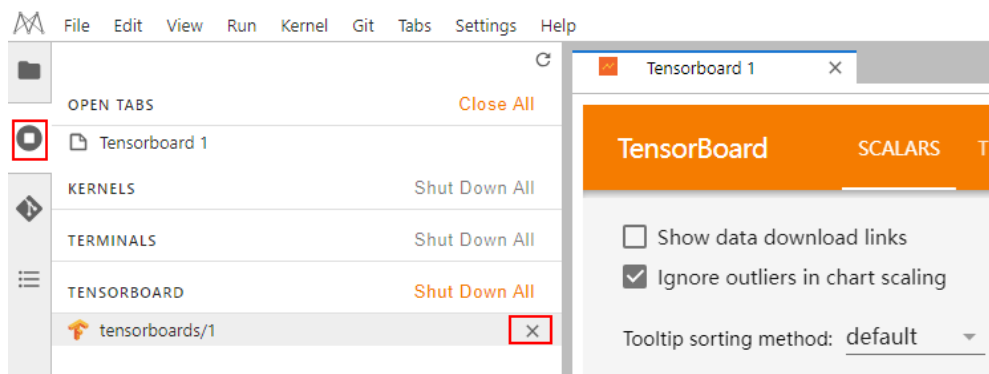
- 方式1：单击下图所示的，进入TensorBoard实例管理界面，该界面记录了所有启动的TensorBoard实例，单击对应实例后面的SHUT DOWN即可停止该实例。

图 12-43 单击 SHUT DOWN 停该实例



- 方式2：在开发环境JupyterLab中的“.ipynb”文件窗口中输入命令，关闭TensorBoard。PID在启动界面有提示或者通过ps -ef | grep tensorboard查看。  
!kill PID


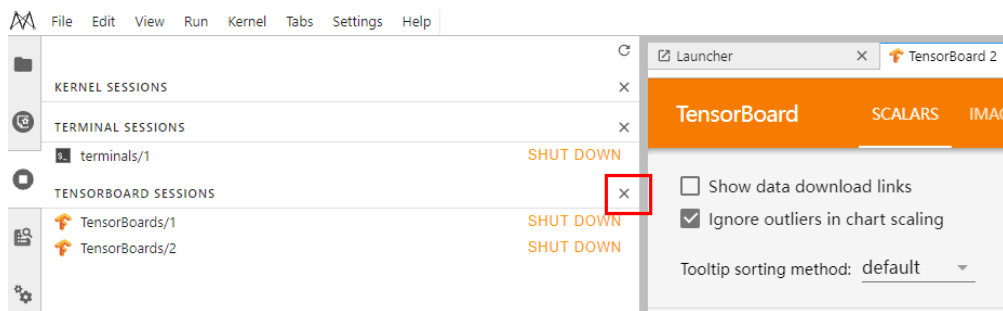
- 方式3：单击下方红框中的按钮可以关闭所有启动的TensorBoard实例。

图 12-44 关闭所有启动的 TensorBoard 实例



- 方式4（不推荐）：直接在JupyterLab中上关闭TensorBoard窗口，此方式仅关闭可视化窗口，并未关闭后台。

## 12.6.8 如何保证训练和调试时文件路径保持一致

### 云上挂载路径

Notebook中挂载SFS后，SFS默认在“/home/ma-user/work”路径下。在创建训练作业时，设置SFS Turbo的“云上挂载路径”为“/home/ma-user/work”，使得训练环境下SFS也在“/home/ma-user/work”路径下。

### ln -s 建立软连接

如果代码中涉及文件绝对路径，由于Notebook调试与训练作业环境不同，可能会导致文件绝对路径不一致，需要修改代码内容。推荐使用软链接的方式解决这个问题，用户只需提前建立好软链接，代码中的地址可保持不变。

新建软链接：

```
ln -s 源目录/文件 目标目录/文件
例如
ln -s /mnt/sfs_turbo/data/coco /coco
```

删除软链接：

```
rm 目标目录/文件
rm /coco
```

# 13 ModelArts+HiLens

## 13.1 手势识别技能开发（ModelArts+华为 HiLens）

ModelArts是面向AI开发者的一站式开发平台，您可以使用ModelArts开发一个用于华为HiLens平台的算法模型，然后基于您自定义的算法模型和逻辑代码新建技能。

本章节提供了一个手势识别技能的样例，介绍从模型训练到查看技能效果，新建一个全新技能的全流程，帮助您快速熟悉华为HiLens技能开发的使用过程。

开始使用样例前，请仔细阅读[准备工作](#)罗列的要求，提前完成准备工作。具体技能开发的步骤如下所示：

1. [准备训练数据](#)
2. [订阅算法](#)
3. [使用订阅算法创建训练作业](#)
4. [转换模型](#)
5. [导入模型至华为HiLens](#)
6. [新建技能](#)
7. [（可选）发布技能](#)
8. [安装技能](#)
9. [启动技能](#)

### 准备工作

- 已注册华为账号并开通华为云，且在使用华为HiLens前检查账号状态，账号不能处于欠费或冻结状态。
- 已购买HiLens Kit设备，并准备好网线，电脑，路由器，HDMI线，显示屏。
- 成功注册设备HiLens Kit设备至华为HiLens控制台，详情请参见[注册HiLens Kit](#)。
- 登录OBS服务，创建桶和文件夹，用于存放样例的训练数据。创建名称为“hilens-gesture” OBS桶，区域选择“华北-北京四”，创建如下文件夹：
  - “gesture-data”：用于存放训练模型的数据。
  - “gesture-data-output”：用于存放模型输出数据。
  - “gesture-data-record”：用于存放日志。

- “gesture-convert-output”：用于存放转换模型后的输出文件。

创建OBS桶和文件夹的操作指导请参见[创建桶](#)和[新建文件夹](#)。为保证模型数据能正常访问，请务必保证创建的OBS桶与华为HiLens在同一区域。

占用OBS资源的操作均会收取一定费用，收费规则请参见[对象存储服务 OBS](#)。

## 准备训练数据

华为HiLens在公共OBS桶中提供了手势识别技能的用于模型训练的示例数据，命名为“gesture\_recognition\_data”，因此本文的操作示例使用此示例模型进行技能开发。您需要执行如下操作，将模型文件上传至您的OBS目录下，即准备工作中您创建的OBS目录“hilens-gesture/gesture-recognition”。

- 步骤1** 单击[示例数据下载链接](#)，将手势识别案例示例数据“gesture\_recognition\_data”下载至本地。
- 步骤2** 在本地，将“gesture\_recognition\_data”压缩包解压。例如解压至本地“gesture\_recognition\_data”文件夹下，包括1个子文件夹“gesture-data”和1个“.py”文件。
- 步骤3** 参考[上传文件](#)，利用OBS Browser+工具将“gesture\_recognition\_data/gesture-data”文件夹下的所有数据上传至“hilens-gesture/gesture-data” OBS路径下，OBS Browser+使用方法请参见[OBS Browser+工具指南](#)。

----结束

## 订阅算法

ModelArts提供了一个“ResNet\_v1\_50”，算法用途为图像分类，您可以使用此算法训练，得到所需的模型。目前“resnet\_v1\_50”算法发布在AI Gallery中。您可以前往AI Gallery，订阅此算法，然后同步至ModelArts中。

- 步骤1** 登录ModelArts管理控制台，在左侧菜单栏中选择“AI Gallery”。进入新版AI Gallery。
- 步骤2** 单击[图像分类-ResNet\\_v1\\_50](#)，进入算法详情页。

由于AI Gallery发布了多个“ResNet\_v1\_50”，本示例选择支持GPU训练+Snt3推理的算法。

图 13-1 选择仅用于 Snt3 推理的算法



- 步骤3** 单击右侧的“订阅”，根据界面提示完成算法订阅。  
订阅算法完成后，页面的“订阅”按钮显示为“已订阅”。
- 步骤4** 单击详情页的“前往控制台”，此时弹出“选择云服务区域”对话框，选择ModelArts对应的区域，然后再单击“确定”。

页面将自动跳转至ModelArts的“算法管理>我的订阅”中同步对应的算法。

图 13-2 前往控制台

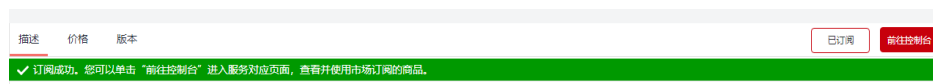
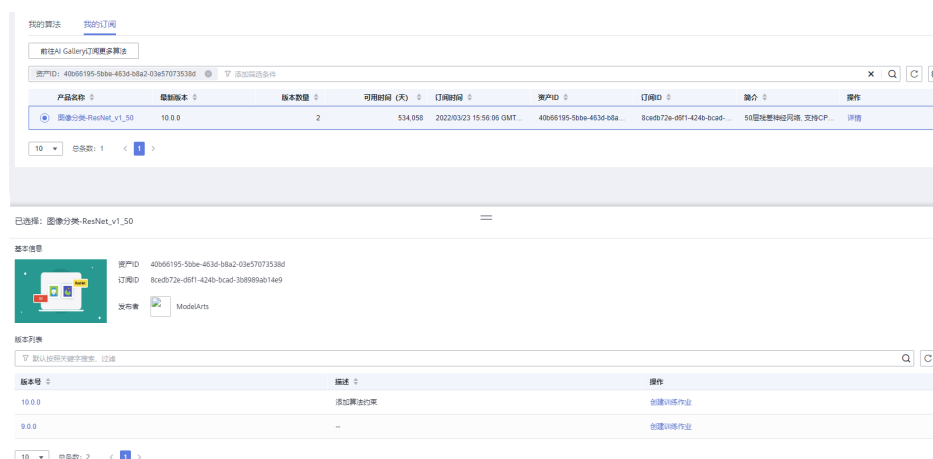


图 13-3 选择云服务区域



步骤5 在ModelArts管理控制台的算法管理页面，算法将自动同步至ModelArts中。

图 13-4 同步算法



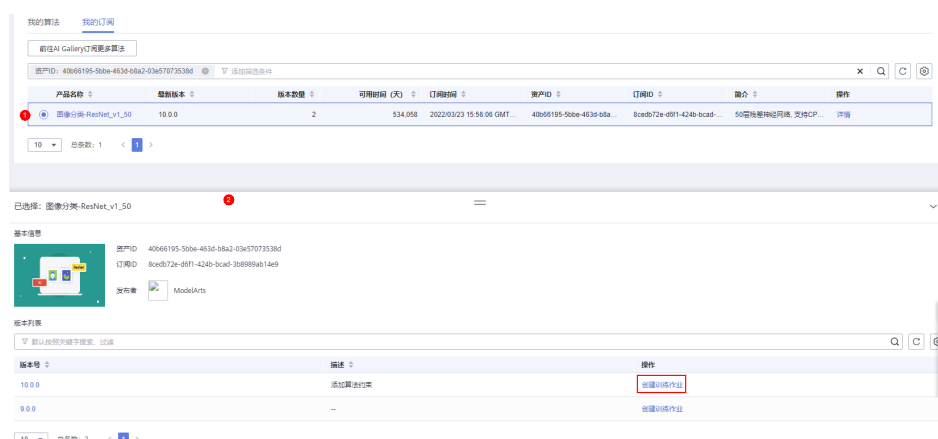
----结束

## 使用订阅算法创建训练作业

算法订阅成功后，算法将呈现在“算法管理>我的订阅”中，您可以使用订阅的“ResNet\_v1\_50”算法创建训练作业，获得模型。

步骤1 进入“算法管理>我的订阅”页面，选择订阅的“ResNet\_v1\_50”算法，单击左侧的单选按钮在列表页底部展开算法详情，在版本列表中，单击“创建训练作业”。

图 13-5 创建训练作业



**步骤2** 在“创建训练作业”页面，参考如下说明填写关键参数。

- “算法> 我的订阅”：系统默认选择订阅的算法，请勿随意修改。
- “训练输入”：选择数据存储位置，然后从弹出的窗口中选择[准备训练数据](#)中已上传训练模型数据的“hilens-gesture/gesture-data”OBS路径。
- “训练输出”：选择训练结果的存储位置（OBS路径）。为避免出现错误，建议选择选择一个空目录用作“训练输出”。本样例选择[准备工作](#)中已创建的OBS桶“hilens-gesture”和文件夹“gesture-data-output”。
- “超参”：建议采用默认值。如需进行调优，可参考[算法详情页](#)的训练参数说明。
- “资源类型”：建议选择GPU规格的资源类型，训练效率会更高一些。

**步骤3** 参数填写完成后，单击“提交”，确认规格，单击“确定”，完成训练作业创建。

**步骤4** 进入“训练管理>训练作业”页面，等待训练作业完成。

训练作业运行需要几分钟时间，请耐心等待。根据经验，选择样例数据集，使用GPU资源运行，预计3分钟左右可完成。

当训练作业的状态变更为“已完成”时，表示已运行结束。

图 13-6 查看训练作业状态



您可以单击训练作业名称，进入详情页面，了解训练作业的“配置信息”、“日志”、“资源占用情况”和“评估结果”等信息。

您也可以在配置的“训练输出位置”对应的OBS目录下获得训练生成的模型。

----结束

## 转换模型

- 步骤1** 在ModelArts管理控制台，选择左侧导航栏的“AI应用管理 > 模型转换”，进入模型转换列表页面。
- 步骤2** 单击左上角的“创建任务”，进入创建任务页面。
- 步骤3** 在“创建任务”页面，按表13-1填写相关信息，如图13-7所示。

表 13-1 创建任务参数

| 参数       | 推荐填写                                                        |
|----------|-------------------------------------------------------------|
| “名称”     | 输入“gesture-recognition”。                                    |
| “描述”     | 输入判断手势技能的简短描述，如：将判断手势技能模型转换为“.om”格式。                        |
| “输入框架”   | 选择“TensorFlow”。                                             |
| “转换输入目录” | 选择转换输入目录为“hilens-gesture/gesture-data-output/frozen_graph”。 |
| “输出框架”   | 选择“MindSpore”。                                              |
| “转换输出目录” | 选择转换输出目录为“hilens-gesture/gesture-convert-output”。           |
| “转换模板”   | 选择“TF-FrozenGraph-To-Ascend-HiLens”。                        |
| “高级选项”   | “输入张量形状”设置为“images:1,224,224,3”，其他选项均为默认值。                  |

图 13-7 创建模型转换任务

The screenshot shows the 'Create Task' form in the ModelArts console. The form is filled with the following information:

- Name:** gesture-recognition
- Description:** (Empty text area)
- Input Framework:** TensorFlow
- Conversion Input Directory:** /modelarts-hilens/gesture/dataset-output0623/frozen\_graph/
- Output Framework:** MindSpore
- Conversion Output Directory:** /modelarts-hilens/gesture/convert-output/
- Conversion Template:** TF-FrozenGraph-To-Ascend-HiLens
- Input Tensor Shape:** images:1,224,224,3
- Input Data Format:** NHWC
- Conversion Output Node:** (Empty text field)
- Preferred Data Format:** 5D
- Generation Precision Model:** 0
- Network Output Data Type:** FP32

- 步骤4** 任务信息填写完成后，单击右下角“立即创建”。

创建完成后，系统自动跳转至“模型转换”中。刚创建的转换任务将呈现在界面中，其“任务状态”为“初始化”。任务执行过程预计需要几分钟到十几分钟不等，请耐心等待，当“任务状态”变为“成功”时，表示任务运行完成并且模型转换成功。

如果“任务状态”变为“失败”，建议单击任务名称进入详情页面，查看日志信息，根据日志信息调整任务的相关参数并创建新的转换任务。

----结束

## 导入模型至华为 HiLens

**步骤1** 登录[华为HiLens管理控制台](#)，在左侧导航栏中选择“基础版>技能开发>模型管理”，进入“模型管理”页面。

### 📖 说明

华为HiLens控制台技能开发所在的区域应和在ModelArts AI Gallery订阅算法的区域[图13-2](#)一致。

**步骤2** 在“模型管理”页面，单击右上角的“导入（转换）模型”。

**步骤3** 在“导入模型”页面，然后参考[表13-2](#)填写参数，信息确认无误后单击“确定”完成导入，如[图13-8](#)所示。

表 13-2 导入模型参数

| 参数     | 推荐填写                                                                                                        |
|--------|-------------------------------------------------------------------------------------------------------------|
| “名称”   | 输入“gesture-recognition”。                                                                                    |
| “版本”   | 输入“1.0.0”。                                                                                                  |
| “描述”   | 输入导入模型的描述。                                                                                                  |
| “模型来源” | 单击“从ModelArts导入”，在右侧下拉框中选择“OM（从转换任务中获取）”，然后在下方转换任务列表中勾选之前在 <a href="#">转换模型</a> 转换的模型“gesture-recognition”。 |

图 13-8 导入模型

The screenshot shows a form for importing a model. It includes the following fields and options:

- 名称**: Input field containing "gesture-recognition".
- 版本**: Input field containing "1.0.0".
- 描述**: Text area containing "摄像头将能识别近距离的基本手势, 包括点赞 (Great)、OK、胜利 (Yeah)、摇滚 (Rock) 等手势." with a character count of 52/100.
- 模型来源**: A dropdown menu with three options: "从OBS导入", "从ModelArts导入" (highlighted in blue), and "OM (从转换任务中获取)".

模型导入后，将进入“模型管理”页面，您导入的模型可从列表中查看模型状态，导入成功后模型“状态”为“导入成功”。

----结束



## 新建技能

- 步骤1** 在华为HiLens管理控制台的左侧导航栏中选择“技能开发>技能管理”，进入技能列表。
- 步骤2** 在“技能管理”页面，单击右上角“新建技能”，进入“创建技能”页面。
- 步骤3** 在“创建技能”页面，在“技能模板”中选择“使用空模板”后，填写基本信息和技能内容。

### 基本信息

按表13-3填写技能的基本信息，如图13-9所示。

表 13-3 技能基本信息参数

| 参数     | 推荐填写                                                                                                          |
|--------|---------------------------------------------------------------------------------------------------------------|
| “技能模板” | 选择“使用空模板”。                                                                                                    |
| “技能名称” | 输入“Gesture_Recognition”。                                                                                      |
| “技能版本” | 输入“1.0.0”。                                                                                                    |
| “适用芯片” | 默认为“Snt3”。                                                                                                    |
| “检验值”  | 根据 <a href="#">准备训练数据</a> 所下载的“手势识别案例”文件夹中的“main.py”文件中init函数参数的值的代码，这里检验值应输入“gesture”。此处的检验值和init函数参数值应保持一致。 |
| “应用场景” | 选择“其他”，文本框中输入“手势识别”。                                                                                          |
| “技能图标” | 上传技能图标。                                                                                                       |
| “技能图片” | 用来向用户介绍技能的使用或技能的效果，可不上传。                                                                                      |
| “OS平台” | 选择“Linux”系统。                                                                                                  |
| “描述”   | 输入技能的描述。                                                                                                      |

图 13-9 填写基本信息

**基本信息**

技能模板 使用空模板 选择已有模板

\* 技能名称

\* 技能版本

\* 适用芯片

\* 检验值

\* 应用场景 其它 手势识别

技能图标

\* OS平台 Linux Android iOS LiteOS Windows

描述

B I H |

长度不能超过2048，且不能包含~^\$%&字符

### 技能内容

根据您的模型和逻辑代码情况，按表13-4填写技能内容，详细参数说明请参见技能内容。

表 13-4 技能内容参数

| 参数       | 推荐填写                                                                                                                                                                                                                                |
|----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| “技能格式”   | 选择“技能包”格式。                                                                                                                                                                                                                          |
| “运行时语言”  | 选择“Python3.7”。                                                                                                                                                                                                                      |
| “代码执行文件” | 默认输入“index.py”。                                                                                                                                                                                                                     |
| “模型”     | 单击加号，您可以在弹出框中，选择导入的模型“gesture-recognition”。                                                                                                                                                                                         |
| “代码上传方式” | 选择“在线编辑”，在代码编辑框中直接编辑代码，可直接复制准备训练数据所下载的“手势识别案例”文件夹中的“.py”文件中的代码内容，请核对代码中模型名称，保持代码中的模型名称与转换模型的模型名称一致。此样例中模型名称应是“gesture-recognition.om”，如下所示。<br><code>model = hilens.Model(hilens.get_model_dir() + "gesture-recognition.om")</code> |

图 13-10 技能内容

**技能内容**

|                          |                                                                                                                                 |                                |                                |
|--------------------------|---------------------------------------------------------------------------------------------------------------------------------|--------------------------------|--------------------------------|
| * 技能格式                   | <input checked="" type="radio"/> 技能包                                                                                            | <input type="radio"/> 容器镜像     |                                |
| * 运行时语言 <small>?</small> | <input checked="" type="radio"/> Python3.7                                                                                      | <input type="radio"/> C/C++    |                                |
| 代码执行文件 <small>?</small>  | <input type="text" value="index.py"/>                                                                                           |                                |                                |
| 模型                       | <div style="border: 1px dashed gray; padding: 5px; display: inline-block;">gesture-recognition — 1.0.0</div> <a href="#">删除</a> |                                |                                |
| * 代码上传方式                 | <input checked="" type="radio"/> 在线编辑                                                                                           | <input type="radio"/> 从OBS上传文件 | <input type="radio"/> 从容器镜像中选择 |

基本信息和技能内容填写完成后，您可以在界面右侧查看其配置参数值，如果某个字段填写错误，在右侧会显示一个小红叉。

**步骤4** 确认信息无误后，单击“确定”完成技能创建。

图 13-11 确认信息并完成新建技能

**基本信息**

|       |              |
|-------|--------------|
| 技能模板  | 使用空模板        |
| *技能名称 | Gesture R... |
| *技能版本 | 1.0.0        |
| *适用芯片 | Ascend310    |
| *检验值  | qesture      |
| *应用场景 | 其它-手势...     |
| 技能图标  |              |
| *OS平台 | Linux        |
| 描述    |              |

**技能内容**

|         |               |
|---------|---------------|
| *技能格式   | file          |
| *运行时语言  | Python3.7     |
| 代码执行... | index.py      |
| 模型      | {{"model v... |
| 模型密钥    |               |
| 代码上传... | 在线编辑          |

**运行时配置 (可选)**

**弹性技能参数 (可选)**

|          |      |
|----------|------|
| web请求uri |      |
| 模型地址     |      |
| 请求方法     | POST |
| 计算资源     | GPU  |

**确定** **取消**

#### ----结束

创建完成后，您的技能将进入“技能开发>技能管理”页面，且状态为“未发布”，您可以执行发布操作，将技能发布至技能市场；您也可以安装技能至设备，并查看设备使用技能效果。

## (可选) 发布技能

**步骤1** 在华为HiLens管理控制台，单击左侧导航栏“技能开发>技能管理”，进入“技能管理”页面。

**步骤2** 选择需要发布的技能，单击右边的“发布”。

**步骤3** 在弹出的“发布技能到技能市场”对话框中，按图13-12设置相关信息，单击“确定”。

图 13-12 发布技能

**发布技能**

\* 发布服务 HiLens 技能市场    ModelArts AI市场

\* 计费策略 免费    收费

\* 计费模式  包年/包月     一次性

\* 计量单位 ②  路数     并发量

\* 规格限制 ②

\* 隐私声明 ②

- 该技能会连接互联网
- 该技能会在设备上保存数据
- 该技能会读取设备摄像头麦克风数据
- 该技能会上传数据至华为云存储服务
- 该技能上传数据到最终用户所配置的服务接口
- 使用该技能会涉及到其他的用户隐私信息，包括

确定 取消

表 13-5 发布技能参数说明

| 参数字段 | 说明                                                                                                                                          |
|------|---------------------------------------------------------------------------------------------------------------------------------------------|
| 发布服务 | 技能发布的服务位置。本样例选择“HiLens技能市场”。                                                                                                                |
| 计费策略 | 技能发布在技能市场的计费策略。可选择“免费”和“收费”。                                                                                                                |
| 计费模式 | 技能发布后的计费模式。 <ul style="list-style-type: none"> <li>• 如果选择“免费”计费策略，仅可选择“一次性”计费模式。</li> <li>• 如果选择“收费”计费策略，可选择“包年/包月”和“一次性”两种计费模式。</li> </ul> |
| 计量单位 | 每份License可用在设备上的规格。有“路数”和“并发量”两种计量方式。如果以“路数”规格，一份License可安装在设备上使用一路视频。                                                                      |
| 规格限制 | 技能在同一设备上最多可以处理视频的路数，或最大并发量。                                                                                                                 |

| 参数字段 | 说明            |
|------|---------------|
| 隐私声明 | 技能涉及到的用户隐私声明。 |

提交之后，将发送至华为HiLens后台，由工作人员进行审核，3个工作日之内完成审核，请您耐心等待。当审核通过后，状态将变更为“审核通过，已发布”。

----结束

## 安装技能

**步骤1** 在“技能开发>技能管理”页面，选择已开发的技能，单击右侧操作列“安装”。

**步骤2** 勾选已注册且状态在线的设备，单击“安装”，安装成功后单击“确定”，完成安装技能操作，如图13-13所示。

安装过程中，华为HiLens管理控制台会将技能包下发到设备。下发技能包需要一段时间，可以从进度条中看到技能安装进度，下发完成后“进度”栏会提示“安装成功”。

图 13-13 安装成功

安装技能“Gesture\_Recognition”到设备。

| 设备名称                                  | 设备状态 | 资源约束                                                             | 固件名称                | 固件版本  | 进度     |
|---------------------------------------|------|------------------------------------------------------------------|---------------------|-------|--------|
| <input checked="" type="radio"/> test | ● 在线 | <input checked="" type="radio"/> 跨数<br><input type="radio"/> 并发量 | HiLens_Device_Ag... | 1.0.9 | ✔ 安装成功 |
| <input type="radio"/> test1           | ● 离线 | <input checked="" type="radio"/> 跨数<br><input type="radio"/> 并发量 | HiLens_Device_Ag... | 1.0.7 | -      |

5 总条数: 2 < 1 >

确定 取消

安装成功后，您可以启动技能查看技能输出数据。

----结束

## 启动技能

**步骤1** 使用HDMI视频线缆连接HiLens Kit视频输出端口和显示器。

**步骤2** 单击左侧导航栏“设备管理>设备列表”，进入“设备列表”页面。

**步骤3** 单击已注册设备的“技能管理”，查看技能状态已安装的手势识别技能状态为“停止”，单击操作列的“启动”，并单击“确定”，确定启动技能运行在端侧设备上。

等待一会，当状态变为“运行中”，则技能成功运行在端侧设备上。

安装技能的状态说明如图13-14所示。

图 13-14 查看技能状态

| 名称                  | ID                             | 版本    | 状态  | 资源约束 | 更新时间                | 操作          |
|---------------------|--------------------------------|-------|-----|------|---------------------|-------------|
| Gesture_Recognition | #60808272a805720172de955e418e2 | 1.0.0 | 运行中 | 16路  | 2020-06-29 15:42:25 | 启动 停止 卸载 更多 |

表 13-6 安装技能状态

| 状态名 | 状态说明               |
|-----|--------------------|
| 停止  | 停止状态，技能停止运行在端侧设备上。 |
| 运行中 | 运行状态，技能成功安装在端侧设备。  |

技能处于“运行中”状态时，您可以通过显示器查看技能输出的视频数据，此样例所开发的手势识别技能可识别一般的手势，技能输出的视频中会用方框标记出手势，并标记出手势含义。

----结束