MindStudio 2.0.0 版本说明

文档版本	01
发布日期	2021-04-22

华为技术有限公司

商标声明


和其他华为商标均为华为技术有限公司的商标。
本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

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

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 用户须知

MindStudio是一套基于IntelliJ框架的开发工具链平台，提供了应用开发、调试、模型转换功能，同时还提供了网络移植、优化和分析功能，为用户开发应用程序带来了极大的便利。

功能简介

- 针对安装与部署，MindStudio提供多种部署方式，支持多种主流操作系统以及容器化部署方式，为开发者提供最大便利。
- 针对算子开发，MindStudio提供包含UT测试、ST测试、TIK算子调试等的全套算子开发流程。支持TensorFlow、PyTorch、MindSpore等多种主流框架的TBE和AI CPU自定义算子开发。
- 针对网络模型的开发，MindStudio支持TensorFlow、Pytorch、Caffe、MindSpore框架的模型训练，支持多种主流框架的模型转换。集成了训练可视化、脚本转换、模型转换、模型量化、精度比对等工具，提升了网络模型移植、分析和优化的效率。
- 针对应用开发，MindStudio集成了Profiling性能调优、编译器、对接MindX SDK的应用开发、可视化pipeline业务流编排等工具，为开发者提供了图形化的集成开发环境，通过MindStudio能够进行工程管理、编译、调试、性能分析等全流程开发，能够很大程度提高开发效率。

2 版本特性

部署形态

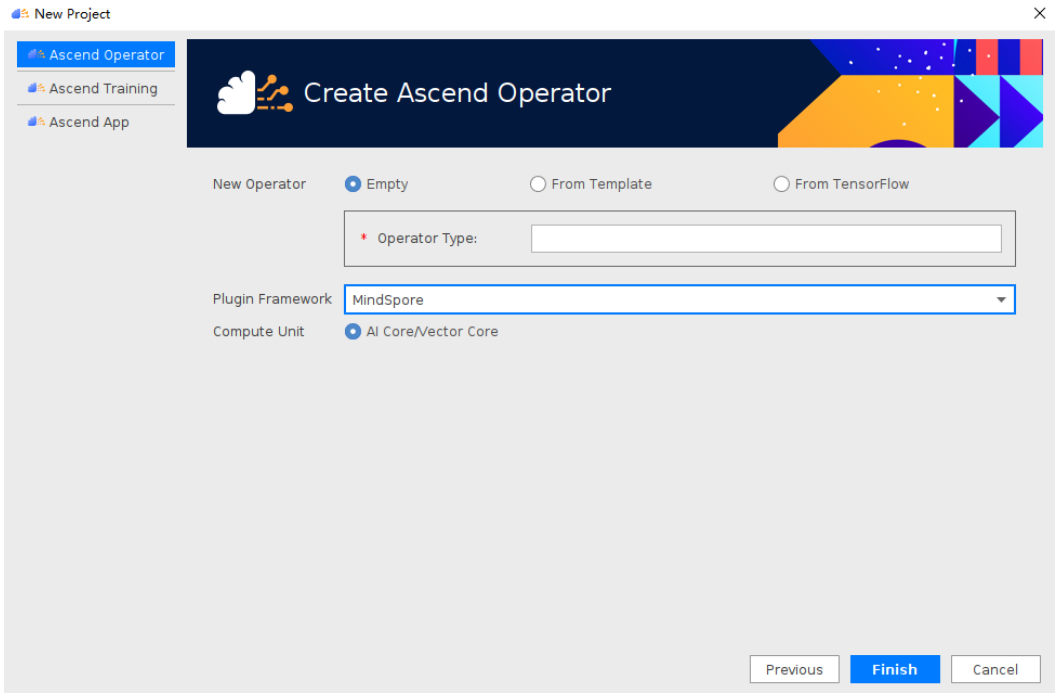
- Ascend-cann-toolkit整包安装non体验优化
- MindStudio新增支持Ubuntu-aarch64和Euler-aarch64操作系统
- MindStudio支持容器化部署方式

图 2-1 全流程开发工具链

算子开发

- 算子自动测试框架支持生成执行报告
- 算子工程ST测试支持将算子计算结果与标杆数据进行比对
- 支持MindSpore算子工程的创建与开发

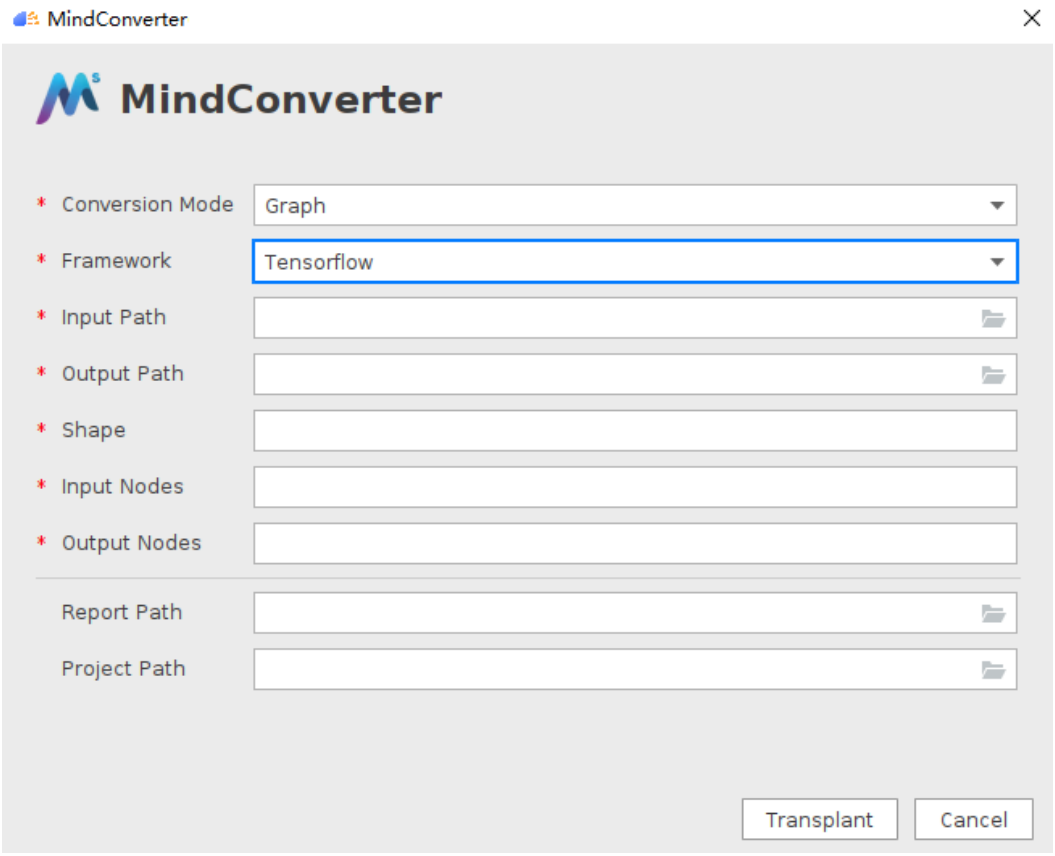
图 2-2 算子开发



模型开发

- 集成MindSpore训练脚本执行功能
- 训练脚本支持一键转换
- 集成MindConverter训练脚本转换
- 支持对接MindInsight训练可视化
- 模型转换AIPP增强——动态AIPP支持多输入节点

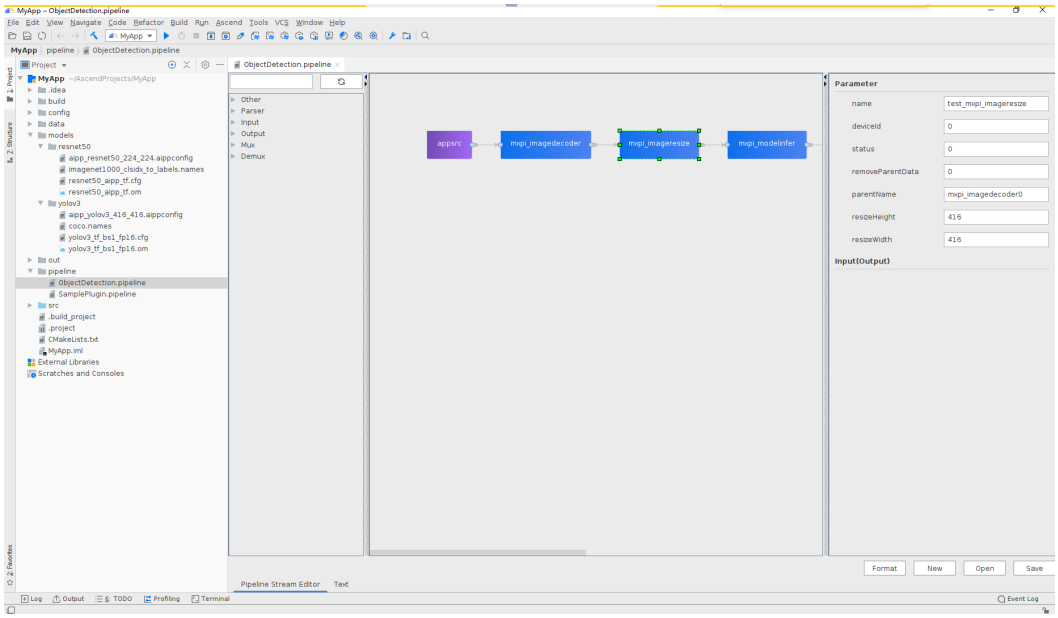
图 2-3 MindConverter



应用开发

- 应用工程远端推送工程目录优化
- 支持在线/离线下载MindX SDK软件包并集成到开发环境
- 支持可视化pipeline业务流编排工作

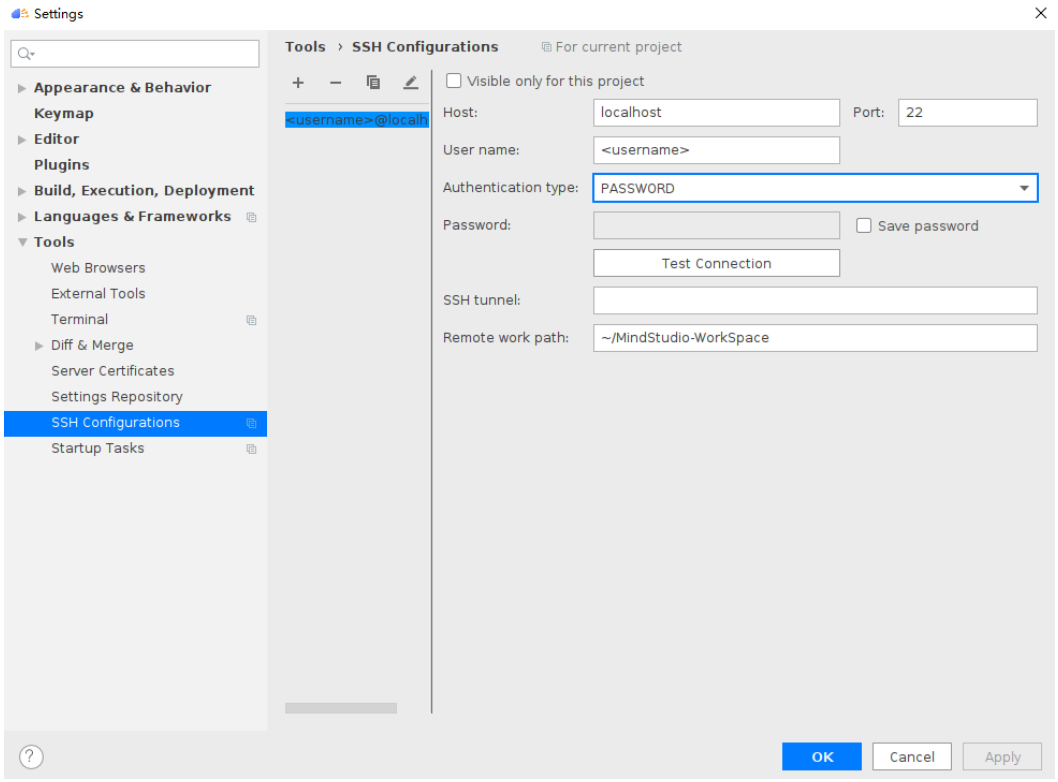
图 2-4 Pipeline 流程编排



开发辅助工具

- 新增系统级Profiling工具调优功能
- 支持TensorFlow子模型导出功能
- 支持模型局部结构和ONNX模型精度比对
- 支持SSH协议连接远端环境

图 2-5 SSH 连接



3 问题修复说明

问题单号	问题描述
DTS202104120QFA94P1200	【应用工程】应用调试无法使用非22的SSH端口。
DTS202104080KLGI1P0F00	【算子工程】算子ut_impl采用Simulator_TMModel模式，运行中终止运行失效。
DTS202104080IPBJ7P1I00	【算子工程】算子ut_impl采用Simulator_TMModel模式，FLOWCTRL数据条没有出现滚动数据或固定值。
DTS202104070RX6DNP0D00	【训练工程】创建新的训练工程，工程页面打开之后，创建页面未消失。
DTS202104070RMDWQP0G00	【应用工程】打开样例工程，没有bulid按钮。
DTS202104070RL2QRP1F00	【MindStudio启动】点击不引入配置进入Welcome界面，无法显示MindStudio logo，页面无法关闭，重启后MindStudio风格丢失。
DTS202104070RJHCRP1I00	【算子工程】创建模板算子工程，Create Ascend Operator页面Template File输入框右侧编辑图标显示不合理。
DTS202104070RHEBMP1300	【命名规范】统一算子圈所有芯片名称命名格式为SoC Version。
DTS202104070RAK70P0D00	【算子工程】算子部署窗口模态化处理。
DTS202103310RMVC3P1D00	【Profiling】Host侧性能数据采集osrt解决ltrace的CPU占用率为100%的问题。

4 漏洞修复说明

表 4-1 漏洞信息

软件名称	软件版本	CVE编号	CVSS	漏洞描述	解决版本
Netty	4.1.47	CVE-2021-21290	5.5	Netty is an open-source, asynchronous event-driven network application framework for rapid development of maintainable high performance protocol servers & clients. In Netty before version 4.1.59.Final there is a vulnerability on Unix-like systems involving an insecure temp file. When netty's multipart decoders are used local information disclosure can occur via the local system temporary directory if temporary storing uploads on the disk is enabled. On unix-like systems, the temporary directory is shared between all user. As such, writing to this directory using APIs that do not explicitly set the file/directory permissions can lead to information disclosure. Of note, this does not impact modern MacOS Operating Systems. The method	MindStudio V100R020C30

软件名称	软件版本	CVE编号	CVSS	漏洞描述	解决版本
				"File.createTempFile" on unix-like systems creates a random file, but, by default will create this file with the permissions "-rw-r--r--". Thus, if sensitive information is written to this file, other local users can read this information. This is the case in netty's "AbstractDiskHttpData" is vulnerable. This has been fixed in version 4.1.59.Final. As a workaround, one may specify your own "java.io.tmpdir" when you start the JVM or use "DefaultHttpDataFactory.setBaseDir(...)" to set the directory to something that is only readable by the current user.	
kotlin-reflect	1.3.70	CVE-2020-29582	5.3	In JetBrains Kotlin before 1.4.21, a vulnerable Java API was used for temporary file and folder creation. An attacker was able to read data from such files and list directories due to insecure permissions.	MindStudio V100R020C30

软件名称	软件版本	CVE编号	CVSS	漏洞描述	解决版本
google-guava	28.2.0.jre	CVE-2020-8908	3.3	A temp directory creation vulnerability exists in all versions of Guava, allowing an attacker with access to the machine to potentially access data in a temporary directory created by the Guava API com.google.common.io.Files.createTempDir(). By default, on unix-like systems, the created directory is world-readable (readable by an attacker with access to the system). The method in question has been marked @Deprecated in versions 30.0 and later and should not be used. For Android developers, we recommend choosing a temporary directory API provided by Android, such as context.getCacheDir(). For other Java developers, we recommend migrating to the Java 7 API java.nio.file.Files.createTempDirectory() which explicitly configures permissions of 700, or configuring the Java runtime's java.io.tmpdir system property to point to a location whose permissions are appropriately configured.	MindStudio V100R020C30