Agent Identity

用户指南

文档版本 01

发布日期 2026-11-06



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

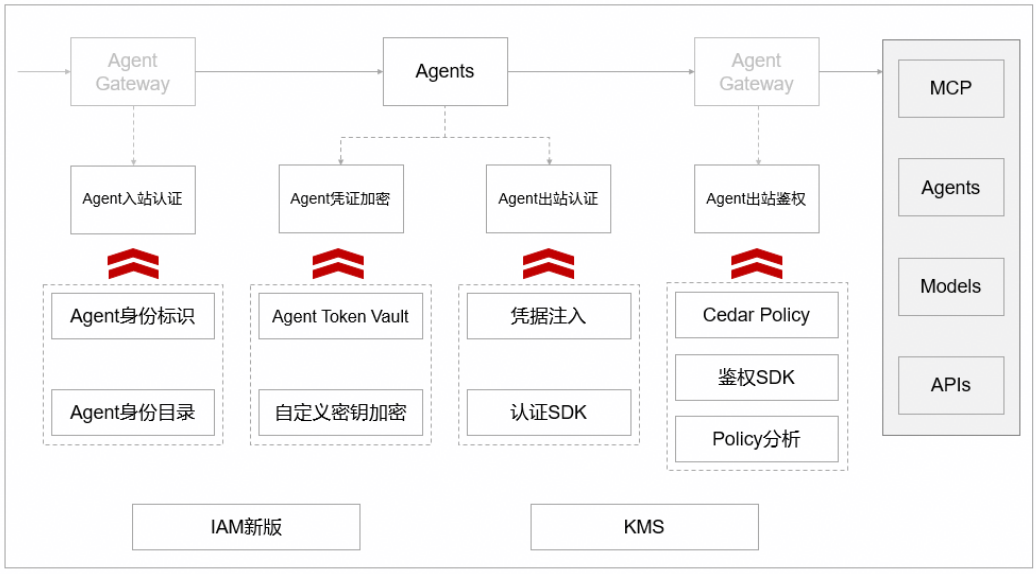
1 什么是智能体身份 1
2 产品优势 2
3 应用场景 3
4 权限管理 4
5 约束与限制 8
6 与其他服务的关系 9
7 基本概念 10

 版权所有 © 华为云计算技术有限公司

1 什么是智能体身份

华为云智能体身份（Agent Identity）专门为 Agent 提供安全身份标识、安全凭证管理、细粒度访问控制的云服务，让智能体能够安全地调用各类第三方外部工具和华为云服务资源。

图 1-1 Agent Identity 架构图



版权所有 © 华为云计算技术有限公司

2 产品优势

作为专门为Agent（智能体）打造的云原生安全与权限架构，Agent Identity的核心优势在于解决Agent在从“演示原型”迈向“企业级生产部署”时面临的身份混淆、凭据泄露与越权风险。

专为 Agent 打造的独立身份（Workload Identity）

- 摆脱硬编码与人机混用：为每个Agent（以及Agent调用的Tool/API）赋予独立、标准的“工作负载身份”，无需在代码中硬编码管理员凭据或混用员工个人账号。
- 隔离与最小权限：做到“一Agent一身份”，避免某个Agent被诱导攻击（Prompt Injection）后导致整个企业云资源失控。

安全的凭据托管与自动化

- 敏感凭据不落代码：集中托管Agent调用第三方SaaS、企业内部API或大模型服务时所需的API Key、OAuth Token、STSToken等凭据，并使用KMS加密后托管至CSMS。
- 无感刷新与自动注入：支持自动与凭证提供商（Credential Provider）进行交互，由Agent Identity自动管理出站访问凭据的申请、刷新与安全注入，Agent执行逻辑无需关注凭据维护。

精细化的访问控制

- 权限策略与业务代码解耦：将权限拦截逻辑（如“Agent不能调用超过$1000的退款API”）交由独立的Cedar Policy引擎（Agent网关）动态评估，无需修改Agent提示词或硬编码业务校验。
- 入参级精细控制（Fine-Grained）：不仅能控制Agent访问哪些第三方工具，还能对API的输入参数进行校验拦截（例如结合Cedar策略语言限制请求参数必须符合某些条件），防止Agent误解读指令导致误操作。

端到端审计与合规追溯

- 清晰的行为账本：完整记录“哪个用户在什么时间触发了哪个Agent、Agent使用了什么凭据、调用了什么工具、做出了什么决策”。
- 满足企业合规：对接云审计服务（CTS），上报操作记录，确保Agent的每一次操作均可溯源、可核查。

版权所有 © 华为云计算技术有限公司

3 应用场景

企业自动化智能体（无人值守场景）

场景描述：DevOps监控、数据同步、后台任务处理等自动化Agent，需要自主访问云资源或内部系统。

核心价值：为Agent赋予独立的工作负载身份，安全获取访问华为云服务（如OBS）或内部API的凭证，所有操作有清晰审计，避免使用共享密钥带来的权限失控和追溯困难问题。

企业内部助手 Agent（多人使用场景）

场景描述：企业内部的知识库问答、HR或IT助手Agent，服务众多员工，需要根据员工身份返回其有权限看到的数据。

核心价值：打通企业身份系统（如Okta、Entra ID等），实现用户身份透传。Agent拿着包含员工身份的令牌访问内部API网关，后端据此进行细粒度权限控制（如部门级、行级数据隔离），确保“员工只能看到自己的东西”。

代表用户访问第三方应用（委托授权场景）

场景描述：智能客服或个人助理Agent，需要代表用户读写其个人数据，例如查看文档、发送邮件等。

核心价值：由Agent Identity托管并实现复杂的OAuth 2.0委托授权流程，并使用凭据库（Token Vault）安全存储和自动刷新令牌。Agent代码全程不接触敏感的 Client Secret或OAuth Token，从根本上消除了凭证硬编码和泄露的风险，极大简化了开发复杂度。

版权所有 © 华为云计算技术有限公司

4 权限管理

如果您需要对华为云上购买的Agent Identity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Agent Identity服务的其它功能。

IAM是华为云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Agent Identity的使用权限，但是不希望他们拥有删除Agent Identity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Agent Identity，但是不允许删除Agent Identity资源的权限，控制他们对Agent Identity资源的使用范围。

身份策略权限管理

Agent Identity服务支持身份策略授权。如表1所示，包括了Agent Identity身份策略中的所有系统身份策略。

表 4-1 Agent Identity 系统身份策略

系统身份策略名称	描述	策略类别
AgentIdentityReadOnlyPolicy	访问智能体身份服务只读权限。	系统身份策略
AgentIdentityFullAccessPolicy	访问智能体身份服务所有权限。	系统身份策略
AgentIdentityServiceLinkedAgencyPolicy	访问智能体身份服务的服务关联委托策略。	系统身份策略

表4-2列出了Agent Identity常用操作与系统身份策略的授权关系，您可以参照该表选择合适的系统身份策略。

版权所有 © 华为云计算技术有限公司

表 4-2 常用操作与系统身份策略的关系

操作	AgentIdentityReadOnlyPolicy	AgentIdentityFullAccessPolicy	AgentIdentityServiceLinkedAgencyPolicy
查询工作负载身份列表	√	√	×
查询策略列表	√	√	×
查询API密钥凭证提供者列表	√	√	×
查询OAuth2凭证提供者列表	√	√	×
查询STS凭证提供者列表	√	√	×
查询策略引擎列表	√	√	×
通过OAuth2三方授权流程获取访问令牌	√	√	×
查询API密钥凭证提供者详情	√	√	×
查询工作负载身份授权配置	√	√	×
查询OAuth2凭证提供者详情	√	√	×
查询策略详情	√	√	×
获取与API密钥凭证提供者关联的API密钥	√	√	×
获取与API密钥凭证提供者关联的API密钥	√	√	×
从STS凭证提供者获取IAM临时凭证	√	√	×
查询STS凭证提供者详情	√	√	×
查询工作负载身份详情	√	√	×
查询策略引擎详情	√	√	×

版权所有 © 华为云计算技术有限公司

操作	AgentIdentityReadOnlyPolicy	AgentIdentityFullAccessPolicy	AgentIdentityServiceLinkedAgencyPolicy
查询策略引擎绑定列表	√	√	×
查询令牌保管库详情	√	√	×
创建API密钥凭证提供者	×	√	×
创建OAuth2凭证提供者	×	√	×
创建策略	×	√	×
创建STS凭证提供者	×	√	×
获取代理工作负载访问令牌	×	√	√
使用JWT令牌获取代表用户操作的代理工作负载访问令牌	×	√	√
使用用户ID获取代表用户操作的代理工作负载访问令牌	×	√	√
创建工作负载身份	×	√	×
删除API密钥凭证提供者	×	√	×
删除OAuth2凭证提供者	×	√	×
删除策略	×	√	×
删除STS凭证提供者	×	√	×
删除工作负载身份	×	√	×
更新API密钥凭证提供者	×	√	×
更新OAuth2凭证提供者	×	√	×
更新策略	×	√	×

版权所有 © 华为云计算技术有限公司

操作	AgentIdentityReadOnlyPolicy	AgentIdentityFullAccessPolicy	AgentIdentityServiceLinkedAgencyPolicy
更新STS凭证提供者	×	√	×
更新工作负载身份	×	√	×
创建策略引擎	×	√	×
删除策略引擎	×	√	×
更新策略引擎	×	√	×
更新令牌保管库配置	×	√	×
创建标签	×	√	×
更新标签	×	√	×
删除标签	×	√	×
查询标签	√	√	×

版权所有 © 华为云计算技术有限公司

5 约束与限制

表 5-1 约束与限制

配额项	值	可调整	说明
工作负载身份	1,000	否	当前区域的账号中可创建的工作负载身份的最大数量。
OAuth2认证类型的出站身份	50	否	当前区域的账号中可创建的用于出站身份的OAuth2凭证提供者的最大数量。
API key认证类型的出站身份	50	否	当前区域的账号中可创建的用于出站身份的API密钥凭证提供者的最大数量。
IAM认证类型的出站身份	50	否	当前区域的账号中可创建的用于出站身份的STS凭证提供者的最大数量。
每个账号、每个region下的策略引擎个数	1,000	否	每个账号每个区域的策略引擎数量。
每个策略引擎下的策略个数	1,000	否	每个策略引擎的策略数量。
单策略大小	10 KB	否	单个策略的最大大小。
所有策略总大小	200 KB	否	策略引擎中每个资源的所有策略的总大小。
Cedar schema大小	400 KB	否	每个策略引擎的Cedar schema大小。此限制适用于与策略引擎关联的所有网关的所有工具生成的合并Cedar schema。schema大小随工具数量及其输入参数的复杂性增长，而不仅仅是工具计数。如果schema超过此限制，请考虑为不同网关使用单独的策略引擎或删除未使用的工具。

版权所有 © 华为云计算技术有限公司

6 与其他服务的关系

Agent Identity需要与其他云服务协同工作，各服务之间的关系如表6-1所示。

表 6-1 Agent Identity 与其他云服务的关系

相关服务	交互功能
统一身份认证服务（IAM）	Agent Identity使用IAM实现用户身份认证和权限管理。通过IAM，企业可以为员工设置不同的Agent Identity访问权限，实现权限隔离和精细化管控。
云审计服务（CTS）	Agent Identity将操作记录上报至CTS，包括工作负载身份创建、凭证申请、策略执行等关键操作，确保Agent的每一次操作均可溯源、可核查，满足企业合规要求。
凭据管理服务（CSMS）	Agent Identity使用CSMS安全存储敏感凭据（API Key、OAuth Token、刷新令牌等），并通过KMS加密保护，确保凭据不暴露在Agent代码或运行环境中。
密钥管理服务（KMS）	KMS为CSMS中的凭据提供加密密钥，保障凭据的机密性和完整性。
安全令牌服务（STS）	Agent Identity通过STS为Agent颁发临时访问凭证（STS Token），支持最小权限原则和凭证自动过期，降低长期凭证泄露风险。

版权所有 © 华为云计算技术有限公司

7 基本概念

工作负载身份

工作负载身份（workload Identity）是专门为AI Agent 打造的“数字身份证”。它为Agent赋予独立的安全身份，解决的是Agent“从哪来（入站合法性）、能干什么（出站凭据与权限）、出了事找谁（可追溯性）”的根本问题。它是实现企业级、生产可用的Agentic AI架构中最底层的安全基石。Agent Identity为Agent颁发全局唯一的身份标识URN，格式为agentIdentity:<region>:<account-id>:workloadIdentity:workloadIdentityDirectory/<workload-directory-id>/<workload-identity-name>）。并关联Agent的入站认证类型（JWT、IAM、API Key），在用户访问Agent时，使用工作负载配置的认证类型进行认证。

工作负载访问令牌

工作负载访问令牌（workload Access Token，简称WAT）是专门为Agent工作负载身份颁发的临时访问凭据，其中包含了工作负载身份和用户的身份信息，用于从凭证库（Token Vault）中换取出站访问凭证进而访问第三方外部工具。

凭证库

凭证库（Token Vault）负责加密存储（KMS）和管理外部资源的凭证，包括OAuth 2.0访问令牌、刷新令牌、客户端凭证（client credentials）以及API Keys。这些凭证由凭证提供商（Credential Provider）在认证流程完成后生成并安全存储到Token Vault，确保敏感信息不暴露在Agent代码或运行环境中。Token Vault通过严格的访问控制机制，仅允许持有有效WAT的Agent访问凭证。

凭证提供商

凭证提供商（Credential Provider）负责管理Agent访问外部资源认证配置，内置支持Google、GitHub、Slack、Salesforce等主流服务的预配置端点，也允许通过自定义OAuth 2.0配置扩展到任意兼容服务器。该组件负责编排完整的认证流程（包括用户同意、授权码交换等），从而让Agent开发者无需手动实现复杂OAuth逻辑或硬编码凭证。认证成功后，生成的短期访问令牌、刷新令牌或API keys将自动存储到Token Vault中，并通过SDK注解（如 @requires_access_token）安全注入Agent代码，实现自动刷新和最小权限访问。

 版权所有 © 华为云计算技术有限公司