AgentSphere

用户指南

文档版本 01

发布日期 2026-10-08

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 智能体沙箱 1
1.1 沙箱概述 1
1.2 开始使用沙箱 3
1.3 沙箱模板 5
1.3.1 沙箱模板概述 5
1.3.2 创建沙箱模板 6
1.3.3 构建沙箱镜像 12
1.3.4 管理沙箱模板 17
1.3.5 配置访问 OBS 服务的终端节点 18
1.4 沙箱实例 20
1.4.1 沙箱实例概述 20
1.4.2 创建沙箱实例 22
1.4.3 监控与日志 23
1.4.4 删除沙箱实例 24
1.5 API Key 管理 25
1.5.1 API Key 概述 25
1.5.2 创建 API Key 26
1.5.3 管理 API Key 27
2 智能体网关 29
2.1 网关实例概述 29
2.2 创建网关实例 30
2.3 管理网关实例 31
2.4 导出网关实例列表信息 33
3 智能体身份 35
3.1 工作负载身份概述 35
3.2 查看工作负载身份 35

 版权所有 © 华为云计算技术有限公司

1 智能体沙箱

1.1 沙箱概述

什么是沙箱

智能体沙箱为AI Agent提供安全隔离的执行环境，支持多种执行环境类型，满足不同Agent任务的运行需求。每个沙箱实例运行在独立的虚拟化环境中，拥有独立的文件系统、网络空间和进程环境，实例间完全隔离，防止恶意代码逃逸和横向攻击。

功能特性

- **安全隔离**：每个沙箱实例运行在独立的虚拟化环境中，进程、文件系统、网络相互隔离，防止恶意代码逃逸和横向攻击。
- **多种沙箱类型**：提供代码解释器沙箱及自定义沙箱，适配不同Agent任务场景。
- **弹性伸缩**：Serverless架构，按需创建和释放，支持快速启动和大规模并发。
- **灵活网络配置**：支持VPC模式和公网模式，VPC模式可访问私有网络资源，公网模式开箱即用访问公网服务。
- **持久化存储**：支持外挂对象存储和文件存储，数据独立于实例生命周期，多实例可共享存储。
- **可观测性**：提供实例运行状态监控和操作日志，支持全链路操作追踪。

核心概念

沙箱模板与沙箱实例

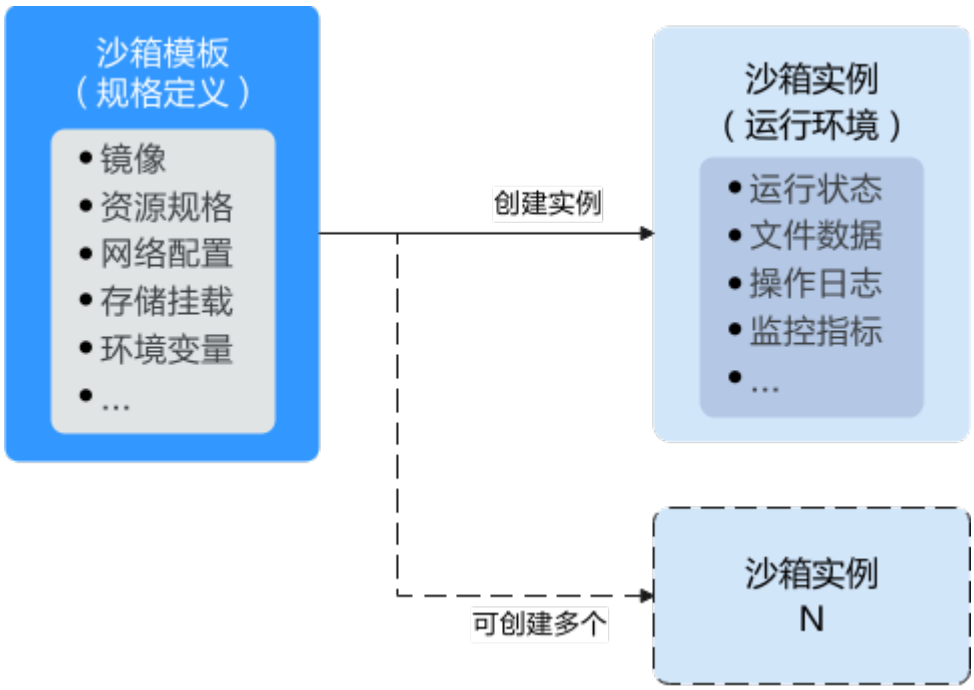
使用沙箱时，您必须要了解模板和实例两个概念：

- **沙箱模板**：可复用的沙箱环境参数配置，避免每次创建沙箱时重复配置，包含镜像、资源规格、网络配置、存储挂载、环境变量等参数。系统提供内置模板，也支持创建自定义模板。
- **沙箱实例**：基于模板创建的运行态沙箱，是实际执行任务的环境。

一个模板可以创建多个实例，两者的关系如下图所示：

版权所有 © 华为云计算技术有限公司

图 1-1 沙箱模板与沙箱实例的关系

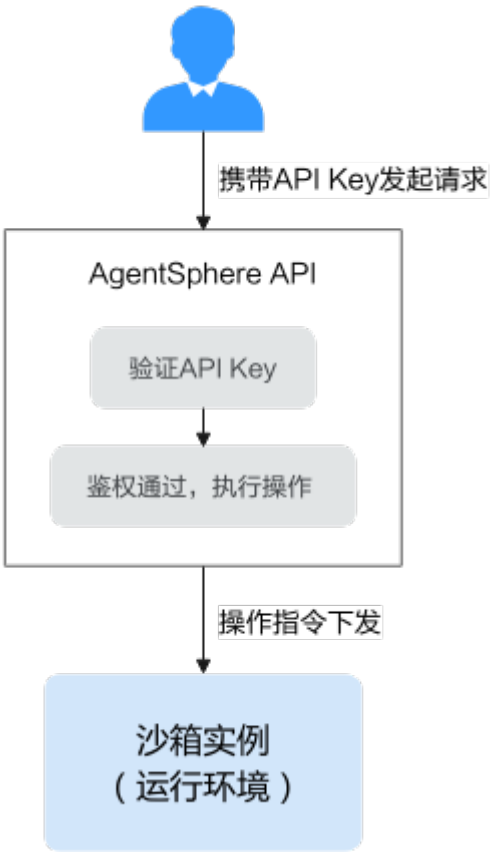


API Key

API Key是调用AgentSphere API和SDK的认证凭证。用户通过API Key鉴权后，才能创建、连接和管理沙箱实例。API Key用于外部调用鉴权，不注入实例内部。一个API Key可操作多个实例，一个实例也可被多个API Key操作（取决于权限配置）。

版权所有 © 华为云计算技术有限公司

图 1-2 API Key 与沙箱实例的关系



相关文档

- 快速了解沙箱完整使用流程，请参见**开始使用沙箱**。
- 了解如何定义沙箱规格，请参见**沙箱模板**。
- 了解沙箱实例的详细操作，请参见**沙箱实例**。
- 获取API调用凭证，请参见**API Key管理**。

1.2 开始使用沙箱

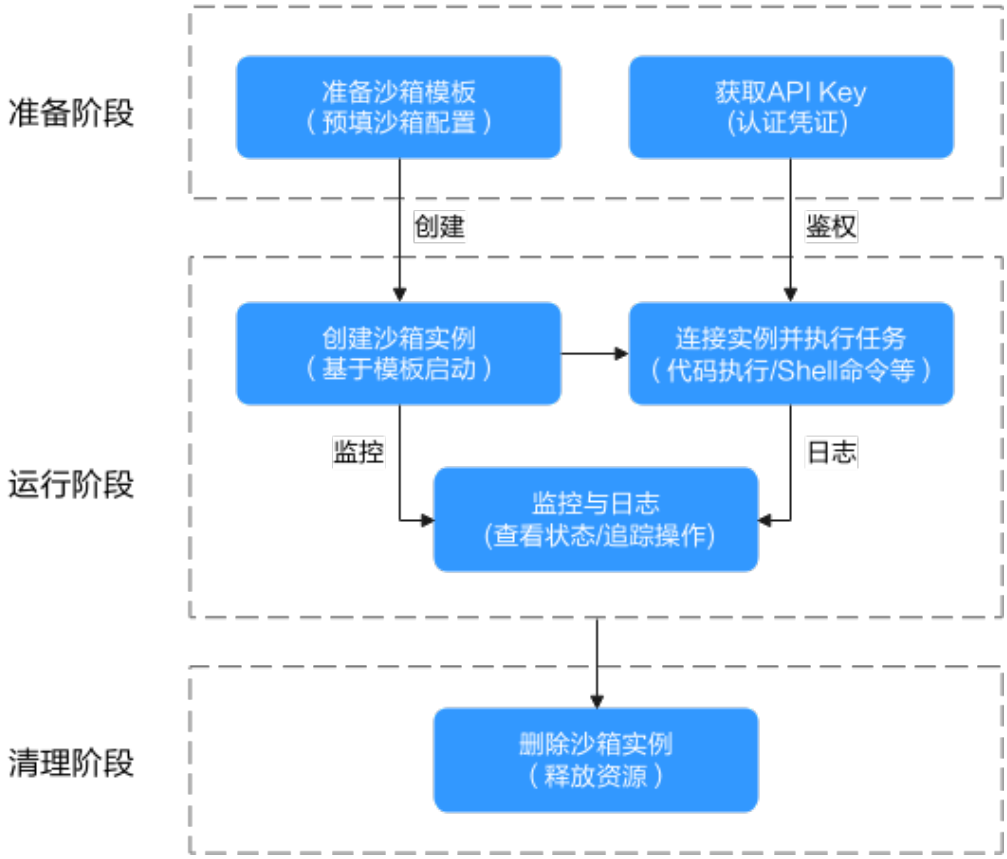
本文主要介绍AgentSphere沙箱的整体使用流程，帮助您了解从准备到运行任务的各环节及其关系，助您快速上手。

使用流程总览

使用沙箱大致可分为三个阶段：准备、运行、清理。

版权所有 © 华为云计算技术有限公司

图 1-3 使用流程总览



准备阶段

- 准备沙箱模板：选择代码解释器模板或创建自定义模板，模板定义了实例的镜像、资源规格、网络配置等，是创建实例的前提。详情请参见**沙箱模板概述**。

  沙箱模板可以分为两大类：

  - 代码解释器模板：预装了Jupyter的运行环境，适合快速验证运行代码，无需额外配置，可直接使用。
  - 自建模板：基于自定义镜像进行创建，适合特殊资源规格和特定网络配置的场景。
- 获取API Key：创建用于调用API和SDK的认证凭证，所有创建、连接、管理沙箱实例的操作都需要通过API Key鉴权。详情请参见**API Key概述**。

运行阶段

准备阶段就绪后，即可进入运行阶段：

1. **创建沙箱实例**

   基于模板创建实例，实例将继承模板中定义的镜像、资源规格、网络配置等。创建时可覆盖模板的部分配置（如环境变量等），无需为临时调整而修改模板。详情请参见**创建沙箱实例**。

   实例创建后自动进入运行状态，即可接受任务执行。
2. **连接实例并执行任务**

   调用API Key通过API/SDK方式连接沙箱实例，并在沙箱中执行任务，例如执行代码、Shell命令等。

版权所有 © 华为云计算技术有限公司

3. **监控与日志**

   任务执行过程中，可随时查看实例的运行状态和资源使用情况，追踪操作记录，用于问题排查和性能分析。详情请参见**监控与日志**。

清理阶段

任务完成后，删除沙箱实例以释放资源。详情请参见**删除沙箱实例**。

如果沙箱实例长时间处在闲置状态，在闲置时间超过超时时间（超时时间可在模板中配置）后，系统会自动释放或休眠。

⚠ 注意

删除操作不可逆，实例内置文件系统中的数据将被清除。如需保留数据，请在删除前导出或使用外挂存储。

相关文档

您可能需要了解的下一步操作：

- 了解创建沙箱模板的详细配置，请参见**创建沙箱模板**。
- 了解创建沙箱实例的详细配置，请参见**创建沙箱实例**。
- 了解创建API Key的详细操作，请参见**创建API Key**。

1.3 沙箱模板

1.3.1 沙箱模板概述

什么是沙箱模板

沙箱模板是沙箱实例的规格定义，描述了实例创建时的运行环境配置，包括镜像、资源规格、网络配置、存储挂载和环境变量等参数。模板是静态定义，本身不运行任务。

通过模板可以将环境配置标准化和复用，避免每次创建实例时重复配置。一个模板可以创建多个沙箱实例。

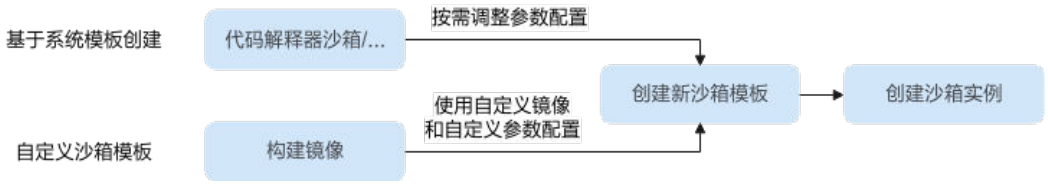
基本使用流程

在使用沙箱模板时，您可以根据需求创建模板。

- 基于系统模板创建（无法自定义镜像）：您可根据系统模板创建新的沙箱模板，并调整模板中的参数配置。
- 自定义沙箱模板（支持自定义镜像）：如果系统模板中的预装环境不满足需求，您可根据需求构建镜像，并创建自定义沙箱模板。

版权所有 © 华为云计算技术有限公司

图 1-4 模板使用流程



沙箱模板类型

模板类型	镜像预装环境	核心能力	典型场景
代码解释器沙箱（系统模板）	Python、JavaScript等多语言环境	通用代码执行环境，可执行多语言代码、Shell命令等。	数据分析、代码生成与验证、自动化脚本执行
自定义沙箱	使用自定义镜像，根据需求预装环境	自定义运行环境与依赖，灵活适配业务需求。	特殊依赖环境、企业定制化需求

相关文档

- 如果您需要自行创建沙箱模板，请参见**创建沙箱模板**。
- 如果您需要管理已有模板，请参见**管理沙箱模板**。
- 如果您需要构建自定义镜像，请参见**构建沙箱镜像**。

1.3.2 创建沙箱模板

您可以创建新的沙箱模板，调整沙箱镜像或参数配置。本文介绍如何创建沙箱模板。

前提条件

- 如果您需要创建自定义沙箱模板，需要先构建沙箱镜像，详情请参见**构建沙箱镜像**。
- 如果您需要使用OBS对象存储，需要先配置访问OBS服务的VPC终端节点，详情请参见**配置访问OBS服务的终端节点**。

创建沙箱模板

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。
- **自定义沙箱**：基于自定义镜像的完全可控开发环境。

----结束

版权所有 © 华为云计算技术有限公司

代码解释器沙箱

步骤1 填写**基础配置**。

参数	参数说明
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。
描述	您可以添加该沙箱模板的描述信息，最多1000字符。
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。
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。
启动命令	沙箱实例启动时执行的命令，适用于需要指定应用入口、挂载点或端口映射等初始化场景。 您可以增加64个镜像启动命令，每个命令长度为1-4096个字符。
环境变量	支持通过键值对的形式为沙箱运行环境设置变量，可用于把外部信息传递给沙箱中运行的程序。 您可以添加50个环境变量。

步骤2 填写**网络配置**。

参数		参数说明
入站（Inbound）网关		入站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。 如果没有可选网关，请单击“新建入站网关实例”进行创建，完成创建后单击刷新按钮。 **注意** 系统将自动创建工作负载身份，用于E2B身份验证。
出站（Outbound）网络配置	VPC模式	沙箱实例可以访问虚拟私有云VPC内的其他服务。 • **虚拟私有云**：选择一个虚拟私有云VPC。 若没有可选虚拟私有云，请单击“新建虚拟私有云”进行创建，完成创建后单击刷新按钮。操作步骤详情请参见**创建虚拟私有云和子网**。 • **子网**：在选定的VPC下选择一个子网。 • **安全组**：为沙箱实例选择安全组，支持同时选择多个安全组（此时安全组规则取并集）。 您可以单击“展开安全组规则”查看具体的“入方向规则”和“出方向规则”。
	公网模式	沙箱实例可通过公网对外访问，适用于需要联网调用第三方API、下载依赖等场景。

版权所有 © 华为云计算技术有限公司

参数	参数说明
运行时信任委托	用于授予OBS桶的访问权限。当配置了OBS对象存储时，此项必填。

步骤3 填写**存储配置**。

参数	参数说明
SFS Turbo文件存储	选择是否挂载SFS Turbo文件存储，勾选后，您可以选择将指定的文件系统目录挂载至沙箱目录。**只有出站（Outbound）网络配置为“VPC模式”时支持SFS Turbo文件存储，同时SFS Turbo安全组需要放通沙箱模板选择的VPC网段。** 如果没有可选文件系统，您可单击“创建文件系统”进行创建，完成创建后单击刷新按钮。相关配置说明请参见**创建SFS Turbo文件系统**。 您最多可以同时挂载5个存储路径（支持选择不同文件系统）。 • **存储路径**：填写文件系统的存储路径，存储路径必须以/开头，且不能包含“..”。 • **读写权限**：为此挂载路径设置“读写”或“只读”权限。 **说明** 如果要对挂载路径进行读写操作，不仅要保证沙箱开启挂载路径的读写权限，还需要保证SFS Turbo文件系统目录允许Linux用户进行读写，具体说明请参见**访问文件无权限**。 • **挂载路径**：挂载路径必须为绝对路径，以/home、/mnt、/data、/tmp开头，且不能包含“..”。
OBS对象存储	选择是否挂载OBS对象存储，勾选后，您可以选择将指定的OBS对象存储桶目录挂载至沙箱目录。**只有出站（Outbound）网络配置为“VPC模式”时支持OBS对象存储。** 如果没有可选对象桶，您可单击“创建OBS桶”进行创建，完成创建后单击刷新按钮。相关配置说明请参见**创建桶**。 **注意** 部分多AZ存储的对象桶可能挂载失败，如果需要挂载多AZ存储的对象桶，请提交工单给OBS服务并提供对象桶名称进行确认。 您最多可以同时挂载5个桶目录（支持选择不同对象桶）。 • **桶目录**：填写对象桶目录。 • **挂载路径**：挂载路径必须为绝对路径，以/home、/mnt、/data、/tmp开头，且不能包含“..”。
托管会话存储	选择是否将Session会话进行持久化存储，通过配置托管的文件存储，保留Agent会话状态，开启后需填写Session会话存储的挂载路径。

步骤4 填写**日志监控配置**。

版权所有 © 华为云计算技术有限公司

参数	参数说明
日志对接LTS	将沙箱的标准输出和标准错误日志采集到LTS日志服务中。您可以使用LTS对云服务日志进行关键词搜索、日志可视化分析、日志告警、日志转储等多种操作。 • **日志组**：云日志服务进行日志管理的基本单位，用于对日志流进行分类，一个日志组下面可以创建多个日志流。 如果没有可选日志组，您可单击“创建日志组”进行创建，完成创建后单击刷新按钮。相关配置说明请参见**管理日志组**。 • **日志流**：日志读写的基本单位，日志组中可以创建日志流，将不同类型的日志分类存储，方便对日志进一步分类管理。 如果没有可选日志流，您可单击“创建日志流”进行创建，完成创建后单击刷新按钮。相关配置说明请参见**管理日志流**。
对接AOM	启用后沙箱的系统指标（如CPU、内存使用率）会上报到您选择的AOM实例，其中基础指标免费，其他指标按需收费，关于价格详情请参见**计费项**。 如果没有可选AOM实例，您可单击“新建实例”进行创建，完成创建后单击刷新按钮。相关配置说明请参见**管理Prometheus实例**。

步骤5 填写**高级配置**。

参数	参数说明
闲置超时时间	沙箱无操作时保持活跃的时长，沙箱在闲置超时时间结束后，自动释放或者休眠，若沙箱有新任务或操作时，闲置超时时间会重置。 若持续有新任务及操作时，沙箱最大运行时长不超过24小时。
健康检查	• **使用默认配置**：默认为ENVD 49983端口，协议为HTTP、检查路径为/health。 • **自定义配置**：配置应用程序健康检查的协议、端口和路径。 **说明** 当镜像内有多个进程时，建议配置健康检查指向启动慢的进程。

步骤6 完成上述配置后，单击“创建”。

----结束

自定义沙箱

步骤1 填写**基础配置**。

参数	参数说明
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。
描述	您可以添加该沙箱模板的描述信息，最多1000字符。

版权所有 © 华为云计算技术有限公司

参数	参数说明
选择镜像	单击“选择镜像”，选择沙箱使用的镜像，镜像数据来源于容器镜像服务（SWR）。 如果您需要使用第三方镜像，可直接输入镜像地址，但需要同时保证沙箱环境可访问镜像仓库。
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。
启动命令	沙箱实例启动时执行的命令，适用于需要指定应用入口、挂载点或端口映射等初始化场景。 您可以增加64个镜像启动命令，每个命令长度为1-4096个字符。
环境变量	支持通过键值对的形式为沙箱运行环境设置变量，可用于把外部信息传递给沙箱中运行的程序。 您可以添加50个环境变量。

步骤2 填写**网络配置**。

参数		参数说明
入站（Inbound）网关		入站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。 如果没有可选网关，请单击“新建入站网关实例”进行创建，完成创建后单击刷新按钮。 **注意** 系统将自动创建工作负载身份，用于E2B身份验证。
出站（Outbound）网络配置	VPC模式	沙箱实例可以访问虚拟私有云VPC内的其他服务。 • **虚拟私有云**：选择一个虚拟私有云VPC。 若没有可选虚拟私有云，请单击“新建虚拟私有云”进行创建，完成创建后单击刷新按钮。操作步骤详情请参见**创建虚拟私有云和子网**。 • **子网**：在选定的VPC下选择一个子网。 • **安全组**：为沙箱实例选择安全组，支持同时选择多个安全组（此时安全组规则取并集）。 您可以单击“展开安全组规则”查看具体的“入方向规则”和“出方向规则”。
	公网模式	沙箱实例可通过公网对外访问，适用于需要联网调用第三方API、下载依赖等场景。
运行时信任委托		用于授予OBS桶的访问权限。当配置了OBS对象存储时，此项必填。

步骤3 填写**存储配置**。

版权所有 © 华为云计算技术有限公司

参数	参数说明
SFS Turbo文件存储	选择是否挂载SFS Turbo文件存储，勾选后，您可以选择将指定的文件系统目录挂载至沙箱目录。**只有出站（Outbound）网络配置为“VPC模式”时支持SFS Turbo文件存储，同时SFS Turbo安全组需要放通沙箱模板选择的VPC网段。** 如果没有可选文件系统，您可单击“创建文件系统”进行创建，完成创建后单击刷新按钮。相关配置说明请参见**创建SFS Turbo文件系统**。 您最多可以同时挂载5个存储路径（支持选择不同文件系统）。 • **存储路径**：填写文件系统的存储路径，存储路径必须以/开头，且不能包含“..”。 • **读写权限**：为此挂载路径设置“读写”或“只读”权限。 **说明** 如果要对挂载路径进行读写操作，不仅要保证沙箱开启挂载路径的读写权限，还需要保证SFS Turbo文件系统目录允许Linux用户进行读写，具体说明请参见**访问文件无权限**。 • **挂载路径**：挂载路径必须为绝对路径，以/home、/mnt、/data、/tmp开头，且不能包含“..”。
OBS对象存储	选择是否挂载OBS对象存储，勾选后，您可以选择将指定的OBS对象存储桶目录挂载至沙箱目录。**只有出站（Outbound）网络配置为“VPC模式”时支持OBS对象存储。** 如果没有可选对象桶，您可单击“创建OBS桶”进行创建，完成创建后单击刷新按钮。相关配置说明请参见**创建桶**。 **注意** 部分多AZ存储的对象桶可能挂载失败，如果需要挂载多AZ存储的对象桶，请提交工单给OBS服务并提供对象桶名称进行确认。 您最多可以同时挂载5个桶目录（支持选择不同对象桶）。 • **桶目录**：填写对象桶目录。 • **挂载路径**：挂载路径必须为绝对路径，以/home、/mnt、/data、/tmp开头，且不能包含“..”。
托管会话存储	选择是否将Session会话进行持久化存储，通过配置托管的文件存储，保留Agent会话状态，开启后需填写Session会话存储的挂载路径。

步骤4 填写**日志监控配置**。

版权所有 © 华为云计算技术有限公司

参数	参数说明
日志对接LTS	将沙箱的标准输出和标准错误日志采集到LTS日志服务中。您可以使用LTS对云服务日志进行关键词搜索、日志可视化分析、日志告警、日志转储等多种操作。 • **日志组**：云日志服务进行日志管理的基本单位，用于对日志流进行分类，一个日志组下面可以创建多个日志流。 如果没有可选日志组，您可单击“创建日志组”进行创建，完成创建后单击刷新按钮。相关配置说明请参见**管理日志组**。 • **日志流**：日志读写的基本单位，日志组中可以创建日志流，将不同类型的日志分类存储，方便对日志进一步分类管理。 如果没有可选日志流，您可单击“创建日志流”进行创建，完成创建后单击刷新按钮。相关配置说明请参见**管理日志流**。
对接AOM	启用后沙箱的系统指标（如CPU、内存使用率）会上报到您选择的AOM实例，其中基础指标免费，其他指标按需收费，关于价格详情请参见**计费项**。 如果没有可选AOM实例，您可单击“新建实例”进行创建，完成创建后单击刷新按钮。相关配置说明请参见**管理Prometheus实例**。

步骤5 填写**高级配置**。

参数	参数说明
闲置超时时间	沙箱无操作时保持活跃的时长，沙箱在闲置超时时间结束后，自动释放或者休眠，若沙箱有新任务或操作时，闲置超时时间会重置。 若持续有新任务及操作时，沙箱最大运行时长不超过24小时。
健康检查	• **使用默认配置**：默认为ENVD 49983端口，协议为HTTP、检查路径为/health。 • **自定义配置**：配置应用程序健康检查的协议、端口和路径。 **说明** 当镜像内有多个进程时，建议配置健康检查指向启动慢的进程。

步骤6 完成上述配置后，单击“创建”。

----结束

相关文档

- 如果您需要管理已有模板，请参见**管理沙箱模板**。
- 如果您需要构建自定义镜像，请参见**构建沙箱镜像**。

1.3.3 构建沙箱镜像

AgentSphere沙箱通过内置的ENVD（环境守护进程，Environment Daemon）来提供文件操作、进程管理和环境变量设置等能力。

由于当前沙箱仅支持单容器部署，ENVD需要作为容器内的常驻进程运行，因此您需要基于自己的业务镜像进行自定义构建，将ENVD集成到镜像中。

版权所有 © 华为云计算技术有限公司

前提条件

- 已安装Docker用于构建镜像。
- 已安装Go语言编译环境，用于编译ENVD二进制，版本建议1.21+。
- 已准备好需要作为基础的业务镜像。
- 已有SWR镜像仓库，构建完成后可推送至SWR供沙箱使用。

操作流程

整体流程分为三个步骤：

1. **编译ENVD二进制**：根据目标镜像的CPU架构编译Linux版本的ENVD。
2. **准备辅助文件**：健康检查脚本和启动脚本。
3. **编写Dockerfile并构建镜像**：将ENVD集成到业务镜像中，并推送至SWR。

步骤一：编译 ENVD 二进制

步骤1 拉取ENVD代码。

```
git clone git@github.com:e2b-dev/infra.git
```

步骤2 进入envd目录，根据目标镜像的CPU架构构建二进制。

```
cd packages/envd
CGO_ENABLED=0 GOOS=linux GOARCH=amd64 go build -ldflags="-s -w" -o envd main.go
```

如果需要构建ARM64架构的镜像，请将其中的*GOARCH=amd64*改为*GOARCH=arm64*。

步骤3 验证编译结果。执行目录下应生成envd二进制文件。

```
ls -la envd
```

----结束

步骤二：准备辅助文件

您需要准备两个辅助文件：健康检查脚本和启动脚本。

健康检查脚本（envd-healthcheck.sh）

ENVD启动后需要一定时间完成初始化。健康检查脚本通过轮询ENVD的状态接口，确保ENVD完全就绪后再启动业务应用，避免后续操作因ENVD未就绪而失败。

步骤1 创建envd-healthcheck.sh文件。

```
vi envd-healthcheck.sh
```

步骤2 按“i”进入编辑模式，输入以下脚本内容。

```
#!/bin/bash
# Custom health check for ENVD Server
# Verifies the server is responsive via the /api/status endpoint
MAX_RETRIES=50
RETRY_INTERVAL=0.2
for i in $(seq 1 $MAX_RETRIES); do
    status_code=$(curl -s -o /dev/null -w "%{http_code}" "http://localhost:49983/health")
    if [ "$status_code" -eq 204 ]; then
        echo "ENVD Server is healthy"
        exit 0
    fi
    if [ $((i % 10)) -eq 0 ]; then
```

 版权所有 © 华为云计算技术有限公司

```
        echo "Waiting for ENVD Server to become healthy... (attempt $i/$MAX_RETRIES)"
    fi
    sleep $RETRY_INTERVAL
done
echo "ENVD Server health check failed after $MAX_RETRIES attempts"
exit 1
```

步骤3 修改完成后，按“Esc”，输入:wq保存并退出文件编辑。

----结束

启动脚本（entrypoint.sh）

容器启动时，需要先启动ENVD并等待其就绪，再执行原有业务启动逻辑。在业务镜像原有的entrypoint基础上，添加ENVD的启动和健康检查逻辑。

步骤1 修改entrypoint.sh文件。

```
vi entrypoint.sh
```

步骤2 按“i”进入编辑模式，添加以下脚本内容。

```
function start_envd() {
    /path/to/envd -isnotfc -port 49983 -verbose &
    /path/to/envd-healthcheck.sh
    if [ $? -ne 0 ]; then
        echo "ENVD Server failed to start, aborting."
        exit 1
    fi
}
echo "Starting ENVD server..."
start_envd
# 原有的启动脚本内容，忽略。
```

请注意替换*/path/to/envd*和*/path/to/envd-healthcheck.sh*为容器中实际路径。

步骤3 修改完成后，按“Esc”，输入:wq保存并退出文件编辑。

----结束

步骤三：构建镜像

Dockerfile 编写

以下Dockerfile以业务镜像为基础，集成ENVD及其辅助文件：

步骤1 创建Dockerfile。

```
vi Dockerfile
```

步骤2 按“i”进入编辑模式，填写以下内容。

```
# 将用户镜像用作Base镜像
FROM <user-image>

# ENVD需要以root身份运行
USER root

# 安装tini作为PID 1进程
RUN apt-get update \
    && apt-get install -y --no-install-recommends \
        tini \
    && rm -rf /var/lib/apt/lists/*

# 复制ENVD二进制、健康检查脚本和启动脚本
COPY local/path/to/envd /image/path/to/envd
COPY local/path/to/envd-healthcheck.sh /image/path/to/envd-healthcheck.sh
```

 版权所有 © 华为云计算技术有限公司

```
COPY local/path/to/entrypoint.sh /image/path/to/entrypoint.sh
RUN chmod +x /image/path/to/envd
RUN chmod +x /image/path/to/envd-healthcheck.sh
RUN chmod +x /image/path/to/entrypoint.sh

# ENVD服务的监听端口
EXPOSE 49983

# 使用tini管理进程，-g 会将停止信号转发给所有子进程
ENTRYPOINT ["/usr/bin/tini", "-g", "--", "/image/path/to/entrypoint.sh"]
```

步骤3 修改完成后，按“Esc”，输入:wq保存并退出文件编辑。

----结束

其他补充场景示例

按需添加运行依赖

您可以在Dockerfile中按需添加其它依赖和配置。例如，如果需要通过ENVD执行Python脚本，镜像中必须包含Python运行环境，则可以在Dockerfile的安装命令部分插入以下内容：

```
RUN apt-get update \
    && apt-get install -y --no-install-recommends python3 \
    && rm -rf /var/lib/apt/lists/*
```

说明

仅当需要安装第三方Python包时才需额外安装python3-pip。

非 root 镜像用户

如果用户镜像使用非root用户运行，需要进行额外适配，ENVD必须以root权限运行，但业务应用仍应以原镜像用户身份运行，遵循最小权限原则。

因此需要在Dockerfile中临时切换到root用户完成安装和授权，再切换回原有用户；在entrypoint.sh中则通过sudo仅提升ENVD进程的权限。

假设原镜像使用appuser用户运行，可以按以下方式进行配置。

步骤1 在Dockerfile中安装sudo，并仅允许appuser免密执行指定的ENVD启动命令：

```
FROM <user-image>

USER root

# 安装tini和sudo
RUN apt-get update \
    && apt-get install -y --no-install-recommends \
        sudo \
        tini \
    && rm -rf /var/lib/apt/lists/*

# 复制文件并设置权限
COPY --chmod=0755 local/path/to/envd /image/path/to/envd
COPY --chmod=0755 local/path/to/envd-healthcheck.sh /image/path/to/envd-healthcheck.sh
COPY --chmod=0755 local/path/to/entrypoint.sh /image/path/to/entrypoint.sh

# 配置sudoers：仅允许appuser免密执行ENVD启动命令
RUN mkdir -p /etc/sudoers.d
RUN echo 'appuser ALL=(root) NOPASSWD:SETENV /image/path/to/envd -isnotfc -port 49983 -verbose' \
        > /etc/sudoers.d/envd \
    && chmod 0440 /etc/sudoers.d/envd

# 切回原镜像用户，原有应用仍以appuser身份运行
```


版权所有 © 华为云计算技术有限公司

```
USER appuser

EXPOSE 49983

ENTRYPOINT ["/usr/bin/tini", "-g", "--", "/image/path/to/entrypoint.sh"]
```

⚠ 注意

请不要配置*appuser ALL=(ALL) NOPASSWD:ALL*，仅授予启动ENVD所需的最小权限。如果修改了ENVD路径或启动参数，需同步更新*/etc/sudoers.d/envd*中的命令。

步骤2 修改entrypoint.sh中启动ENVD的命令，使用*sudo -n*提权启动ENVD，*-n*参数确保无法免密执行时立即失败，避免启动过程阻塞等待密码输入。

```
function start_envd() {
        sudo -n -E /image/path/to/envd -isnotfc -port 49983 -verbose &
        /image/path/to/envd-healthcheck.sh
        if [ $? -ne 0 ]; then
                echo "ENVD Server failed to start, aborting."
                exit 1
        fi
}
echo "Starting ENVD server..."
start_envd
# 原有的启动脚本内容保持不变
```

entrypoint.sh和原有应用仍以appuser身份运行，只有ENVD进程以root身份运行。

----结束

构建并验证镜像

构建镜像命令如下：

```
docker build -t my-sandbox-image:latest .
```

其中，*my-sandbox-image:latest*为镜像名称和版本名称。

建议在推送前本地运行验证：

```
docker run --rm -p 49983:49983 my-sandbox-image:latest
```

验证要点：

- 启动日志中出现“ENVD Server is healthy”。
- 原有业务应用正常启动。

推送镜像到 SWR

构建并验证通过后，可将镜像推送到华为云容器镜像服务（SWR），供沙箱模板使用。

以基础版SWR为例，步骤如下：

步骤1 登录**SWR控制台**，选择左侧导航栏的“组织管理”，单击页面右上角的“创建组织”，创建一个组织。

如已有组织可跳过此步骤。

步骤2 在左侧导航栏选择“我的镜像”，单击右侧“客户端上传”，在弹出的页面中单击“生成登录指令”，单击 复制临时登录指令。

版权所有 © 华为云计算技术有限公司

步骤3 在集群节点上执行上一步复制的登录指令，登录成功会显示“Login Succeeded”。

步骤4 给镜像打上SWR标签

```
docker tag my-sandbox-image:latest swr.cn-north-4.myhuaweicloud.com/<namespace>/my-sandbox-image:latest
```

其中，*swr.cn-north-4.myhuaweicloud.com*为镜像仓库地址可在SWR控制台上查询，登录指令中末尾的域名即为镜像仓库地址；*<namespace>*为SWR中已创建的组织名称。

步骤5 推送镜像到 SWR：

```
docker push swr.cn-north-4.myhuaweicloud.com/<namespace>/my-sandbox-image:latest
```

推送完成后，可在SWR控制台对应组织的镜像列表中查看到该镜像。

----结束

相关文档

在创建沙箱模板时，即可选择已上传的SWR镜像，详情请参见创建沙箱模板。

1.3.4 管理沙箱模板

沙箱模板创建后，您可以根据业务变化对模板进行操作，包括复制和删除。

沙箱模板操作

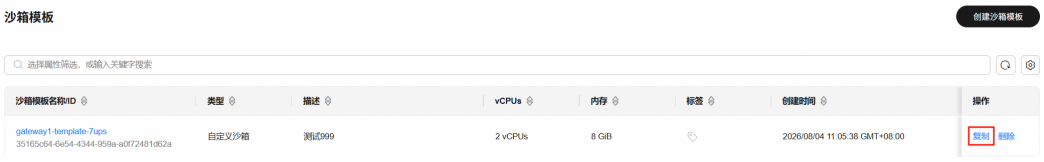
操作	说明
复制沙箱模板	您可以复制现有沙箱模板的配置来创建新的沙箱模板。
删除沙箱模板	如果沙箱模板无需再使用，您可以将其删除。沙箱模板删除后，将无法恢复，请谨慎操作。

复制沙箱模板

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“复制”按钮。

图 1-5 复制沙箱模板



步骤3 系统会自动填充复制的沙箱模板配置，您也可以根据需要进行修改，具体参数说明详情请参见创建沙箱模板。

步骤4 确定配置后单击“创建”。

----结束

版权所有 © 华为云计算技术有限公司

删除沙箱模板

> **⚠ 注意**
>
> 沙箱模板删除后无法恢复，请谨慎操作。

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 1-6 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

1.3.5 配置访问 OBS 服务的终端节点

在使用AgentSphere时，您可能需要配置访问OBS服务的VPC终端节点（VPCEP）。

配置访问 OBS 服务的 VPC 终端节点

步骤1 登录**VPC终端节点控制台**。

步骤2 在“终端节点”页面，单击“购买终端节点”。

步骤3 根据界面提示配置必选参数。更多参数说明，请参见**购买终端节点**。

表 1-1 终端节点配置参数

参数	说明
区域	终端节点所在区域，需要与AgentSphere沙箱所在区域保持一致。
计费模式	仅支持按需计费。按需计费是后付费模式，按终端节点的实际使用时长计费，可以随时开通/删除终端节点。
服务类别	选择“按名称查找服务”。
服务名称	通过**表1-2**查找当前区域的服务名称，单击“验证”，显示“已找到服务”表示填写无误。
创建内网域名	如果您需要以域名的方式访问终端节点，则选择“创建内网域名”，终端节点创建完成后，即可通过内网域名直接访问终端节点。

版权所有 © 华为云计算技术有限公司

参数	说明
虚拟私有云	需要选择AgentSphere沙箱所在的虚拟私有云。
路由表	选择一个已有的路由表。

表 1-2 OBS 终端节点服务名称

区域	名称
西南-贵阳一	com.myhuaweicloud.cn-southwest-2.v4.obsv2.region
华南-广州	com.myhuaweicloud.cn-south-1.v4.obsv2.region
华北-北京四	com.myhuaweicloud.cn-north-4.v4.obsv2.region

图 1-7 创建 OBS 服务的 VPC 终端节点

步骤4 参数配置完成，单击“立即购买”，进行规格确认。

- 规格确认无误，单击“提交”，任务提交成功。
- 参数信息配置有误，需要修改，单击“上一步”，修改参数，然后单击“提交”。

版权所有 © 华为云计算技术有限公司

步骤5 返回终端节点列表，如果终端节点状态为“已接受”，表示终端节点已成功连接至终端节点服务。

----结束

1.4 沙箱实例

1.4.1 沙箱实例概述

什么是沙箱实例

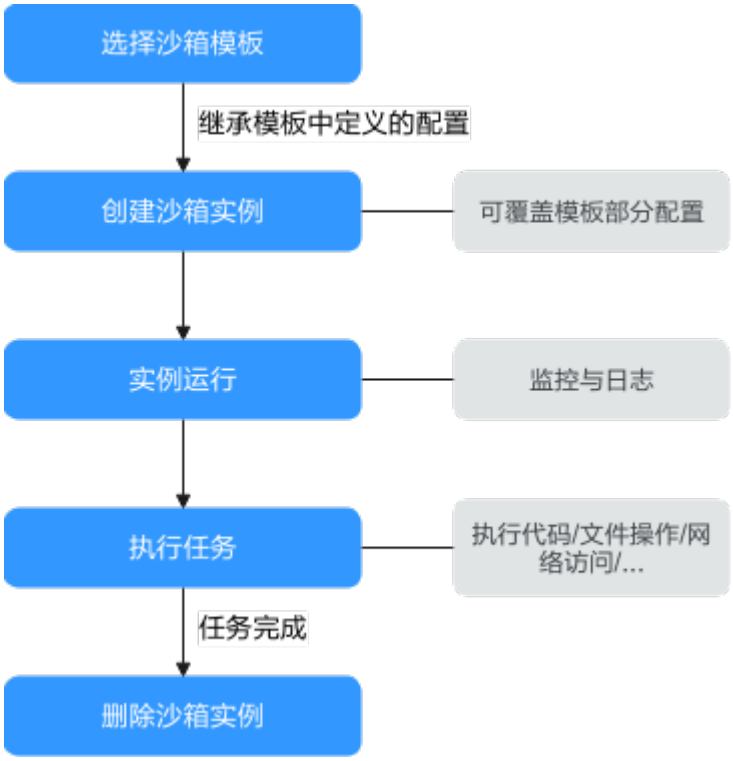
沙箱实例是基于沙箱模板创建的运行态沙箱，是AgentSphere中实际执行任务的环境。每个实例运行在独立的虚拟化环境中，拥有独立的文件系统、网络空间和进程环境，实例间完全隔离。

基本使用流程

沙箱实例是基于沙箱模板创建的运行环境，创建时从模板继承配置，创建后则独立于模板运行：

- 创建时：实例从模板继承镜像、资源规格、网络配置、存储挂载、环境变量等配置。
- 创建后：实例的配置独立于模板，已创建的实例不受模板状态影响。
- 覆盖配置：创建实例时可填写配置参数，这些配置会覆盖模板中的同名配置（如环境变量），无需修改模板。

图 1-8 基本使用流程



版权所有 © 华为云计算技术有限公司

沙箱实例的管理方式

沙箱实例创建完成后，AgentSphere提供多种方式管理和使用沙箱实例：

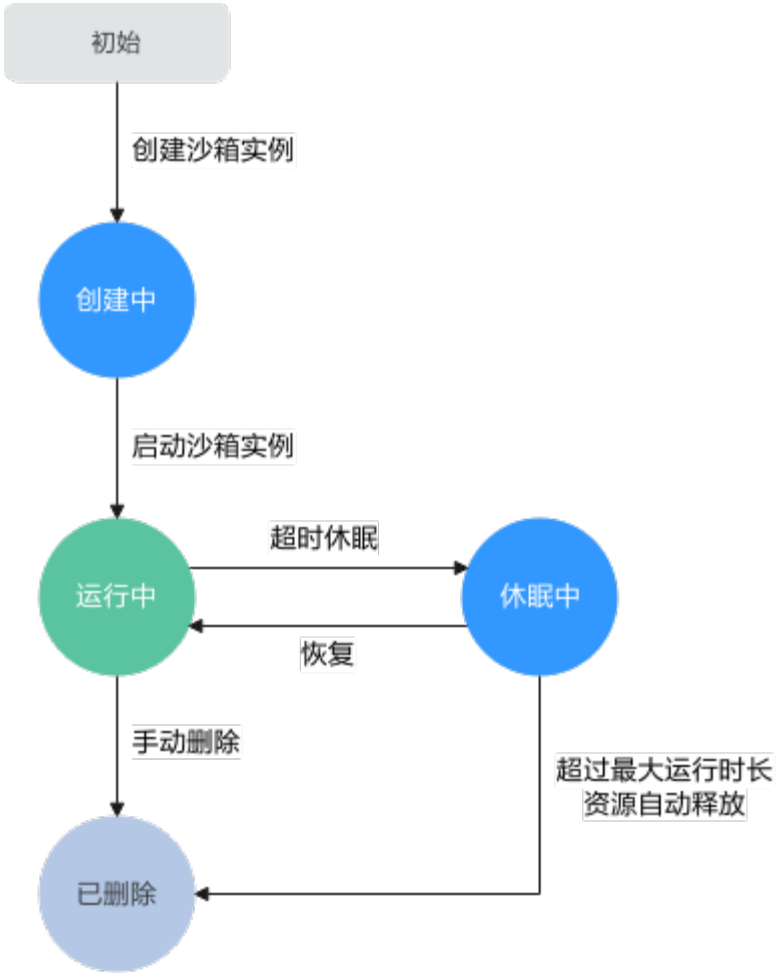
管理方式	适用场景
控制台	可视化管理沙箱实例，适合运维和调试场景。
API/SDK	通过兼容E2B的API接口管理沙箱，适合系统集成和自动化。

沙箱实例的生命周期

表 1-3 生命周期说明

状态	说明
创建中	实例正在创建中
运行中	实例正常运行，可接受任务
休眠中	实例暂停，资源释放，上下文保留
已删除	实例已销毁，不可恢复

图 1-9 沙箱实例的生命周期



版权所有 © 华为云计算技术有限公司

相关文档

- 了解创建沙箱实例的详细配置，请参见**创建沙箱实例**。
- 如需查看已有实例的监控与日志信息，请参见**监控与日志**。
- 如需手动删除实例，请参见**删除沙箱实例**。

1.4.2 创建沙箱实例

沙箱实例基于沙箱模板创建，创建时从模板继承镜像、资源规格、网络配置等参数，同时支持覆盖部分配置（如环境变量等）。实例创建后自动进入运行中状态，即可接受Agent任务执行。本文介绍如何创建沙箱实例。

前提条件

如果您需要使用OBS对象存储，需要先配置访问OBS服务的VPC终端节点，详情请参见**配置访问OBS服务的终端节点**。

创建沙箱实例

步骤1 登录AgentSphere控制台。

步骤2 在左侧导航栏中选择“沙箱实例”，并单击右上角的“创建沙箱实例”。

步骤3 填写**基础配置**。

参数	参数说明
沙箱名称	自定义沙箱名称。 沙箱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1-56个字符。
选择沙箱模板	选择沙箱创建的模板，沙箱模板中定义了沙箱资源配额、网络配置、权限配置等必要参数。 如果没有可选沙箱模板，您可单击“创建沙箱模板”进行创建，完成创建后单击刷新按钮。相关配置说明请参见**创建沙箱模板**。
元数据标签	用于标识、分类和筛选沙箱资源，便于在大规模部署或自动化测试中进行批量管理。元数据标签采用键值对的形式，最多可以添加10个。
环境变量	运行沙箱时动态传入的配置参数，允许在不重新构建镜像的情况下，灵活调整应用的行为和设置。环境变量采用键值对的形式，最多可以添加50个。

步骤4 填写**沙箱配置**。

版权所有 © 华为云计算技术有限公司

参数	参数说明
SFS Turbo文件存储	选择是否挂载SFS Turbo文件存储，勾选后，您可以选择将指定的文件系统目录挂载至沙箱目录。**只有出站（Outbound）网络配置为“VPC模式”时支持SFS Turbo文件存储，同时SFS Turbo安全组需要放通沙箱模板选择的VPC网段。** 如果没有可选文件系统，您可单击“创建文件系统”进行创建，完成创建后单击刷新按钮。相关配置说明请参见**创建SFS Turbo文件系统**。 您最多可以同时挂载5个存储路径（支持选择不同文件系统）。 • **存储路径**：填写文件系统的存储路径，存储路径必须以/开头，且不能包含“..”。 • **读写权限**：为此挂载路径设置“读写”或“只读”权限。 **说明** 如果要对挂载路径进行读写操作，不仅要保证沙箱开启挂载路径的读写权限，还需要保证SFS Turbo文件系统目录允许Linux用户进行读写，具体说明请参见**访问文件无权限**。 • **挂载路径**：挂载路径必须为绝对路径，以/home、/mnt、/data、/tmp开头，且不能包含“..”。
OBS对象存储	选择是否挂载OBS对象存储，勾选后，您可以选择将指定的OBS对象存储桶目录挂载至沙箱目录。**只有出站（Outbound）网络配置为“VPC模式”时支持OBS对象存储。** 如果没有可选对象桶，您可单击“创建OBS桶”进行创建，完成创建后单击刷新按钮。相关配置说明请参见**创建桶**。 **注意** 部分多AZ存储的对象桶可能挂载失败，如果需要挂载多AZ存储的对象桶，请提交工单给OBS服务并提供对象桶名称进行确认。 您最多可以同时挂载5个桶目录（支持选择不同对象桶）。 • **桶目录**：填写对象桶目录。 • **挂载路径**：挂载路径必须为绝对路径，以/home、/mnt、/data、/tmp开头，且不能包含“..”。

步骤5 完成上述配置后，单击“确认”。

----结束

相关文档

- 如果您需要查看沙箱实例的监控与日志信息，请参见**监控与日志**。
- 如果您需要删除已有沙箱实例，请参见**删除沙箱实例**。

1.4.3 监控与日志

AgentSphere提供沙箱实例的运行状态监控和日志采集能力。通过监控可查看实例的CPU、内存等资源使用情况，帮助您掌握实例运行健康状况；通过日志可追踪实例的标准输出和标准错误信息，用于问题排查和性能分析。

版权所有 © 华为云计算技术有限公司

前提条件

创建沙箱实例时，选择的沙箱模板中已配置“日志对接LTS”或“对接AOM”，详情请参见**日志监控配置**。

监控

步骤1 登录AgentSphere控制台，在左侧导航栏中选择“沙箱实例”。

步骤2 找到目标实例，单击实例名称。

步骤3 切换至“监控”页签，查看监控信息。

图 1-10 监控

----结束

日志

步骤1 登录AgentSphere控制台，在左侧导航栏中选择“沙箱实例”。

步骤2 找到目标实例，单击实例名称。

步骤3 切换至“日志”页签，查看日志信息。

----结束

1.4.4 删除沙箱实例

当沙箱实例完成任务或不再需要时，您可以手动删除实例以释放资源。删除后实例内置文件系统中的数据将被清除且不可恢复，如需保留数据请在删除前导出或使用外挂存储。

删除沙箱实例

⚠ 注意

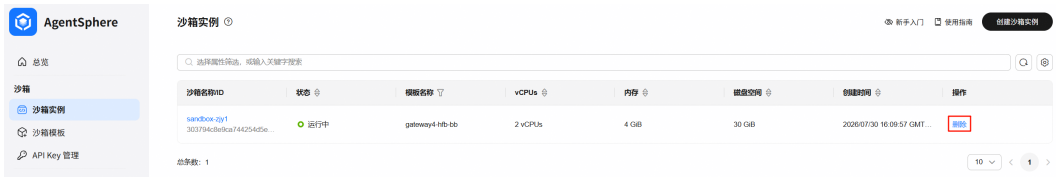
沙箱实例删除后无法恢复，请谨慎操作。

步骤1 登录AgentSphere控制台，在左侧导航栏中选择“沙箱实例”。

步骤2 找到目标实例，单击操作列的“删除”按钮。

版权所有 © 华为云计算技术有限公司

图 1-11 删除沙箱实例



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

----结束

1.5 API Key 管理

1.5.1 API Key 概述

什么是 API Key

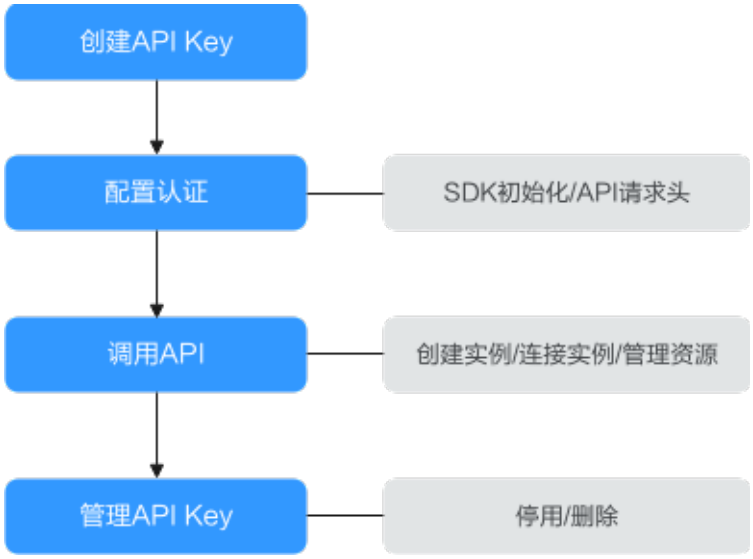
API Key是调用AgentSphere API和SDK的认证凭证，通过API或SDK操作沙箱资源时（如创建沙箱模板、创建沙箱实例等），需携带API Key进行身份鉴权。

基本使用流程

API Key的使用流程可大致分为创建、配置、调用、停用/删除四个环节。具体如下：

1. 在控制台创建API Key，API Key仅在创建时显示一次，需立即妥善保存。
2. 获取API Key后，在SDK或API请求中配置认证信息，即可调用AgentSphere的各类接口操作沙箱资源。
3. 当API Key不再使用时，应及时删除。

图 1-12 API 使用流程



版权所有 © 华为云计算技术有限公司

安全建议

- 妥善保管API Key：API Key生成后仅显示一次，请务必保存，切勿将API Key硬编码在代码中或提交到版本库，建议通过环境变量或密钥管理服务注入。
- 定期轮换：建议定期轮换API Key，降低泄露风险。
- 及时清理：不再使用的API Key应及时删除，避免遗留安全隐患。

相关文档

- 了解创建API Key的详细操作，请参见**创建API Key**。
- 管理已有API Key，请参见**管理API Key**。

1.5.2 创建 API Key

API Key是沙箱的长期访问凭证，用于E2B API和SDK的认证，适用于自动化脚本、CI/CD流水线和长期运行的后台服务。本文介绍如何在控制台创建API Key。

⚠ 注意

请妥善保管您的API Key，建议定期重置以确保安全。

前提条件

使用IAM用户创建API Key时，请先确认该用户已启用“编程访问”，具体确认方法请参见**管理IAM用户的基本信息**。

操作步骤

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

1.5.3 管理 API Key

API Key创建后，您可以根据安全策略和业务变化对其进行管理，包括停用和删除操作。停用API Key可临时暂停其访问权限，支持再次启用；删除API Key则永久移除该凭证，适用于不再使用的场景。

停用 API Key

停用API Key后，所有使用此专属凭证的集成应用程序访问权限将被暂停，您将无法使用未启用的专属凭证进行认证，但停用API Key后支持再次启用。

步骤1 登录AgentSphere控制台，在左侧导航栏中选择“API Key管理”。

步骤2 找到目标API Key，单击操作列的“停用”按钮。

图 1-13 停用 API Key

步骤3 在弹窗中单击“确定”。API Key状态将被置为“已停用”。

----结束

删除 API Key

您无法直接删除生效中的API Key，如果您需要删除API Key，请先停用该API Key，确认无影响后再删除。

⚠ 注意

API Key删除后无法恢复，请谨慎操作。

步骤1 登录AgentSphere控制台，在左侧导航栏中选择“API Key管理”。

步骤2 找到“已停用”的目标API Key，单击操作列的“删除”按钮。

图 1-14 删除 API Key

版权所有 © 华为云计算技术有限公司

步骤3 在二次确认弹窗中确认待删除的API Key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

2 智能体网关

2.1 网关实例概述

智能体网关（Agent Gateway）是面向Agent应用的企业级智能体网关，用于管理客户端、 Agent与其他工具之间的所有交互。作为Agent与外部系统、数据源及Agent间交互的统一流量入口与策略执行中枢，负责统一处理来自多端的异构请求，负责高效、稳定地调用各类工具与服务。

网关实例是用户创建的承载数据交互人的智能体网关实例，执行具体的数据交互任务。

实例区域

不同区域的资源之间内网不互通。建议选择靠近业务的区域，可以降低网络时延、提高访问速度。

公网和私网部署

Agent Gateway支持用户进行公网部署、私网部署、公私网混合部署的形态，可以根据实际业务诉求进行网络配置。

- **Agent Gateway公网部署**

  通过给Agent Gateway绑定EIP共享带宽，使其支持转发公网流量请求，通过公网域名对外提供服务，将来自公网的请求分发到已经关联到实例的目标进行处理。

  说明

  当前仅支持共享公网入口，公网访问开启后将产生公网出流量费用（按实际使用量计费）。

- **Agent Gateway私网部署**

  通过给Agent Gateway绑定私网IP，使其支持转发私网流量请求，通过私网域名对外提供服务，将来自私网的请求分发到已经关联到实例的目标进行处理。

相关文档

- 创建网关实例，请参见**创建网关实例**。
- 管理网关实例，请参见**管理网关实例**。

版权所有 © 华为云计算技术有限公司

2.2 创建网关实例

智能体网关（Agent Gateway）实例作为Agent流量统一出入口，对出入站流量进行统一管理。智能体网关当前支持入站功能，入站实例部署在沙箱或Agent前，用以将流量转发至沙箱或Agent应用，并提供网络访问配置、安全防护、身份认证等能力。

约束与限制

- 智能体网关当前只支持入站能力，出站能力暂不支持。
- 一个网关实例最多可关联10个VPC。

创建网关实例

步骤1 登录Agentsphere控制台。

步骤2 在左侧导航栏中选择“网关实例”，并单击右上角的“创建网关实例”。

步骤3 根据界面提示配置网关实例的基本信息，配置参数如表2-1所示。

表 2-1 网关实例的基本信息

参数	说明
区域	不同区域的资源之间内网不互通。请选择靠近业务的区域，可以降低网络时延、提高访问速度。
网关部署位置	网关部署位置。 • 入站：从用户/外部系统进入Agent内部的流量方向，负责将所有流入Gateway的流量进行身份权限验证等网络防控。 • 出站：从Agent内部发送给外部系统/API的流量方向，负责对所有流出Agent的流量进行出站访问的网络控制策略。（出站当前版本暂不支持）
名称	待创建网关实例的名称。 • 长度范围为1~52个字符。 • 名称由小写英文字母、数字组成，可使用中划线分隔，但不能以中划线开头，且不能连续使用中划线。
描述	根据需要在文本框中输入对该网关实例的描述信息。 描述信息内容不能超过255个字符，且不能包含“<”和“>”。

步骤4 根据界面提示进行网关实例网络配置，网络配置参数如表2-2所示。

版权所有 © 华为云计算技术有限公司

表 2-2 网关实例的网络配置

参数	说明
公网访问	如果勾选了公网访问，您的Agent将通过共享公网入口对外提供服务。 • 公网出流量按实际用量计费； • 当前仅支持共享公网带宽入口，多租户高峰期可能存在带宽争用。
私网访问	私网访问通过关联VPC（虚拟私有云）实现，Agent与企业内部系统在同一VPC内通信，流量不经过公网，具备更低延迟和更高安全性。
VPC	如果勾选了“私网访问”，则需要选择VPC和子网。 网关实例所属虚拟私有云。 可以选择使用已有的虚拟私有云网络，或者单击“创建虚拟私有云”创建新的虚拟私有云。
子网	如果勾选了“私网访问”，则需要选择VPC和子网。 子网为网关实例提供私网IP地址，**用于与内网中的资源进行通信**。 可以选择使用已有的子网，或者单击“创建子网”创建新的子网。

步骤5 单击“立即创建”，完成创建。

步骤6 返回网关实例列表页面，即可查看新创建的实例。

----结束

相关文档

- 管理网关实例，请参见**管理网关实例**。
- 导出网关实例列表信息，请参见**导出网关实例列表信息**。

2.3 管理网关实例

网关实例创建后，可以根据实际业务需求对网关实例的配置进行调整。

关联 VPC

网关实例创建后，可以为网关实例新增关联多个VPC，一个网关实例最多可关联10个VPC。

步骤1 登录Agentsphere控制台，在左侧导航栏中选择“网关实例”。

步骤2 在网关实例列表页面，单击目标网关实例的名称，进入网关实例详情页。

步骤3 切换到网关实例的“基本信息”页签，单击私网访问区域的“关联”。

步骤4 在“关联VPC”对话框中，选择需要新增关联的VPC和子网。

版权所有 © 华为云计算技术有限公司

步骤5 单击“确定”，完成关联。

----结束

解关联 VPC

步骤1 登录Agentsphere控制台，在左侧导航栏中选择“网关实例”。

步骤2 在网关实例列表页面，单击目标网关实例的名称，进入网关实例详情页。

步骤3 切换到网关实例的“基本信息”页签，在私网访问区域已关联的虚拟私有云列表中，单击待解关联VPC所在行。

步骤4 在私网访问区域，待解关联的VPC所在行，单击操作列的“解关联”。

步骤5 在“解关联VPC”对话框中，确认需要解关联的VPC信息，并输入“YES”。

步骤6 单击“确定”，完成解关联。

----结束

开启公网访问

当前仅支持共享公网入口，公网访问开启后将产生公网出流量费用（按实际使用量计费），请谨慎操作。

步骤1 登录Agentsphere控制台，在左侧导航栏中选择“网关实例”。

步骤2 在网关实例列表页面，待开启公网访问的网关实例所在行，单击操作列的“开启公网访问”。

步骤3 在“开启公网访问”对话框中，单击“确定”，开启公网访问。

----结束

关闭公网访问

⚠ 注意

关闭公网访问会导致关联的沙箱模板无法正常工作，所有通过公网入口的Agent服务将立即中断，当前活跃的公网连接将被断开，外部用户和系统将无法通过公网地址访问您的Agent，请谨慎操作。

步骤1 登录Agentsphere控制台，在左侧导航栏中选择“网关实例”。

步骤2 在网关实例列表页面，待关闭公网访问的网关实例所在行，单击操作列的“关闭公网访问”。

步骤3 网关实例是否关联目标?

- 是，执行**步骤4**。
- 否，执行**步骤5**。

步骤4 在“关闭公网访问”对话框中，输入“YES”。

版权所有 © 华为云计算技术有限公司

步骤5 单击“确定”，关闭公网访问。

----结束

修改私网访问

可以为网关实例新增关联VPC，或者解关联VPC。

步骤1 登录Agentsphere控制台，在左侧导航栏中选择“网关实例”。

步骤2 在网关实例列表页面，待修改私网访问的网关实例所在行，单击操作列的“修改私网访问”。

步骤3 在网关实例“基本信息”页签中，为网关实例新增关联或者解关联VPC。

具体操作请参见**关联VPC**和**解关联VPC**。

----结束

删除网关实例

当确认网关实例不需要继续使用时，可以根据需求随时释放网关实例。删除后无法恢复，请谨慎操作。

待删除的网关实例不能存在关联私网或者关联目标，如果存在，请提前解除关联。

步骤1 登录Agentsphere控制台，在左侧导航栏中选择“网关实例”。

步骤2 在网关实例列表页面，待删除网关实例所在行，单击操作列的“删除”。

步骤3 在“删除网关实例”对话框中，确认需要删除的网关实例信息，并输入“DELETE”。

步骤4 单击“确定”，完成删除。

----结束

相关文档

- 创建网关实例，请参见**创建网关实例**。
- 导出网关实例列表信息，请参见**导出网关实例列表信息**。

2.4 导出网关实例列表信息

操作场景

可以将当前账号下拥有的网关实例信息，以Excel文件的形式导出至本地。

当前支持导出全部实例的信息、导出选中部分实例的信息。导出的信息包括网关实例的名称、ID、状态、网关部署位置、私网访问、公网访问、关联目标、创建时间和描述等信息。

导出实例的信息

步骤1 登录Agentsphere控制台，在左侧导航栏中选择“网关实例”。

步骤2 在网关实例列表左上方，单击“导出”。

版权所有 © 华为云计算技术有限公司

1. 选择“导出全部数据到XLSX”：系统会将当前区域内所有网关实例的信息自动导出为Excel文件，并下载至本地。
2. 选择“导出已选中数据到XLSX”：系统会将当前区域内所选中的网关实例的信息自动导出为Excel文件，并下载至本地。

----结束

查看导出的实例信息

系统会将网关实例的信息自动导出为Excel文件，并下载至本地。

每一行数据对应一个网关实例的信息。

相关文档

- 创建网关实例，请参见**创建网关实例**。
- 管理网关实例，请参见**管理网关实例**。

版权所有 © 华为云计算技术有限公司

3 智能体身份

3.1 工作负载身份概述

工作负载身份是指AI智能体在运行、调用服务、访问资源、执行跨系统交互等工作负载场景中，用于标识自身身份、完成权限校验、实现安全交互的核心凭证体系，是保障智能体资源访问安全、权限精细化管控、交互行为可追溯的核心基础。

当前AgentSphere仅支持API Key类型的工作负载身份，在创建沙箱模板配置网关后系统将会自动创建。

当前暂不允许手动创建工作负载身份。由AgentSphere创建的API Key认证类型工作负载身份不支持修改和删除。

API Key 认证类型工作负载身份

API Key认证类型工作负载身份，是一种极简、高效的静态密钥认证身份模式，通过唯一的字符串密钥（API Key）作为智能体的身份标识与认证凭证。该模式无需复杂的授权流程与账号体系，仅需为智能体分配一组专属API Key，智能体在发起接口调用、资源访问请求时，通过请求头、参数携带API Key，服务端校验密钥合法性后即可完成身份认证与请求放行。

该身份模式部署简单、接入成本低、响应速度快，无需依赖独立的身份管理系统，适配绝大多数标准化接口调用场景。但核心短板是API Key多为静态固定凭证，一旦泄露易被滥用，且默认权限粒度较粗，难以实现精细化权限管控，通常仅支持密钥启停、黑白名单等基础管控能力，主要适用于内部调试、非核心资源调用、低风险轻量化交互场景。

3.2 查看工作负载身份

操作场景

创建沙箱模板成功后，您可以进入智能体身份模块查看系统自动创建的工作负载身份的详细信息。

版权所有 © 华为云计算技术有限公司

查看工作负载身份

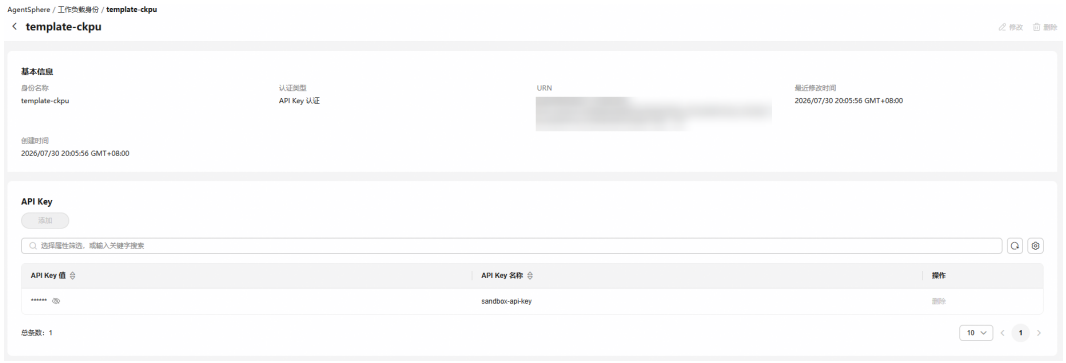
步骤1 登录AgentSphere控制台。

步骤2 在左侧导航窗格中，选择“工作负载身份”。

步骤3 在工作负载身份列表找到目标工作负载身份，单击目标工作负载身份名称。进入工作负载身份详情页面。

步骤4 工作负载身份详情页面可以查看到工作负载身份信息。

图 3-1 查看工作负载身份



----结束

版权所有 © 华为云计算技术有限公司