Agent 沙箱服务

产品简介

腾讯云

【联系我们】

我们致力于为您提供个性化的售前购买咨询服务，及相应的技术售后服务，任何问题请联系 4009100100或95716。

文档目录

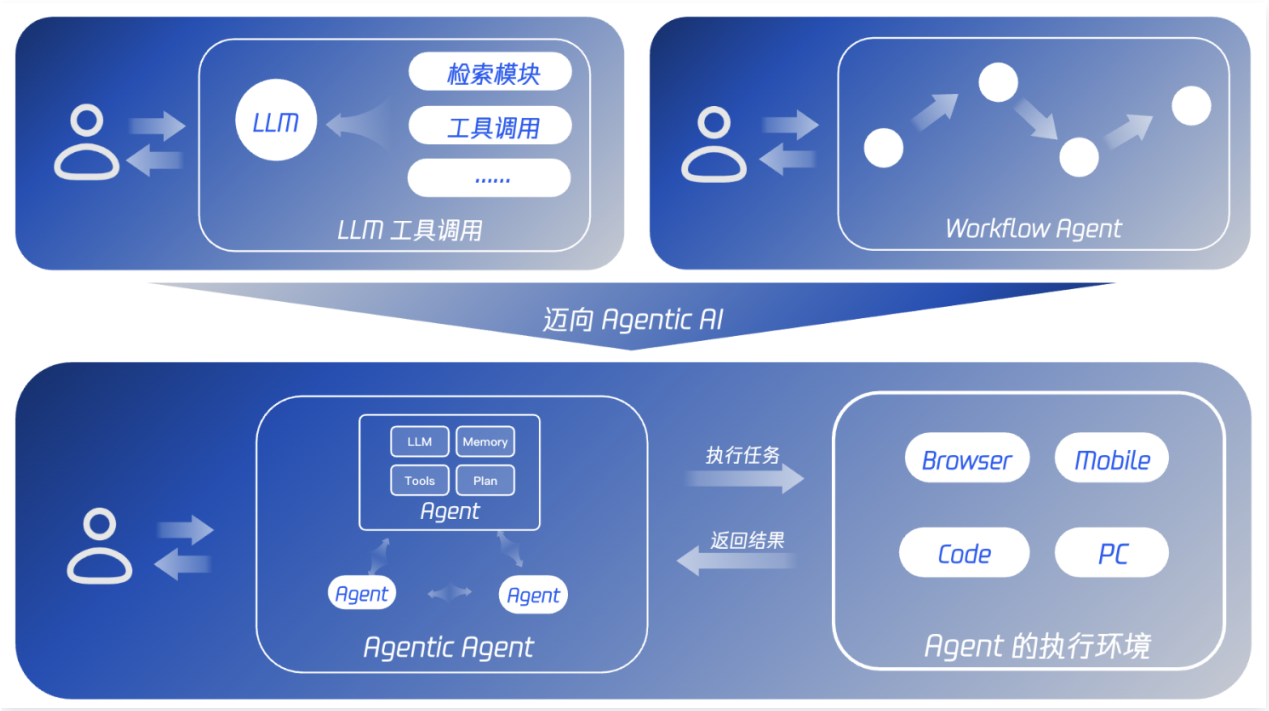
产品简介
产品概述

最近更新时间：2025-09-28 18:50:42

Agentic 时代来临，为什么必须为“数字员工”配备沙箱

在过去两年里，Agent 从实验室的探索逐渐走向生产环境，不再只是模型能力的展示，而是真实承担起企业中的“数字员工”角色。随着任务日益复杂，既要写代码、调用工具，又要操作浏览器、处理数据，对工作环境的要求也越来越高：

- 既要足够自由，支持多种场景的多样化任务操作。
- 又要足够安全，避免误删数据或越权操作。
- 还要具备弹性和并发能力，支撑大规模落地。



随着 Agent 从工具调用逐渐演进到真正的 Agentic Agent ——能自主规划、动态调用工具并与环境交互，对运行环境提出了更高标准。为了让这些数字员工安全、稳定地完成复杂任务，我们迫切需要一个数字世界的沙箱，为 Agent 提供专属办公环境。

正是基于这样的需求，Agent 沙箱应运而生。它为数字员工提供了一个安全隔离、极速启动的“虚拟办公环境”，让每个 Agent 都能像真实员工一样高效开展工作，同时解决了场景灵活、安全性与规模化并发三大核心挑战，成为 Agent 从研发走向生产的关键基座。

腾讯云 Agent 沙箱服务产品介绍

Agent 沙箱服务，支持毫秒级启动与数万实例并发，提供了 Code、Browser、Computer 等多种沙箱类型的托管服务，为 AI Agent 提供安全、隔离、高性能的执行环境。产品依托腾讯云强大的底层算力与调度能力，提供超

大规模的弹性资源供给，保障 Agent 在生产环境的稳定可用。

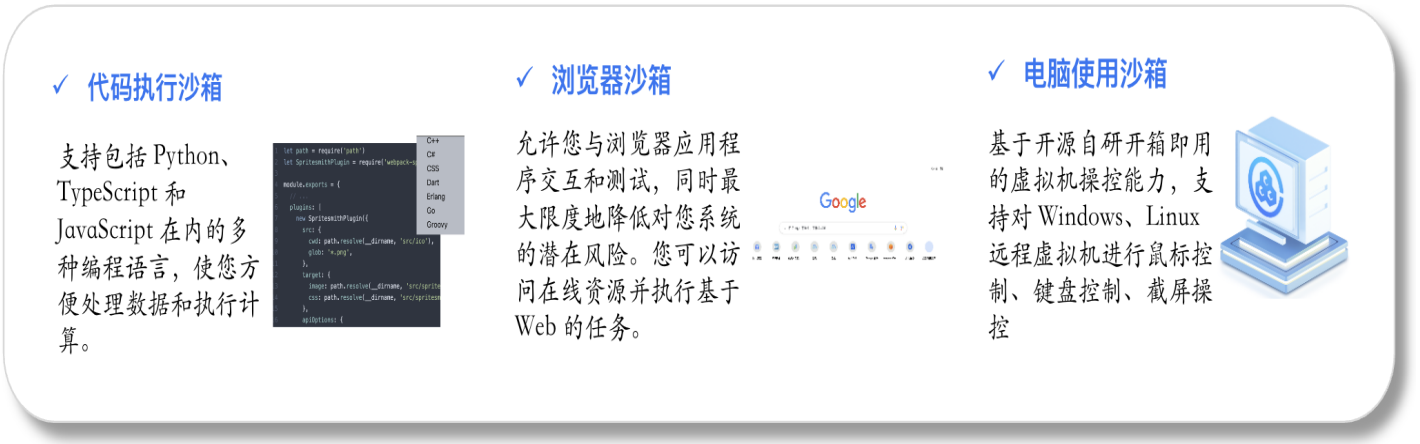
产品功能

Agent 沙箱服务在功能上涵盖两个维度：一是在沙箱类型上，支持代码沙箱、浏览器沙箱等多种形态；二是在沙箱使用上，提供完整的沙箱生命周期管理与内部操作能力。同时，产品还支持多样化的接入方式——不仅提供工程师 / Agent友好的 SDK、CLI、MCP、RESTful API，还兼容社区开源沙箱协议，方便用户灵活集成。

多种沙箱类型支持

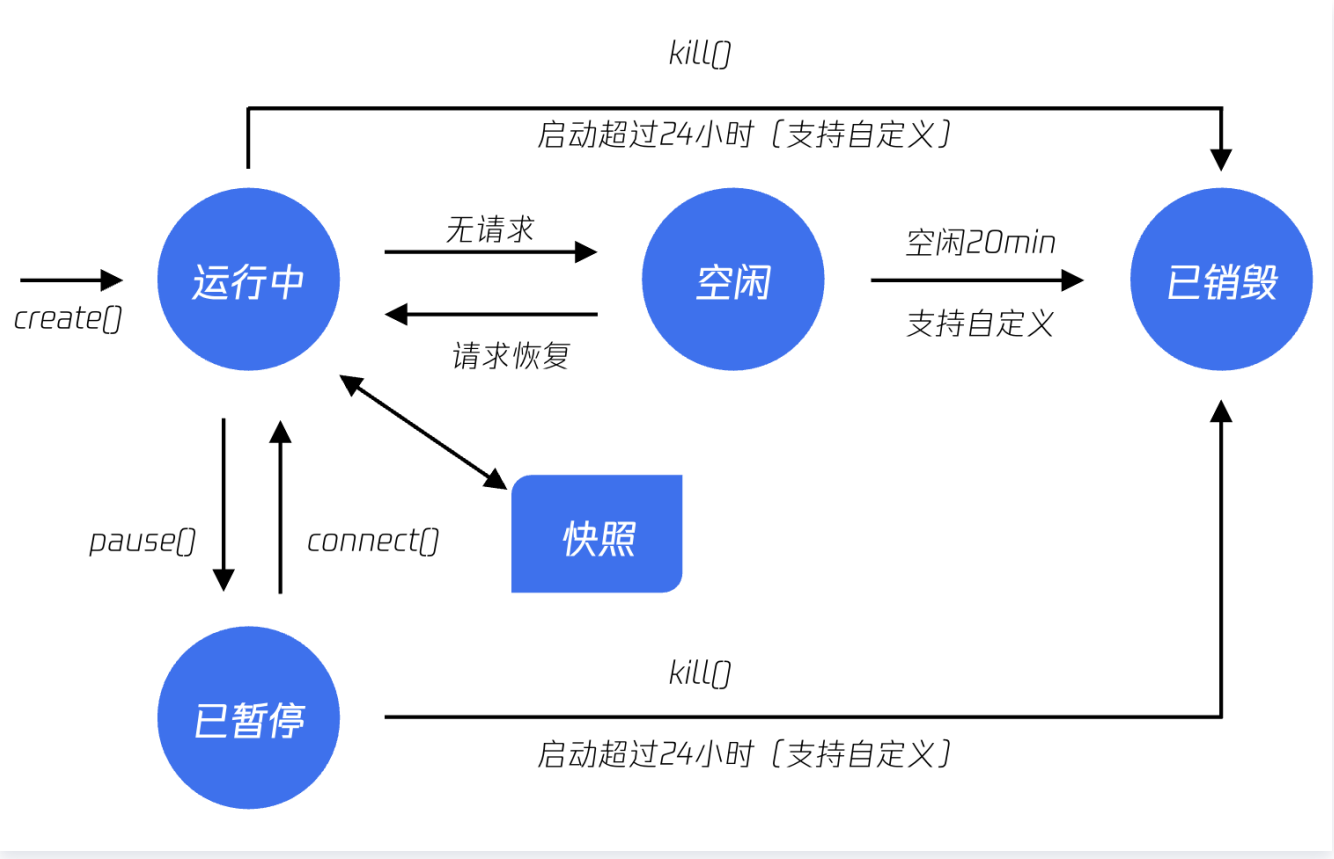
Agent 沙箱服务支持多种主流沙箱类型，并提供高度灵活的定制能力，满足智能体在不同场景下的运行需求。

- 代码执行沙箱：支持 Python、JavaScript 等多种编程语言，适用于数据处理、科学计算、图表生成、Vibe Coding 等安全代码运行场景。
- 浏览器沙箱：提供安全隔离的浏览器交互与测试环境，有效降低对本地系统的潜在风险，适用于 Deep Research、通用 Agent 等浏览器操作场景。
- 电脑沙箱（即将上线）：提供完整的远程虚拟机操控能力，支持对 Windows、Linux 系统进行鼠标控制、键盘输入、实时截屏等操作。
- 自定义沙箱（即将上线）：支持根据业务需求为智能体量身定制执行环境，包括：
  - 环境定制： 自由选择操作系统、预装软件、依赖库和工具链。
  - 资源配置： 按需灵活配置 CPU、内存、存储资源，提升资源利用率。

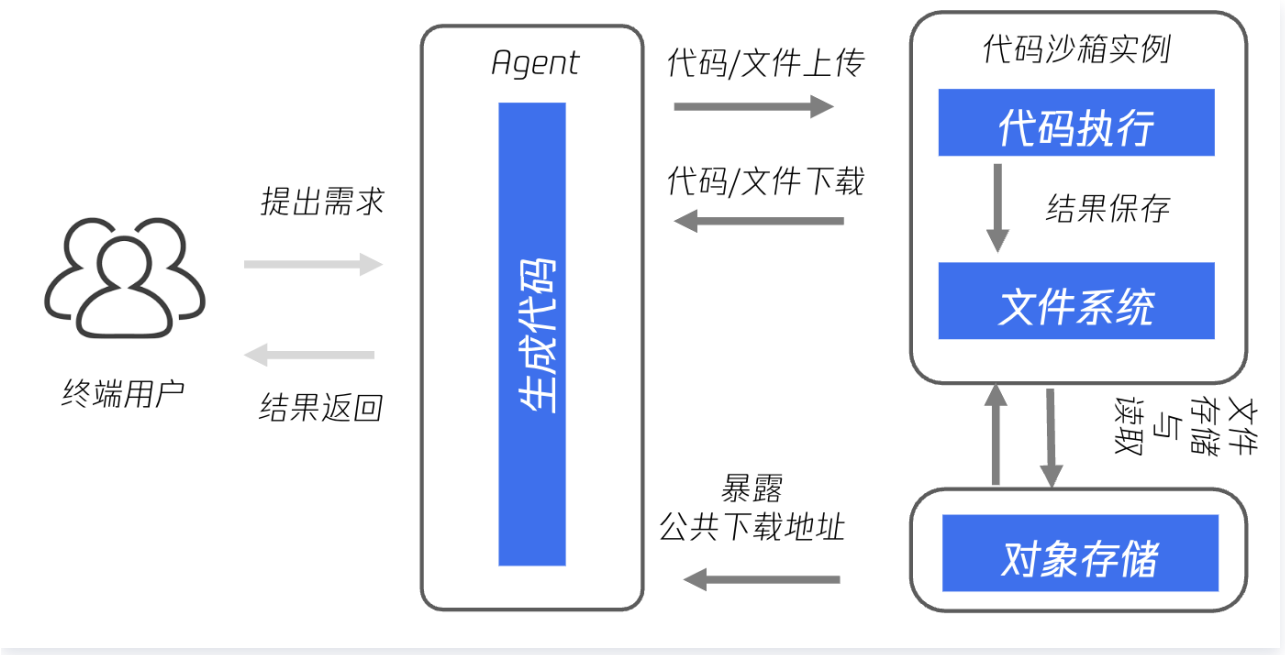


完善的沙箱操作能力

Agent 沙箱服务提供完整的沙箱操作能力，涵盖生命周期管理、内部文件操作以及细粒度的权限控制。
在沙箱的基础生命周期管理上，Agent 沙箱服务支持启动、超时删除、自动空闲回收和暂停等能力，不仅覆盖多样化业务场景，还能有效降低资源消耗，帮助用户实现更高效的使用体验。



在文件操作方面，沙箱支持目录和文件的创建、读取、编辑与搜索，为 Agent 提供完整的内部文件管理能力；同时支持外挂存储，对接外部对象存储，方便文件的上传、下载与共享。借此，Agent 可以在沙箱中直接处理数据或中间结果，并安全地与外部系统交互，大幅提升了业务场景下的灵活性和效率。



在权限管理方面，沙箱提供细粒度的角色控制能力，可灵活配置沙箱对腾讯云资源的访问范围，为 Agent 赋予安全且精细化的操作权限，从而在保障安全的同时释放更强大的云上操作能力。

备注：上述产品性能数据统计时间2025年8月，来自腾讯实验室测试结果。

应用场景

最近更新时间：2025-09-28 18:50:42

Vibe Coding

在 Vibe Coding 场景中，本地 IDE Copilot 模式虽然便捷，但存在严重安全风险：AI 生成的代码直接运行在本地环境，一旦包含 `rm -rf` 等危险指令，可能造成数据不可逆损失。
因此，逐步转向云端模式，如 AI 编程、前端页面生成、云端 IDE 等。AI 生成的代码在**云端沙箱环境**中运行，与本地隔离，既能避免入侵风险，又具备更强的资源弹性与可扩展性。

数据处理、PPT 制作等

通用 Agent 或企业办公 Agent 可以通过代码生成的方式完成数据清洗、数据分析、图表制作、甚至 PPT 制作。所有代码均在**云端沙箱**中运行，与本地彻底隔离，既安全可信，又具备弹性算力，真正成为企业数字员工的办公工具，让办公自动化更高效、更安心。

GUI Agent

在 GUI Agent 场景中，智能体成为具备全栈交互能力的虚拟人类。依托云端沙箱的安全隔离与弹性算力，它能够在不同环境中模拟人机操作：

- Browser Use Agent：在浏览器沙箱中执行网页打开、元素点击、数据采集与自动下单。
- Computer Use Agent：在虚拟桌面处理 Excel、生成 PPT、管理文件，实现办公自动化。
- Mobile Use Agent：在虚拟手机中操控 App，支持自动化测试与高并发业务操作。

GUI Agent 有效解决企业存量系统改造困难的问题，从“代码/API 驱动”演进为“操作驱动”，在云沙箱的助力下，覆盖 Web、桌面和移动端场景，成为真正的 虚拟数字员工。

强化学习场景

在 GUI-Agent 强化学习场景中，Agent 如学徒般，通过反复尝试、反馈和优化逐步掌握复杂界面操作。云端沙箱是核心执行环境，提供：

- 安全隔离：操作严格限制在沙箱内，避免影响真实系统与账号。
- 可观测性：完整记录操作轨迹、状态转移与奖励信号，支持精细化训练分析。
- 弹性扩展：支持大规模并发创建沙箱实例，支持模型训练，满足高强度算力需求。

依托沙箱，GUI-Agent 能在安全、可控、可扩展的环境中持续进化，最终具备自主完成复杂办公与操作任务的能力，真正成长为 “数字员工”。

产品优势

最近更新时间：2025-09-28 18:50:42

Agent 沙箱服务提供极致性能、强大的安全隔离能力、Serverless 的弹性供给以及业务友好的生态兼容：

极致性能

依托腾讯云百万核资源池，沙箱可实现100ms级启动速度，支持自定义规格与秒级弹性伸缩，轻松应对突发任务高峰。通过 Cube 安全沙箱、资源池化、镜像预热及快照等技术，确保毫秒级交付可用实例。

安全隔离

基于 Cube 等安全沙箱技术，提供内核级强隔离的运行环境，有效防止因 Agent 执行任意代码而导致的数据泄露与越权风险。提供内置的监控、审计和日志能力，确保整个执行过程透明、可控、可追溯。

弹性供给

基于 Serverless 架构实现“即开即用、用完即销毁”的体验。资源按需动态调度，用户无需预留和管理底层算力，既能满足大规模并发需求，又能在闲时自动回收，极大程度降低成本，做到真正的“即用即走”。

生态兼容

兼容主流社区开源沙箱协议，既方便开发者快速集成，也让已有业务可以低成本迁移到腾讯云环境中，实现与现有系统的丝滑衔接。

基本概念

最近更新时间：2025-09-28 18:50:42

沙箱工具

Agent 沙箱服务以沙箱工具为基础单元，管理资源调度和运行。由沙箱镜像和沙箱配置构成，包括：

- 沙箱镜像：支持代码、浏览器等类型的沙箱镜像。
- 沙箱配置：运行沙箱所需资源配置、网络策略、日志监控、持久化存储等。

沙箱实例

沙箱实例是实际执行沙箱镜像的安全且隔离的运行环境，具备独立的生命周期。沙箱工具支持运行多个沙箱实例。

沙箱快照

沙箱快照是沙箱实例某个具体的运行时快照，Agent 沙箱服务将默认提供 code 沙箱和浏览器沙箱的初始化沙箱快照，并实现资源预热，以实现沙箱实例的快速启动。

沙箱配额

最近更新时间：2025-09-28 18:50:42

沙箱服务的配额限制包括：创建沙箱的数量配额限制、沙箱回收时间限制。

沙箱数量配额

如果您需要更多的配额项数量，可通过 在线咨询 提出配额申请。

配额项	默认值	说明	是否可提配
沙箱工具数配额	10	单一主账号下，同时存在的最大沙箱工具数。	是
沙箱实例数配额	10	单一主账号下，可创建的沙箱实例总量上限（运行中+空闲中）。避免过度生成实例。	是

沙箱回收时间

配额项	默认值	说明	是否可提配
沙箱实例运行时长	5min	单个沙箱实例在创建后可存续的最长时间，超时将自动销毁。避免长期占用资源。	可在创建沙箱工具、沙箱实例时自行修改。