AgentSphere

快速入门

文档版本 01

发布日期 2026-09-29

华为云计算技术有限公司

版权所有 © 华为云计算技术有限公司 2026。 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

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。

华为云计算技术有限公司

地址： 贵州省贵安新区黔中大道交兴功路华为云数据中心 邮编：550029

网址： https://www.huaweicloud.com/

目 录

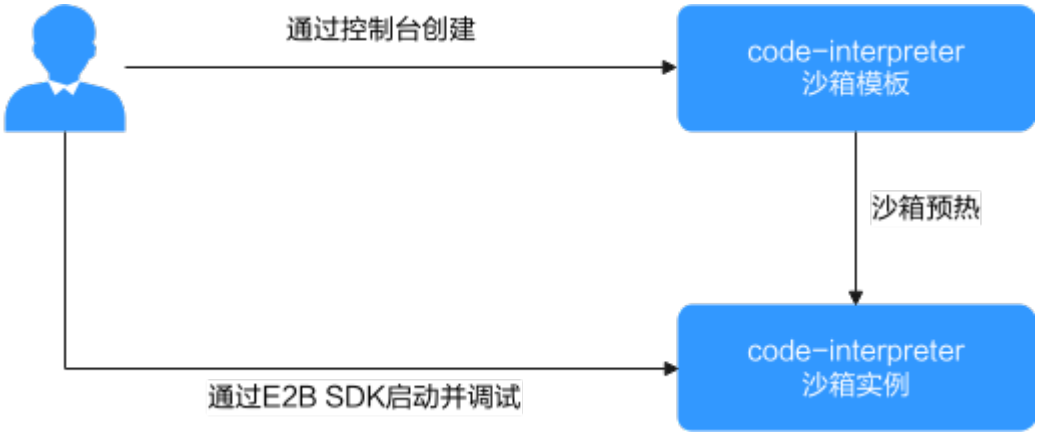
1 5 分钟开通沙箱并运行代码.....1

 版权所有 © 华为云计算技术有限公司

1 5 分钟开通沙箱并运行代码

在AI Agent开发中，Agent通常需要执行用户提交的代码或脚本（如数据处理、数学计算、图表生成等），直接在服务器上执行未知代码存在安全风险，可能导致系统资源被耗尽或敏感数据泄露。AgentSphere服务提供隔离的轻量级容器运行环境，具备资源隔离、快速启动、按需弹性伸缩的优势，可安全高效地执行AI Agent提交的代码，适用于AI Agent代码执行、在线编程、自动化测试、数据处理等需要安全隔离的场景。

本文以“代码解释器沙箱”为例，指导您完成AgentSphere沙箱服务的开通、模板配置、API Key创建，并通过Python SDK启动沙箱实例执行代码。



操作流程

操作步骤	说明	预计耗时
准备工作	注册华为账号并完成实名认证。	-
步骤一：服务开通及授权	当您的账号在当前区域中首次使用AgentSphere时，您需要为AgentSphere进行授权。	约10秒
步骤二：创建沙箱模板	新建沙箱模板，选择基础镜像并配置运行环境、启动命令等参数。	约2分钟
步骤三： 创建API Key	生成用于SDK认证的API Key。	约30秒

版权所有 © 华为云计算技术有限公司

操作步骤	说明	预计耗时
步骤四：启动并调试沙箱	使用Python SDK开通沙箱实例，上传测试代码并运行。	约2分钟
步骤五：清理测试资源	如果您在完成实践后不需要继续使用沙箱，请及时清理资源。	约30秒

准备工作

- 在开始操作前，请您先注册华为账号并完成实名认证，详情请参见**注册华为账号并开通华为云**和**个人实名认证**。
- 已准备好用于运行Python脚本的本地环境（Python版本需满足**e2b-code-interpreter**要求）。

步骤一：服务开通及授权

AgentSphere运行时需要访问其他云服务，当您首次登录AgentSphere控制台时，系统将自动请求获取当前区域下的相关云资源权限并创建权限委托。如果您在当前区域已完成授权，可忽略本步骤。

步骤1 使用华为账号登录AgentSphere控制台。

步骤2 单击控制台左上角的 ，选择区域。

步骤3 在首次登录某个区域的AgentSphere控制台时将跳出“开通及授权服务”弹窗，请您在仔细阅读后单击“开通授权”。

步骤4 授权成功后，您可正常使用智能体沙箱、智能体网关及智能体身份服务。

----结束

步骤二：创建沙箱模板

沙箱模板定义了沙箱实例的镜像、规格、网络和权限等参数，是创建沙箱实例的基础配置。

步骤1 登录AgentSphere控制台。

步骤2 在左侧导航栏中选择“沙箱模板”，并单击右上角的“创建沙箱模板”。

步骤3 选择沙箱模板类型。

- **代码解释器沙箱**：基于函数计算的多语言代码执行环境。本示例中选择该类型。
- **自定义沙箱**：基于自定义镜像的完全可控开发环境。

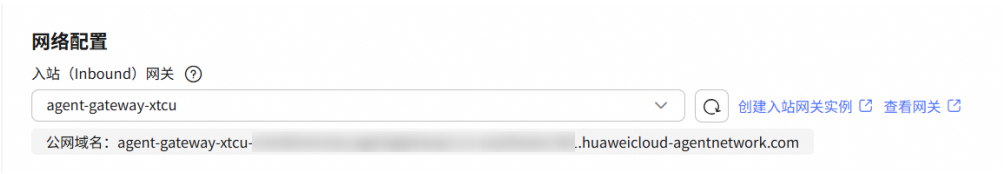
步骤4 填写模板**基础配置**，以下内容为必填项：

 版权所有 © 华为云计算技术有限公司

参数	说明	示例
沙箱模板名称	自定义沙箱模板名称。 沙箱模板名称需以小写字母开头，以小写字母或数字结尾，可以包含小写字母、数字和中划线，长度为1-48个字符。	code-interpreter-demo
资源配额	选择沙箱实例使用的CPU和内存，支持不同的CPU/内存配比。 您可以根据沙箱程序运行需求进行选择，资源配额过小可能导致沙箱运行失败，过大则会导致资源浪费。	2vCPUs 8GiB
沙箱实例配额	设置此沙箱模板创建实例的上限，所有模板实例配额总数上限为10000。	10

步骤5 配置网络与权限。

- **入站（Inbound）网关：**用于接收外部请求，配置后可通过网关访问沙箱内的服务，可选择已有网关或新建网关实例。



- **出站（Outbound）网络配置**：出站网络用于为沙箱实例分配IP地址，有两种模式供选择，本文档选择**VPC模式**。

  选择**VPC模式**时，以下参数为必填：

参数	说明
VPC	沙箱使用的VPC。请选择已有VPC，如无VPC请先创建。
子网	沙箱使用的VPC子网。
安全组	沙箱出方向关联的安全组，用于控制出站网络访问规则。

 版权所有 © 华为云计算技术有限公司

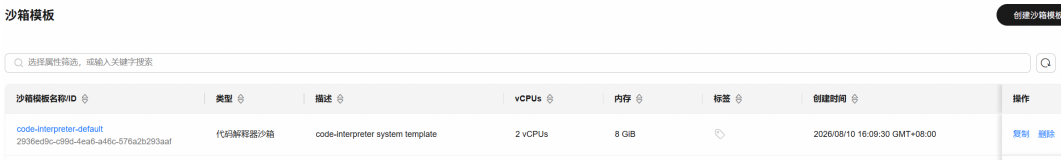
说明

如需沙箱通过公网访问外部服务，可选择**公网模式**，此时只需配置入站网关。

- **运行时信任委托**：非必填，授权AgentSphere在创建沙箱时访问用户的其他云服务资源如OBS，创建沙箱模板挂载OBS存储桶时，需要配置运行时信任委托。

步骤6 确认信息无误后，单击“创建”。

创建成功后，在沙箱模板列表中记录**模板ID**，后续步骤将使用。



----结束

步骤三： 创建 API Key

API Key用于E2B API和SDK的认证，请妥善保管您的API Key，建议定期重置以确保安全。

步骤1 登录AgentSphere控制台。

步骤2 在左侧导航栏中选择“API Key管理”，并单击右上角的“创建API Key”。

步骤3 设置API Key参数。

参数	参数说明
有效期	根据需求设置API Key的有效期，过期后该API Key将不可用。
描述	您可以添加该API Key的描述信息。

步骤4 单击“确定”，系统将自动为您生成API Key。

注意

为保障安全，生成的API Key将仅显示一次，请务必保存，关闭该页面后将无法再次查看。

您可以单击“下载API Key凭证”将API Key保存至本地。

----结束

版权所有 © 华为云计算技术有限公司

步骤四：启动并调试沙箱

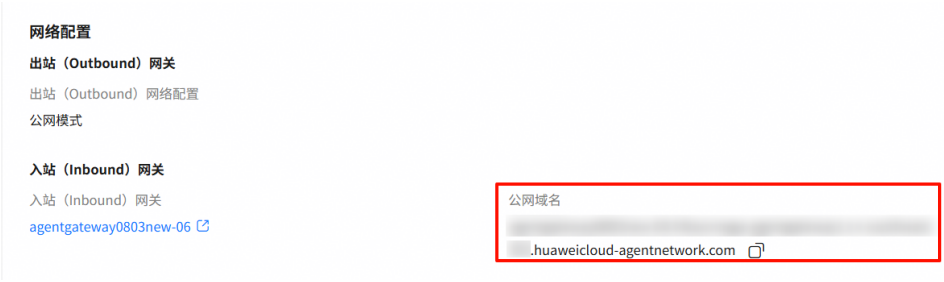
本步骤使用Python SDK（E2B）创建沙箱实例，并演示代码执行核心功能。

步骤1 安装E2B SDK。

```
pip install e2b-code-interpreter==2.9.1
```

步骤2 使用SDK创建沙箱实例，并替换其中4个参数：

- **E2B_SANDBOX_URL**：沙箱网关域名，可在控制台中找到对应的“沙箱模板”，然后单击模板名称进入详情页，在“网络配置”中查看其入站网关的“公网域名”。



- **E2B_API_URL**：智能体沙箱API访问地址，请通过《AgentSphere SDK参考》“配置本地E2B SDK执行环境”章节查询当前区域的API访问地址。
- **E2B_API_KEY**：步骤三中获取的API Key。
- **TEMPLATE**：步骤二中获取的模板ID。

设置环境变量：

```
export E2B_API_URL=https://agentsphere.<region>.myhuaweicloud.com
export E2B_SANDBOX_URL=https://<your-sandbox-url>.huaweicloud-agentnetwork.com
export E2B_API_KEY=<your_api_key>
```

将以下代码保存为e2b_create_code_interpreter.py：

```
# e2b_create_code_interpreter.py
import os
from e2b_code_interpreter import Sandbox
TEMPLATE="<template_id>"

# Create sandbox
sbx = Sandbox.create(
    template=TEMPLATE, api_key=E2B_API_KEY,
    api_url=E2B_API_URL, sandbox_url=E2B_SANDBOX_URL, timeout=60,
)
print(f"Sandbox created successfully, sandbox_id={sbx.sandbox_id}")

# Run code test
result = sbx.run_code("print('hello world')")
print(f"Output: {result.logs.stdout}")

# Cleanup sandbox
sbx.kill()
print("Sandbox cleaned up")
```

步骤3 执行脚本，预期如下图。

```
python e2b_create_code_interpreter.py
```

```
(myenv) root[redacted]-agentsphere-workuse:/home/e2b# python e2b_create_code_interpreter.py
Sandbox created successfully, sandbox_id=e0c61318ae301235a6f813d6f2dec67685571884bda6510392bf0750c33c4756
Output: ['hello world\n']
Sandbox cleaned up
```

----结束

版权所有 © 华为云计算技术有限公司

步骤五：清理测试资源

由于Sandbox实例在步骤四测试后已通过sbx.kill()自动清理，无需手动清理。如不再使用沙箱模板，请手动删除。

步骤1 登录AgentSphere控制台，在左侧导航栏中选择“沙箱模板”。

步骤2 找到目标沙箱模板，单击操作列的“删除”按钮。

图 1-1 删除沙箱模板

步骤3 在二次确认弹窗中确认待删除的沙箱模板信息，如果您确定要删除，请输入“DELETE”并单击“确定”。

----结束

版权所有 © 华为云计算技术有限公司