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 通过 IAM 授予使用 Agent Identity 的权限 1
1.1 通过 IAM 身份策略授予使用 Agent Identity 的权限 1
2 管理工作负载身份 4
2.1 工作负载身份概述 4
2.2 创建工作负载身份 6
2.3 查看工作负载身份 11
2.4 修改工作负载身份 12
2.5 删除工作负载身份 13
3 管理出站身份 15
3.1 出站身份概述 15
3.2 创建出站身份 16
3.3 修改出站身份 19
3.4 删除出站身份 20
3.5 为出站身份设置标签 21
4 管理策略集 23
4.1 策略集概述 23
4.2 创建策略集 24
4.3 创建策略 24
4.4 编辑策略 27
4.5 将实例绑定至策略集 28
4.6 将实例从策略集解绑 29
4.7 删除策略集 29
4.8 删除策略 30
4.9 为策略集设置标签 31
5 管理凭证库 33
5.1 凭证库概述 33
5.2 为凭证库设置标签 33

 版权所有 © 华为云计算技术有限公司

1 通过 IAM 授予使用 Agent Identity 的权限

1.1 通过 IAM 身份策略授予使用 Agent Identity 的权限

如果您需要对您所拥有的Agent Identity进行身份策略的权限管理，您可以使用**统一身份认证服务**（Identity and Access Management，简称IAM），通过IAM，您可以：

- 根据企业的业务组织，在您的账号中，给企业中不同职能部门的员工创建用户或用户组，让员工拥有唯一安全凭证，并使用Agent Identity资源。
- 根据企业用户的职能，设置不同的访问权限，以达到用户之间的权限隔离。
- 将Agent Identity资源委托给更专业、高效的其他账号或者云服务，这些账号或者云服务可以根据权限进行代运维。

如果账号已经能满足您的要求，您可以跳过本章节，不影响您使用Agent Identity服务的其他功能。

本章节为您介绍使用身份策略的授权方法，操作流程如**图1-1**所示。

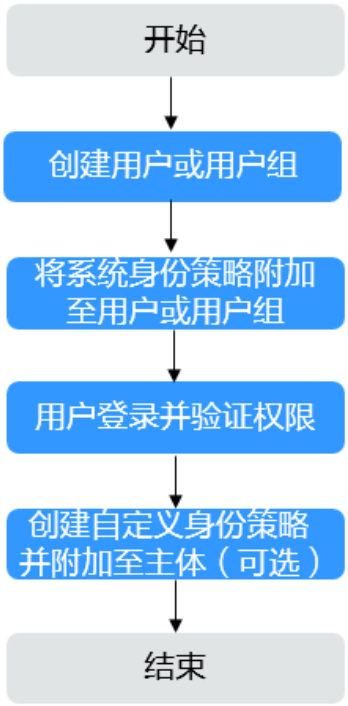
前提条件

在授权操作前，请您了解可以添加的Agent Identity权限，并结合实际需求进行选择。Agent Identity支持的系统身份策略，请参见**权限管理**。若您需要对除Agent Identity之外的其他服务授权，IAM支持服务的所有权限请参见**授权参考**。

版权所有 © 华为云计算技术有限公司

示例流程

图 1-1 给用户授予 Agent Identity 权限流程



1. **创建用户**或**创建用户组**

   在IAM控制台创建用户或用户组。

2. **将系统身份策略附加至用户或用户组**

   为用户或用户组授予Agent Identity只读权限的系统身份策略“AgentIdentityReadOnlyPolicy”，或将身份策略附加至用户或用户组。

3. **用户登录**并验证权限

   使用已授权的用户登录控制台，验证权限：

   - 在“服务列表”中选择Agent Identity，进入Agent Identity主界面，单击右上角“创建工作负载身份”，尝试创建工作负载身份，如果无法创建工作负载身份（假设当前权限仅包含AgentIdentityReadOnlyPolicy），表示“AgentIdentityReadOnlyPolicy”已生效。
   - 在“服务列表”中选择除Agent Identity外（假设当前策略仅包含AgentIdentityReadOnlyPolicy）的任一服务，若提示权限不足，表示“AgentIdentityReadOnlyPolicy”已生效。

Agent Identity 自定义身份策略样例

如果系统预置的Agent Identity系统身份策略，不满足您的授权要求，可以创建自定义身份策略。自定义身份策略中可以添加的授权项（Action）请参考**身份策略授权参考**。

目前华为云支持以下两种方式创建自定义身份策略：

- 可视化视图创建自定义身份策略：无需了解策略语法，按可视化视图导航栏选择云服务、操作、资源、条件等策略内容，可自动生成策略。

版权所有 © 华为云计算技术有限公司

- JSON视图创建自定义身份策略：可以在选择策略模板后，根据具体需求编辑策略内容；也可以直接在编辑框内编写JSON格式的策略内容。

具体创建步骤请参见：**创建自定义身份策略并附加至主体**。

您可以在创建自定义身份策略时，通过资源类型（Resource）元素来选择特定资源，以及条件键（Condition）元素来控制策略何时生效。支持的资源类型和条件键请参考**身份策略授权参考**。下面为您介绍常用的Agent Identity自定义身份策略样例。

示例：授权创建和删除工作负载身份的权限。

```
{
  "Version": "5.0",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "agentIdentity::createWorkloadIdentity",
        "agentIdentity::deleteWorkloadIdentity",
        "csms:secret:create",
        "csms:secret:delete",
        "kms:cmk:createDataKey"
      ]
    }
  ]
}
```


版权所有 © 华为云计算技术有限公司

2 管理工作负载身份

2.1 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。根据认证机制、凭证形态、权限管控粒度与适用场景的差异，华为云工作负载身份主要分为**IAM认证、OAuth 2.0认证、API Key认证、无认证**四种核心类型，四种身份模式的安全等级、运行机制、适用场景差异显著，共同覆盖了智能体从公开测试、轻量化调用到企业级合规部署的全场景需求。

IAM 认证类型工作负载身份概述

IAM认证类型的工作负载身份，是基于企业级身份权限管理体系构建的标准化、精细化身份凭证，属于高安全等级的官方认证模式。该模式下，智能体被视为独立的工作负载主体，在IAM系统中完成专属身份注册、账号创建与权限绑定，核心依托IAM的账号体系、角色权限策略、资源访问规则实现身份认证与授权管控。

其核心特性是支持最小权限原则落地，管理员可针对单个智能体或智能体分组，精准配置资源访问范围、操作权限、访问时段等精细化策略，同时支持身份生命周期全流程管理，包括身份创建、权限变更、过期失效、注销回收等。认证过程依托加密签名、令牌校验、会话管控等机制，且全程可记录审计日志，能够精准追溯智能体的每一次资源访问、接口调用行为，广泛适用于企业生产环境、涉密业务、核心数据交互等高合规、高安全要求的智能体工作负载场景。

OAuth 2.0 认证类型工作负载身份

OAuth 2.0认证类型的工作负载身份，是基于OAuth 2.0开放授权协议构建的轻量化、第三方授权身份模式，核心解决智能体跨平台、跨系统、跨服务的授权访问问题。该模式并非依靠固定账号密码认证，而是通过授权码、客户端凭证、令牌（Token）流转的方式，实现智能体与目标服务之间的临时授权交互。

在该身份体系下，智能体作为客户端主体，向授权服务器发起授权申请，通过合法校验后获取短期有效的访问令牌，凭借令牌完成资源调用与身份校验。其核心优势是无需暴露核心账号凭证，支持授权范围自定义、令牌有效期可控，兼顾安全性与灵活性，主要适用于智能体对接第三方开放平台、跨系统协同调用、轻量化对外服务等需要临时授权、按需开放权限的工作负载场景，是开放式生态下智能体交互的主流身份模式。

 版权所有 © 华为云计算技术有限公司

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。

无认证类型工作负载身份

无认证类型工作负载身份是指智能体在运行交互过程中，不依托任何身份凭证、认证协议与权限校验机制的极简运行模式。该模式下，智能体无需注册身份、无需配置密钥、无需申请授权，所有对外请求、资源访问、服务调用均无需经过身份校验与权限核验，服务端默认放行所有来自该智能体的交互请求。

该模式的核心特点是零接入成本、零认证耗时、部署极致简单，完全消除了身份认证带来的开发与运维成本。但安全性极低，无任何权限管控、访问溯源、风险防护能力，任何获取请求地址的主体均可模拟智能体发起请求，仅适用于本地测试、内网隔离环境调试、公开演示、临时原型验证等无安全风险、无需合规管控的非生产工作负载场景。

各类工作负载身份的区别

四种工作负载身份在安全等级、认证机制、权限管控、运维成本、适用场景等核心维度存在区别，具体区别如表2-1所示。

表 2-1 各类工作负载身份的区别

对比维度	IAM认证	OAuth 2.0认证	API Key认证	无认证
安全等级	安全等级最高，依托完整的身份权限体系、审计追溯、动态权限管控，可抵御身份伪造、越权访问、凭证泄露等各类风险。	较IAM认证次之，通过动态短期令牌、按需授权降低凭证泄露风险，安全性适中。	安全等级较低，静态密钥存在泄露、复用、滥用风险。	无任何安全防护，安全等级最低，存在极高的非法访问风险。
认证机制	基于专属账号体系与加密校验，依托后台权限策略动态核验身份。	基于标准化授权协议，通过令牌动态流转、临时授权完成认证。	静态密钥一对一校验，认证逻辑简单固定。	无任何校验机制，直接放行所有请求。

版权所有 © 华为云计算技术有限公司

对比维度	IAM认证	OAuth 2.0认证	API Key认证	无认证
权限管控能力	支持精细化、颗粒化权限管控，可精准限定访问资源、操作权限、访问时段，支持角色分组、权限分级与动态调整。	支持按需授权、限定令牌权限范围，可灵活调整临时授权边界。	仅支持全局权限或基础黑白名单管控，无法实现精细化权限拆分。	无任何权限管控能力，无访问限制。
运维与接入成本	需搭建、维护身份管理体系，配置权限策略、审计日志，接入流程复杂，运维成本最高。	需对接授权服务器、配置授权规则、管控令牌生命周期，接入与运维成本中等。	无需复杂部署，仅需分配与启停密钥，接入简单、运维成本极低。	零配置、零运维，接入成本最低。
适用场景差异	用于企业生产环境、核心业务、涉密数据交互等高合规、高安全场景。	适用于跨平台、第三方对接、临时授权的开放式交互场景。	适用于内部非核心业务调用、轻量化固定交互场景。	适用于本地测试、原型验证、内网调试等非生产、无安全风险场景。

2.2 创建工作负载身份

操作场景

工作负载身份可为AI智能体等程序载体提供独立可信的机器身份，实现消除静态密钥风险、精细化权限隔离、全链路操作审计、多环境统一身份管控能力。若业务存在智能体承接用户交互或后台自动调度，程序需访问云资源、内部接口、第三方工具，且有安全合规治理需求时，需创建工作负载身份并配套身份提供商，搭建可信访问链路。

原理说明

创建工作负载身份会在IAM中注册专属机器实体并分配唯一标识，通过身份提供商建立与IAM的信任委托；负载校验身份通过后自动获取可轮换短期凭证，依靠该身份完成入站准入校验、出站资源访问管控，所有操作携带身份标识留存日志，实现身份、权限、凭证一体化闭环治理。

约束与限制

- 当前区域的账号中可创建的工作负载身份的最大数量为1000个。
- 创建API Key认证类型的工作负载身份，最多可以添加10个API Key。

版权所有 © 华为云计算技术有限公司

创建 IAM 认证类型的工作负载身份

步骤1 登录**智能体身份控制台**。

步骤2 在左侧导航窗格中，选择“工作负载身份”。单击右上角“创建工作负载身份”。

步骤3 输入“身份名称”。身份名称只能包含英文字母、数字或特殊字符(_-)，长度不能超过56个字符。

步骤4 选择“入站身份认证”。此处选择“IAM认证”。将IAM身份配置为入站身份认证，以验证调用者的身份。

步骤5 （可选）为工作负载身份添加标签。

标签以键值对的形式表示，用于标识工作负载身份，便于对工作负载身份进行分类和搜索。此处的标签仅用于工作负载身份的过滤和管理。一个存储库最多添加20个标签。

如果您的组织设定了智能体身份的相关**标签策略**，则需按照标签策略规则为存储库添加标签。标签如果不符合标签策略的规则，则可能会导致工作负载身份创建失败，请联系组织管理员了解标签策略详情。

标签的设置说明如**表2-2**所示。

表 2-2 标签说明

参数	说明	举例
键	输入标签的键，同一个工作负载身份标签的键不能重复。键可以自定义，也可以选择预先在标签服务（TMS）创建好的标签的键。 键命名规则如下： • 长度不能超过128个字符。 • 可以包含任意语种的字母、数字和空格，以及_.:/=+-@字符，但首尾不能包含空格，且不能以_sys_开头。	Key_0001
值	输入标签的值，标签的值可以重复，并且可以为空。 标签值的命名规则如下： • 长度不能超过255个字符。 • 可以包含任意语种的字母、数字和空格，以及_.:/=+-@&字符。	Value_0001

步骤6 单击“创建”，创建成功的工作负载身份将会出现在工作负载身份列表。

----结束

创建 OAuth 2.0 认证类型的工作负载身份

步骤1 登录**智能体身份控制台**。

步骤2 在左侧导航窗格中，选择“工作负载身份”。单击右上角“创建工作负载身份”。

步骤3 输入“身份名称”。身份名称只能包含英文字母、数字或特殊字符(_-)，长度不能超过56个字符。

版权所有 © 华为云计算技术有限公司

步骤4 选择“入站身份认证”。此处选择“OAuth 2.0认证”。将JWT（如OAuth令牌）配置为入站身份认证，以验证传入的令牌签名和范围。

步骤5 根据参数说明表格，完成创建OAuth 2.0认证类型工作负载身份的参数设置。

表 2-3 参数说明

参数	示例	说明
Discovery URL	https://{base URL}/.well-known/openid-configuration	输入您的身份提供商（例如 Okta、Cognito等）提供的Discovery URL，该URL通常可在该提供商的文档中找到。 URL格式如下：*https://{base URL}/.well-known/openid-configuration*，其中*base URL*由企业IdP定义，如Google提供的Openid-configuration为https://accounts.google.com/.well-known/openid-configuration，Cognito的URL格式为https://cognito-idp.*region*.amazonaws.com/*userPoolId*/.well-known/openid-configuration，Okta的URL格式为https://*OKTA_DOMAIN*/.well-known/openid-configuration。
允许的受众	-	这用于认证为OAuth 2.0指定的受众是否在智能体身份运行中指定的受众匹配或为其子集。
允许的客户端	-	这用于认证为OAuth 2.0指定的客户端标识符是否被允许访问智能体身份。
允许的范围	-	仅当令牌包含此处配置的至少一个必须范围时才允许访问。
自定义声明	-	仅当令牌中的特定声明与预定义字符串值相匹配时才允许访问。

步骤6 （可选）为工作负载身份添加标签。

标签以键值对的形式表示，用于标识工作负载身份，便于对工作负载身份进行分类和搜索。此处的标签仅用于工作负载身份的过滤和管理。一个存储库最多添加20个标签。

如果您的组织设定了智能体身份的相关**标签策略**，则需按照标签策略规则为存储库添加标签。标签如果不符合标签策略的规则，则可能会导致工作负载身份创建失败，请联系组织管理员了解标签策略详情。

标签的设置说明如**表2-4**所示。

 版权所有 © 华为云计算技术有限公司

表 2-4 标签说明

参数	说明	举例
键	输入标签的键，同一个工作负载身份标签的键不能重复。键可以自定义，也可以选择预先在标签服务（TMS）创建好的标签的键。 键命名规则如下： • 长度不能超过128个字符。 • 可以包含任意语种的字母、数字和空格，以及_.:/=+-@字符，但首尾不能包含空格，且不能以_sys_开头。	Key_0001
值	输入标签的值，标签的值可以重复，并且可以为空。 标签值的命名规则如下： • 长度不能超过255个字符。 • 可以包含任意语种的字母、数字和空格，以及_.:/=+-@&字符。	Value_0001

步骤7 单击“创建”，创建成功的工作负载身份将会出现在工作负载身份列表。

----结束

创建 API Key 认证类型的工作负载身份

步骤1 登录**智能体身份控制台**。

步骤2 在左侧导航窗格中，选择“工作负载身份”。单击右上角“创建工作负载身份”。

步骤3 输入“身份名称”。身份名称只能包含英文字母、数字或特殊字符(_-)，长度不能超过56个字符。

步骤4 选择“入站身份认证”。此处选择“API Key认证”。将预设的密钥对（键和值）配置为入站身份认证，以验证请求中携带的密钥合法性。

步骤5 单击“添加API Key”，输入API Key的值和名称。如不添加API Key，系统将默认生成一条API Key。最多可以添加10个API Key。

步骤6 （可选）为工作负载身份添加标签。

标签以键值对的形式表示，用于标识工作负载身份，便于对工作负载身份进行分类和搜索。此处的标签仅用于工作负载身份的过滤和管理。一个存储库最多添加20个标签。

如果您的组织设定了智能体身份的相关**标签策略**，则需按照标签策略规则为存储库添加标签。标签如果不符合标签策略的规则，则可能会导致工作负载身份创建失败，请联系组织管理员了解标签策略详情。

标签的设置说明如**表2-5**所示。

 版权所有 © 华为云计算技术有限公司

表 2-5 标签说明

参数	说明	举例
键	输入标签的键，同一个工作负载身份标签的键不能重复。键可以自定义，也可以选择预先在标签服务（TMS）创建好的标签的键。 键命名规则如下： ● 长度不能超过128个字符。 ● 可以包含任意语种的字母、数字和空格，以及_.:/=+-@字符，但首尾不能包含空格，且不能以_sys_开头。	Key_0001
值	输入标签的值，标签的值可以重复，并且可以为空。 标签值的命名规则如下： ● 长度不能超过255个字符。 ● 可以包含任意语种的字母、数字和空格，以及_.:/=+-@&字符。	Value_0001

步骤7 单击“创建”，创建成功的工作负载身份将会出现在工作负载身份列表。

----结束

创建无认证类型的工作负载身份

步骤1 登录**智能体身份控制台**。

步骤2 在左侧导航窗格中，选择“工作负载身份”。单击右上角“创建工作负载身份”。

步骤3 输入“身份名称”。身份名称只能包含英文字母、数字或特殊字符(_-)，长度不能超过56个字符。

步骤4 选择“入站身份认证”。此处选择“无认证”。无需对入站身份进行认证，允许匿名访问资源。

步骤5 （可选）为工作负载身份添加标签。

标签以键值对的形式表示，用于标识工作负载身份，便于对工作负载身份进行分类和搜索。此处的标签仅用于工作负载身份的过滤和管理。一个存储库最多添加20个标签。

如果您的组织设定了智能体身份的相关**标签策略**，则需按照标签策略规则为存储库添加标签。标签如果不符合标签策略的规则，则可能会导致工作负载身份创建失败，请联系组织管理员了解标签策略详情。

标签的设置说明如**表2-6**所示。

 版权所有 © 华为云计算技术有限公司

表 2-6 标签说明

参数	说明	举例
键	输入标签的键，同一个工作负载身份标签的键不能重复。键可以自定义，也可以选择预先在标签服务（TMS）创建好的标签的键。 键命名规则如下： ● 长度不能超过128个字符。 ● 可以包含任意语种的字母、数字和空格，以及_.:/=+-@字符，但首尾不能包含空格，且不能以_sys_开头。	Key_0001
值	输入标签的值，标签的值可以重复，并且可以为空。 标签值的命名规则如下： ● 长度不能超过255个字符。 ● 可以包含任意语种的字母、数字和空格，以及_.:/=+-@&字符。	Value_0001

步骤6 单击“创建”，创建成功的工作负载身份将会出现在工作负载身份列表。

----结束

2.3 查看工作负载身份

操作场景

工作负载身份创建成功后，您可以进入工作负载身份详情中查看工作负载身份的详细信息。

查看工作负载身份

步骤1 登录**智能体身份控制台**。

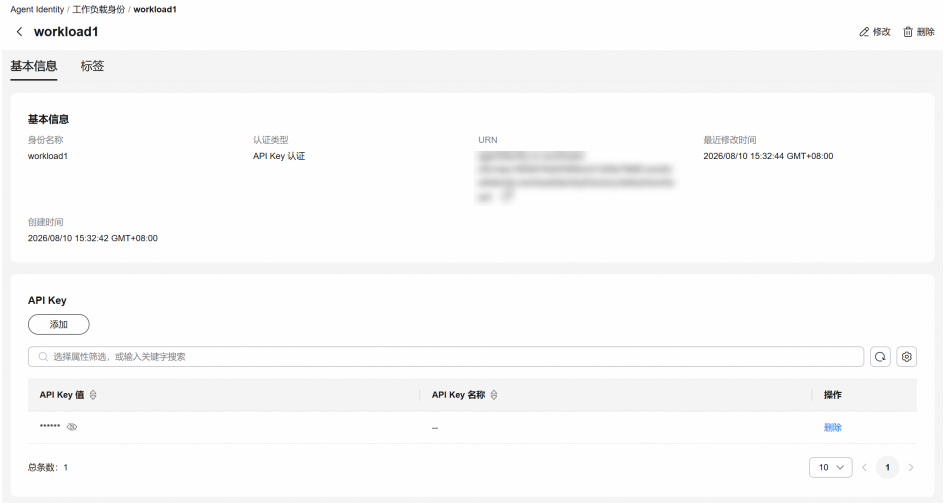
步骤2 在左侧导航窗格中，选择“工作负载身份”。

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。

 版权所有 © 华为云计算技术有限公司

图 2-1 查看工作负载身份



----结束

2.4 修改工作负载身份

操作场景

当原有业务场景发生变化时，可以根据需要修改工作负载身份。修改工作负载身份后会变更智能体鉴权逻辑，可能会导致访问不可用，请谨慎操作。

约束与限制

仅API Key认证类型和OAuth 2.0认证类型的工作负载身份支持修改。

修改 API Key 认证类型的工作负载身份

步骤1 登录**智能体身份控制台**。

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“操作”列下的“修改”。

步骤4 根据需要修改API Key值和API Key名称。

图 2-2 修改 API Key



 版权所有 © 华为云计算技术有限公司

步骤5 单击“确定”。

----结束

修改 OAuth 2.0 认证类型的工作负载身份

步骤1 登录**智能体身份控制台**。

步骤2 在工作负载身份列表找到目标工作负载身份，单击“操作”列下的“修改”。

步骤3 请根据业务参考**表2-3**修改对应的参数。

步骤4 单击“确定”。

----结束

2.5 删除工作负载身份

操作场景

在智能体平台日常权限治理中，针对已下线、停用、废弃的智能体，需执行工作负载身份删除操作。业务迭代下线、智能体版本升级替换、临时测试智能体任务结束后，对应的旧版工作负载身份会处于闲置状态，长期留存易造成身份台账冗余、权限边界混乱。

闲置的无效身份存在被复用、非法调用的安全风险，违反权限最小化治理规范。本次操作适用于所有无业务承载、不再参与任务调度与权限校验的智能体身份。删除操作仅清空智能体的平台授信身份及关联授权策略，不影响智能体程序与业务日志数据，可有效清理冗余身份资源，回收闲置权限，规避安全隐患，保障平台身份管理合规、可控、可审计。

删除工作负载身份

步骤1 登录**智能体身份控制台**。

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“操作”列下的“删除”。

步骤4 确认信息无误，输入“DELETE”。单击“确定”。

图 2-3 删除工作负载身份



 版权所有 © 华为云计算技术有限公司

步骤5 删除完成后，如在工作负载身份列表未查看到目标工作负载身份，表示删除操作执行成功。

----结束

 版权所有 © 华为云计算技术有限公司

3 管理出站身份

3.1 出站身份概述

出站身份（Outbound Identity）是智能体身份体系中与入站身份相对的一类身份形态。**入站身份**解决“谁来调用Agent”的认证与授权问题；**出站身份**则解决“Agent代表谁、以什么凭据去访问下游资源”的问题。Agent完成入站认证后，在调用第三方服务、云服务或内部工具时，需要以合法且受控的身份出示凭据，这一身份即出站身份。出站身份的凭据由智能体身份平台统一托管、加密存储，并在Agent调用时按需注入，避免密钥在代码中硬编码。出站身份支持OAuth客户端、API Key、IAM委托三种认证类型。

OAuth 客户端

OAuth客户端是在身份提供商处注册的应用程序，使用OAuth 2.0协议代表用户请求访问用户的数据。智能体身份平台将Agent注册为资源方的OAuth客户端，托管Client ID与Client Secret；Agent调用支持OAuth 2.0的下游服务时，平台自动完成令牌的申请、注入与续期，Agent无需接触密钥明文。按授权流不同分为两种：

- **授权码流**（Authorization Code Flow）：以“代表用户”的方式授权，令牌携带用户上下文与权限范围（scope），适合访问用户个人数据（如操作GitHub仓库）。
- **客户端凭证流**（Client Credentials Flow）：以“应用资深”身份进行机器到机器（M2M）认证，适合服务间调用。

API Key

API Key是用于身份验证和授权访问资源的唯一标识符。资源方为调用方颁发固定字符串密钥，Agent调用时在请求头（如Authorization或x-api-key）中携带。智能体身份平台对API Key加密存储并托管，Agent通过凭据标识按需获取明文。该方式接入简单、通用性强，适用于不支持OAuth的简单API、LLM服务及内部低风险工具；密钥长期有效、需定期轮换，泄露风险相对较高，应避免暴露在代码或日志中。

IAM 委托

基于统一身份认证服务的委托认证方式。为Agent关联一个专属IAM信任委托并配置权限策略，Agent运行时通过信任委托接口（如AssumeAgency）获取临时安全凭证

 版权所有 © 华为云计算技术有限公司

（ STS Token ），再以临时凭证访问云服务资源。该方式无需长期密钥落盘，临时凭证自动过期并轮换，权限由角色策略精细管控且可审计，适合访问云厂商内部资源。

三种认证类型的区别

表 3-1 三种认证类型的区别

对比维度	OAuth客户端	API Key	IAM 委托
认证机制	OAuth 2.0 授权框架，令牌交换	静态密钥，请求头携带	信任委托+临时安全凭证（ STS Token ）
身份主体	用户（授权码流）或应用（客户端凭证流）	应用本身	云账号下的IAM信任委托（工作负载身份）
凭证有效期	短时令牌，可刷新续期	长期静态，需定期轮换	极短时（分钟～小时级），自动轮换
权限粒度	scope权限范围，细粒度且可撤销	随API Key绑定权限，粒度较粗	权限策略精细管控，可审计
典型场景	第三方SaaS（GitHub等）	简单API、LLM服务、内部低风险工具	云资源访问、跨账号委托
安全特征	免共享密码，令牌可过期、可撤销	简单直接，需加密存储、防泄露	无长期密钥，临时凭证自动过期，安全性最高
运维成本	中（需维护客户端凭证与授权配置）	低	较高（需设计权限策略）

3.2 创建出站身份

操作说明

当智能体需要主动向外发起网络请求、调用外部业务接口或访问下游服务时，需配置专属出站身份。默认状态下智能体无对外访问身份，无法完成合规出站通信。运维人员可在管理界面为单智能体或批量智能体创建出站身份，绑定对应的访问主体信息。该配置用于解决智能体对外访问无身份标识、请求无法鉴权、访问日志无法对应具体智能体的问题，适配日常智能体对外调用、数据外拉、跨服务交互的常规运维场景。

原理描述

智能体出站身份创建基于身份标识绑定与权限隔离机制实现。系统为目标智能体生成唯一合规出站身份凭证，关联智能体本体特征信息与预设访问白名单，完成身份确权绑定。当智能体发起对外出站请求时，系统自动携带专属身份凭证完成链路校验，依托身份标识实现访问主体精准定位、权限动态校验及行为日志留存。通过独立出站身份隔离不同智能体的访问链路，杜绝越权访问、身份混淆问题，构建轻量化、高安全的智能体出站访问信任体系。

版权所有 © 华为云计算技术有限公司

创建 OAuth 认证类型的出站身份

步骤1 登录**智能体身份控制台**。

步骤2 在左侧导航窗格中，选择“出站身份”。单击右上角“创建出站身份”。

步骤3 输入“身份名称”。身份名称只能包含英文字母、数字或特殊字符(_-)，长度不能超过56个字符。

步骤4 认证类型选择“OAuth客户端”。OAuth客户端是在身份提供商处注册的应用程序，使用OAuth 2.0协议代表用户请求访问用户的数据。

步骤5 根据参数说明表格，完成创建OAuth认证类型出站身份的参数设置。

表 3-2 参数说明

参数	说明
提供商	OAuth客户端对接的身份提供商（IdP），即签发令牌的授权服务器所在平台。 • 自定义提供商：使用Discovery URL（自动获取配置详细信息）或通过手动输入服务器元数据来设置自定义OAuth提供程序。 • 预置的提供商：默认OAuth提供程序已部分预配置，您只需要为这些预定义的提供程序指定客户端ID和密钥即可。当前支持Microsoft和Github。
提供商类型配置	配置自定义提供商时，获取元数据信息的方式。 • Discovery URL：使用Discovery URL动态获取凭证提供商的配置信息，配置变更可自动同步，减少手工维护。 • 自定义配置：自定义硬编码配置凭证提供商的元数据信息，适用于不支持Discovery的提供商。
客户端ID	身份提供商或授权服务器分配给客户端应用程序的唯一标识符。与客户端密钥配对使用，属于公开信息。
客户端密钥	分配给客户端应用程序的唯一密钥值，用户在发出请求时针对客户端进行身份验证。属于敏感凭据，泄露可能导致令牌被冒领，需妥善保管并定期轮换。
Discovery URL	当提供商类型配置选择“Discovery URL”时，需要填写此参数。 提供一个Discovery URL，供客户端用户发现您的身份提供商，并与之集成。自动获取授权端点、令牌端点、响应类型等配置信息。
签发者	当提供商类型配置选择“自定义配置”时，需要填写此参数。 授权服务器的基本URL，用于标识令牌的签发者。系统据此校验访问令牌中的签发者（issuer）声明是否与配置一致，防止伪造或跨域令牌滥用。

 版权所有 © 华为云计算技术有限公司

参数	说明
授权端点	当提供商类型配置选择“自定义配置”时，需要填写此参数。 授权服务器执行用户授权流程的端点URL。智能体发起授权请求时，用户通过该端点完成登录和授权同意，授权服务器据此返回授权码。
令牌端点	当提供商类型配置选择“自定义配置”时，需要填写此参数。 客户端使用授权码等凭据交换访问令牌的端点URL。智能体获取授权码后，调用该端点换取访问令牌。
响应类型（可选）	授权服务器支持的OAuth 2.0响应类型，决定授权流程返回的凭据形态。不配置时使用授权服务器默认行为。
租户ID	当提供商选择“预置的提供商”且提供商类型配置选择“预置提供商”的“Microsoft”时，需要填写此参数。 分配给Microsoft Entra租户的唯一标识符，用于定位应用注册所属的目录和授权范围。

步骤6 单击右下角“立即创建”。创建成功的出站身份将会显示在出站身份列表中。

----结束

创建 API Key 类型的出站身份

步骤1 登录**智能体身份控制台**。

步骤2 在左侧导航窗格中，选择“出站身份”。单击右上角“创建出站身份”。

步骤3 输入“身份名称”。身份名称只能包含英文字母、数字或特殊字符(_-)，长度不能超过56个字符。

步骤4 认证类型选择“API Key”。

步骤5 输入API Key的值。

图 3-1 输入 API Key



 版权所有 © 华为云计算技术有限公司

步骤6 单击右下角“立即创建”。创建成功的出站身份将会显示在出站身份列表中。

----结束

创建 IAM 委托类型的出站身份

步骤1 登录**智能体身份控制台**。

步骤2 在左侧导航窗格中，选择“出站身份”。单击右上角“创建出站身份”。

步骤3 输入“身份名称”。身份名称只能包含英文字母、数字或特殊字符(_-)，长度不能超过56个字符。

步骤4 认证类型选择“IAM委托”。

步骤5 在下拉列表中选择已创建的IAM信任委托，或单击右侧“新建IAM信任委托”，创建操作请参考**信任委托**。

图 3-2 创建 IAM 委托类型的出站身份



步骤6 单击右下角“立即创建”。创建成功的出站身份将会显示在出站身份列表中。

----结束

3.3 修改出站身份

操作说明

当智能体出站调用的访问凭据或授权配置发生变化时，您需要修改出站身份。常见场景如下：

- 凭证更换：API Key泄露或到期轮转，需重新生成并更新访问凭据。
- 权限调整：出站调用的授权范围变更，需修改使用的IAM信任委托。
- 合作方信息变更：对接的提供商信息发生调整，需重新配置提供商信息。

修改后，新配置立即生效，原凭据随即失效。

 版权所有 © 华为云计算技术有限公司

约束与限制

不支持修改出站身份的认证类型、提供商类型和预置提供商。

修改出站身份

步骤1 登录**智能体身份控制台**。

步骤2 在左侧导航窗格中，选择“出站身份”。

步骤3 在出站身份列表找到目标出站身份，单击“操作”列下的“修改”。

步骤4 根据需要出站身份的信息，相关参数说明请参见**3.2 创建出站身份**。

步骤5 单击右下角“确定”。信息修改完成后，可以单击出站身份名称查看修改后的情况。

----结束

3.4 删除出站身份

操作说明

当智能体不再需要向外部服务发起出站调用，或现有出站身份无法满足业务要求时，您需要删除出站身份。例如，智能体停止对外调用导致出站身份不再使用、需要更换智能体的认证类型或提供商类型、访问凭据泄露需重新配置，以及与第三方平台或云服务商的合作终止等场景。删除后，该出站身份立即失效，使用该身份的出站调用将认证失败，请确认无运行中的任务依赖该身份后再执行删除。

删除出站身份

步骤1 登录**智能体身份控制台**。

步骤2 在左侧导航窗格中，选择“出站身份”。

步骤3 在出站身份列表找到目标出站身份，单击“操作”列下的“删除”。

警告

删除出站身份，可能导致Agent出现越权访问，从而产生信息泄露，请谨慎操作。

图 3-3 删除出站身份



 版权所有 © 华为云计算技术有限公司

步骤4 输入“DELETE”，单击“确定”。

删除完成后，出站身份列表中将不存在目标出站身份。

----结束

3.5 为出站身份设置标签

操作说明

出站身份支持通过标签进行标识和分类管理。当您需要按业务、部门或环境等维度对出站身份进行分组管理，或在成本核算、权限控制、资源检索等场景下快速识别出站身份时，可为出站身份设置标签。例如，为不同业务线创建的出站身份分别添加对应标签，便于成本统计和运维定位。设置标签后，您可以通过标签筛选出站身份，并基于标签进行批量管理。

为出站身份设置标签

步骤1 登录**智能体身份控制台**。

步骤2 在左侧导航窗格中，选择“出站身份”。

步骤3 在出站身份列表找到目标出站身份，单击目标出站身份的名称。

步骤4 选择“标签”页签显示已添加的标签。

- 添加标签
  a. 单击左上角的“编辑标签”。
  b. 在右侧弹窗中单击“添加标签”。设置需要添加的标签的键和值。

  标签以键值对的形式表示，用于标识云资源，便于对云资源进行分类和搜索。此处的标签仅用于出站身份的过滤和管理。一个出站身份最多添加20个标签。

  图 3-4 添加标签

  标签的设置说明如**表3-3**所示。

 版权所有 © 华为云计算技术有限公司

表 3-3 标签说明

参数	说明	举例
键	输入标签的键，同一个出站身份标签的键不能重复。标签的键为必选，无默认取值。键可以自定义，也可以选择预先在标签服务（TMS）创建好的标签。 键命名规则如下： ■ 长度不能超过128个字符。 ■ 可以包含任意语种的字母、数字和空格，以及_.:/=+-@字符，但首尾不能包含空格，且不能以_sys_开头。	Key_0001
值	输入标签的值，标签的值可以重复，标签的值非必选，并且可以为空。无默认取值。 标签值的命名规则如下： ■ 长度不能超过255个字符。 ■ 可以包含任意语种的字母、数字和空格，以及_.:/=+-@&字符。	Value_0001

c. 单击“确定”，完成标签的添加。添加成功后，标签将会展示在标签列表中。

- 编辑标签
  a. 单击左上角的“编辑标签”。
  b. 在右侧弹窗中修改标签的键和值，参数说明如表3-3所示。
  c. 单击“确定”，完成标签的编辑。编辑完成后，可以在标签列表中查看标签。
- 删除标签
  a. 单击左上角的“编辑标签”。
  b. 在右侧弹窗中，单击待删除标签右侧的“删除”。
  c. 单击“确定”，完成标签的删除。删除成功后，标签列表中将不存在该标签。

----结束

 版权所有 © 华为云计算技术有限公司

4 管理策略集

4.1 策略集概述

策略集简介

智能体身份策略集是用于统一管理智能体出站身份访问策略的配置集合。策略集通过集中定义访问规则，将智能体对外部服务的调用行为纳入统一管控，实现对越权访问的预防、异常调用的发现以及安全事件的审计追溯。

您可以将策略集绑定到指定实例，主要为凭证库。绑定后，策略集规则即对通过该凭证库发起的出站调用生效。一个策略集可应用于多个凭证库，多个策略集也可同时绑定一个凭证库，便于按业务、部门或安全等级对访问策略进行灵活编排。

执行模式

策略集支持设置两种执行模式：

- **拦截模式**：策略规则被强制执行。智能体发起出站调用时，系统实时评估调用请求与策略规则的匹配情况，对符合策略的请求予以放行，对不符合策略的请求直接拦截并记录失败原因，从源头防止未授权访问。
- **观察模式**：策略规则仅被评估和记录，不实际拦截访问。系统对不符合策略规则的调用生成告警日志和审计记录，调用本身仍正常执行。该模式适用于策略上线初期的灰度验证，便于在真实流量中评估规则准确性和影响范围，确认无误后再切换为拦截模式。

策略简介

智能体身份策略是定义智能体访问行为的授权规则，包含在策略集中，主要用于配置凭证的访问控制策略。每条策略通过效果、主体范围、主体类型、资源范围、资源类型、操作范围和条件等要素，精确描述“谁在什么条件下、对什么资源、可以执行什么操作”。其中，效果用于指定策略是允许还是拒绝访问；主体范围和主体类型用于限定策略适用的调用主体及其类型；资源范围和资源类型用于限定策略可访问的资源对象及类型；操作范围用于限定允许执行的操作；条件用于通过条件表达式进一步约束策略的生效场景，如调用时间、调用来源等。

策略支持使用Cedar编辑器进行编辑。Cedar是一种用于描述授权策略的结构化语言，您可以在编辑器中通过可视化方式或文本方式配置策略要素，系统在保存时自动进行

 版权所有 © 华为云计算技术有限公司

语法校验，确保策略格式正确。配置完成的策略包含在策略集中，随策略集绑定至凭证库等实例后生效。

4.2 创建策略集

操作说明

当您需要对智能体的出站调用进行安全管控，或需要为指定凭证库配置差异化的访问控制规则时，您需要创建策略集。例如，限制凭证库仅允许访问特定目标服务、为不同业务线设置不同的调用权限，或先以观察模式验证策略规则后再切换为拦截模式等场景。创建策略集后，您可以将策略集绑定到凭证库等实例，策略规则随即对绑定实例的出站调用生效。

创建策略集

步骤1 登录**智能体身份控制台**。

步骤2 在左侧导航窗格中，选择“策略集”。单击右上角“创建策略集”。

步骤3 输入“名称”。策略集名称只能包含英文字母、数字或特殊字符(_)且必须以字母开头，长度不能超过48个字符。

图 4-1 创建策略集



步骤4 （可选）输入策略集的描述。

步骤5 实例类型选择“凭证库”。表示策略集的规则将对后续绑定的凭证库生效。

步骤6 单击“立即创建”。返回策略集列表，创建成功的策略集将在策略集列表中展示。

----结束

4.3 创建策略

操作说明

当您需要对凭证库中凭据的访问行为进行管控，或现有策略无法满足业务访问需求时，您需要创建策略。例如，限制凭据仅允许访问特定目标服务、设置凭据可执行的

 版权所有 © 华为云计算技术有限公司

操作范围，或按不同业务线配置差异化的访问规则等场景。创建策略时，您可以通过效果、主体范围、主体类型、资源范围、资源类型、操作范围和条件等要素配置访问规则，并使用 Cedar 编辑器完成编写。创建完成后，策略包含在策略集中，随策略集绑定至凭证库后生效。

创建策略

步骤1 登录**智能体身份控制台**。

步骤2 在左侧导航窗格中，选择“策略集”。

步骤3 在策略集列表找到目标策略集，单击目标策略集名称。

步骤4 选择“策略”页签，单击“添加策略”。

步骤5 配置策略的基本信息。输入“名称”。策略名称只能包含英文字母、数字或特殊字符(_)且必须以字母开头，长度不能超过48个字符。

步骤6 配置策略语句。根据**表4-1**中的信息配置策略语句参数。

图 4-2 配置策略语句

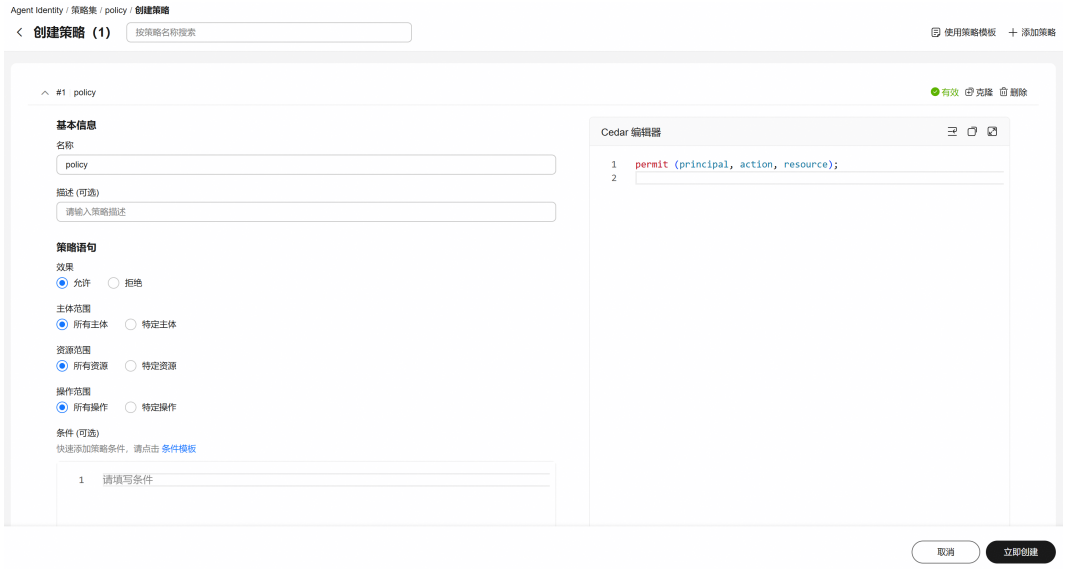


表 4-1 策略语句参数

参数	说明
效果	策略对符合条件的访问请求执行的结果，决定访问是放行还是拦截。 ● 允许：放行符合条件的访问请求，允许调用执行。 ● 拒绝：拦截符合条件的访问请求，禁止调用执行。 显式拒绝优先于允许。

版权所有 © 华为云计算技术有限公司

参数	说明
主体范围	策略适用的调用主体范围，即“哪些主体可以使用该策略”。 ● 所有主体：策略对全部调用主体生效，不区分主体类型。 ● 特定主体：策略仅对指定的主体生效，需进一步选择主体及主体类型。 – IAM身份：策略仅对IAM身份的主体类型生效，填写URN后策略仅对该主体生效；不填则对该类型下全部主体生效。
资源范围	策略可访问的资源范围，即“能访问哪些资源”。 ● 所有资源：策略对全部资源生效，不区分资源类型。 ● 特定资源：策略仅对指定的资源生效，需进一步选择资源及资源类型。 – OAuth客户端：策略仅对OAuth客户端的资源类型生效。填写URN后策略仅对该资源生效；不填则对该类型下全部资源生效。 – API Key：策略仅对API Key的资源类型生效。填写URN后策略仅对该资源生效；不填则对该类型下全部资源生效。 – IAM委托：策略仅对IAM委托的资源类型生效。填写URN后策略仅对该资源生效；不填则对该类型下全部资源生效。
操作范围	策略允许或拒绝执行的操作范围，即“能执行哪些操作”。 ● 所有操作：策略对全部操作生效。 ● 特定操作：策略仅对指定的操作生效，需在“选择操作”中选择具体操作。 – GetResourceOAuth2Token：通过OAuth2两方/三方授权流程获取访问令牌，以访问外部资源。 – GetResourceApiKey：获取与API密钥凭证提供者关联的API密钥。 – GetResourceStsToken：从STS凭证提供者获取IAM临时凭证。
条件（可选）	策略生效的附加约束条件，通过条件表达式限定访问场景。 ● 不配置：策略对全部场景生效，不做额外约束。 ● 配置：需通过条件表达式进一步限定策略的生效场景。

版权所有 © 华为云计算技术有限公司

步骤7 确认配置无误后，单击“立即创建”。

步骤8 在弹窗中单击“确定”。

返回策略列表。查看到新创建的策略存在策略列表中，且“状态”为生效，表示策略创建成功。

----结束

4.4 编辑策略

操作说明

当策略集中某条策略的访问规则不再满足业务需求时，您可以编辑该策略。例如，凭证可访问的目标服务或操作范围发生变化、需要收窄或扩大授权范围，或调整策略的生效条件等场景。编辑策略时，您可以通过Cedar编辑器修改效果、主体范围、资源范围、操作范围和条件等要素。编辑完成后，新规则立即生效，建议先以观察模式验证策略效果后再切换为拦截模式。

编辑策略

步骤1 登录**智能体身份控制台**。

步骤2 在左侧导航窗格中，选择“策略集”。

步骤3 在策略集列表找到目标策略集，单击目标策略集名称。

步骤4 在策略列表找到目标策略，单击“操作”列下的“编辑”。

步骤5 根据表中的信息完成策略的修改，单击“确定”。

图 4-3 编辑策略



 版权所有 © 华为云计算技术有限公司

步骤6 在弹窗中输入“CONFIRM”，单击“确定”。

返回策略列表。查看到策略的更新时间为修改时间时，表示策略编辑成功。

----结束

4.5 将实例绑定至策略集

操作说明

创建策略集后，策略规则需要绑定至实例后方可生效。当您需要将策略集的访问控制规则应用到指定凭证库，或需要为不同业务、不同安全等级的凭证库应用差异化的策略集时，您需要将策略集绑定至对应实例。例如，新增凭证库后为其绑定已有策略集，或业务安全要求变化时调整凭证库绑定的策略集。绑定完成后，策略规则随即对通过该实例发起的出站调用生效，您可以根据策略执行情况调整绑定关系。

将策略集绑定至实例

步骤1 登录智能体身份控制台。

步骤2 在左侧导航窗格中，选择“策略集”。

步骤3 在策略集列表找到目标策略集，单击“操作”列下的“绑定实例”。此处以实例类型是“凭证库”的策略集为例。

步骤4 在右侧弹窗的下拉列表中选择对应的凭证库。

步骤5 选择“拦截模式”。支持以下两种模式：

- **拦截模式**：根据权限策略的判定结果，允许或拒绝请求。
- **观察模式**：仅记录权限策略的判定结果，不阻断请求。

图 4-4 绑定实例



步骤6 单击“确定”，完成绑定实例。

策略集创建成功后，可以单击目标策略集名称，在策略集详情页的“绑定实例”页签中查看已绑定成功的实例。

----结束

版权所有 © 华为云计算技术有限公司

4.6 将实例从策略集解绑

操作说明

当策略集不再适用于指定实例，或实例的访问管控方式需要调整时，您需要将实例从策略集解绑。例如，实例对应的业务发生变化、访问管控已迁移至其他策略集，或实例即将下线时，可先解绑策略集，再重新绑定其他策略集或删除实例。解绑后，策略集的规则不再对该实例的出站调用生效，该实例恢复为未绑定策略集的状态。

将实例从策略集解绑

步骤1 登录**智能体身份控制台**。

步骤2 在左侧导航窗格中，选择“策略集”。

步骤3 在策略集列表找到目标策略集，单击目标策略集名称。

步骤4 选择“绑定实例”页签，找到目标实例，单击“操作”列下的“解绑”。

图 4-5 解绑实例



步骤5 输入“UNBIND”，单击“确定”。

返回绑定实例列表，查看到目标实例不存在，则表示解绑实例成功。

----结束

4.7 删除策略集

操作说明

当不再需要使用策略集时，您可以删除策略集。例如，访问管控需求已取消、策略规则已迁移至其他策略集，或绑定的实例已全部解绑时，可将策略集删除。删除前，请先解绑该策略集绑定的实例，确保相关出站调用已迁移至其他策略集或不再受管控。删除后，策略集及其包含的策略规则将不可恢复。

版权所有 © 华为云计算技术有限公司

删除策略集

步骤1 登录智能体身份控制台。

步骤2 在左侧导航窗格中，选择“策略集”。

步骤3 在策略集列表找到目标策略集，单击“操作”列下的“删除”。

图 4-6 删除策略集



步骤4 确认策略集信息无误后，输入“DELETE”，单击“确定”。

返回策略集列表，查看到目标策略集不存在，则表示策略集删除成功。

----结束

4.8 删除策略

操作说明

当策略集中的某条策略不再适用或无需继续管控时，您可以删除该策略。例如，凭证的访问需求发生变化、策略规则配置有误需重新配置，或策略集中存在冗余策略需简化规则时，可将对应策略删除。删除前，请确认该策略管控的访问需求已取消，或已由策略集中的其他策略覆盖。删除后，该策略立即失效，策略集中剩余的策略继续生效。

删除策略

步骤1 登录智能体身份控制台。

步骤2 在左侧导航窗格中，选择“策略集”。

步骤3 在策略集列表找到目标策略集，单击目标策略集名称。

步骤4 选择“策略”页签，找到目标策略，单击“操作”列下的“删除”。

版权所有 © 华为云计算技术有限公司

图 4-7 删除策略



步骤5 确认策略信息无误后，输入“DELETE”，单击“确定”。

返回策略列表，查看到目标策略不存在，则表示策略删除成功。

----结束

4.9 为策略集设置标签

操作说明

策略集支持通过标签进行标识和分类管理。当您需要按业务、部门或环境等维度对策略集进行分组管理，或在成本核算、权限控制、资源检索等场景下快速识别策略集时，可为策略集设置标签。例如，为不同业务线使用的策略集分别添加对应标签，便于成本统计和运维定位。设置标签后，您可以通过标签筛选策略集，并基于标签进行批量管理。

为策略集设置标签

步骤1 登录智能体身份控制台。

步骤2 在左侧导航窗格中，选择“策略集”。

步骤3 在策略集列表找到目标策略集，单击目标策略集的名称。

步骤4 选择“标签”页签。

- 添加标签
  a. 单击左上角的“编辑标签”。
  b. 在右侧弹窗中单击“添加标签”。设置需要添加的标签的键和值。
     标签以键值对的形式表示，用于标识云资源，便于对云资源进行分类和搜索。此处的标签仅用于策略集的过滤和管理。一个策略集最多添加20个标签。

 版权所有 © 华为云计算技术有限公司

图 4-8 添加标签



标签的设置说明如表4-2所示。

表 4-2 标签说明

参数	说明	举例
键	输入标签的键，同一个策略集标签的键不能重复。标签的键为必选，无默认取值。键可以自定义，也可以选择预先在标签服务（TMS）创建好的标签。 键命名规则如下： ■ 长度不能超过128个字符。 ■ 可以包含任意语种的字母、数字和空格，以及_.:/=+-@字符，但首尾不能包含空格，且不能以_sys_开头。	Key_0001
值	输入标签的值，标签的值可以重复，标签的值非必选，并且可以为空。无默认取值。 标签值的命名规则如下： ■ 长度不能超过255个字符。 ■ 可以包含任意语种的字母、数字和空格，以及_.:/=+-@&字符。	Value_0001

c. 单击“确定”，完成标签的添加。添加成功后，标签将会展示在标签列表中。

- 编辑标签
  a. 单击左上角的“编辑标签”。
  b. 在右侧弹窗中修改标签的键和值，参数说明如表4-2所示。
  c. 单击“确定”，完成标签的编辑。编辑完成后，可以在标签列表中查看标签。
- 删除标签
  a. 单击左上角的“编辑标签”。
  b. 在右侧弹窗中，单击待删除标签右侧的“删除”。
  c. 单击“确定”，完成标签的删除。删除成功后，标签列表中将不存在该标签。

----结束

 版权所有 © 华为云计算技术有限公司

5 管理凭证库

5.1 凭证库概述

凭证库简介

智能体身份凭证库是智能体身份体系中用于集中管理出站访问凭据的实例，是出站身份认证与访问控制的基础设施。智能体对外部服务发起调用所需的各类凭据，如 OAuth 客户端的访问令牌、API Key 以及 IAM 委托的临时凭证等，均由凭证库统一存储和维护。通过凭证库，您可以将凭据的创建、存储、轮换和审计纳入统一管理，避免凭据散落在业务配置中。

凭证库支持对凭据进行安全存储，凭据在库内加密保存，不对外明文展示，从源头降低凭据泄露风险。同时，凭证库支持凭据的生命周期管理，包括凭据的创建、更新、轮换和删除，确保过期或已泄露的凭据能够及时处置。

凭证库是策略集的主要绑定实例。您可以将策略集绑定至凭证库，通过策略集中的策略对凭据的使用范围进行管控，例如限制凭据可访问的目标服务、可执行的操作以及生效条件。绑定策略集后，通过该凭证库发起的出站调用将受到策略约束，实现 "凭据统一管理、访问统一管控"。

您可以在凭证库中为凭证设置标签，按业务、部门或环境等维度进行分类管理，并通过标签快速检索和批量操作。凭证库可绑定智能体身份策略集，绑定后，策略集对通过该凭证库发起的出站调用进行访问控制，支持拦截模式和观察模式两种执行方式，实现越权访问的预防与异常调用的审计追溯。

智能体发起出站调用时，系统根据调用需求从凭证库中匹配对应凭证，完成身份认证后访问目标服务。凭证库将分散的出站身份凭证统一纳管，配合策略集实现凭证管理、访问控制和审计追溯一体化，为智能体对外部服务的安全访问提供基础支撑。

5.2 为凭证库设置标签

操作说明

凭证库支持通过标签进行标识和分类管理。当您需要按业务、部门或环境等维度对凭证库进行分组管理，或在成本核算、权限控制、资源检索等场景下快速识别凭证库时，可为凭证库设置标签。例如，为不同业务线使用的凭证库分别添加对应标签，便

 版权所有 © 华为云计算技术有限公司

于成本统计和运维定位。设置标签后，您可以通过标签筛选凭证库，并基于标签进行批量管理。

为凭证库设置标签

步骤1 登录**智能体身份控制台**。

步骤2 在左侧导航窗格中，选择“凭证库”。

步骤3 在凭证库列表找到目标凭证库，单击目标凭证库的名称。

步骤4 选择“标签”页签。

- 添加标签
  a. 单击左上角的“编辑标签”。
  b. 在右侧弹窗中单击“添加标签”。设置需要添加的标签的键和值。

  标签以键值对的形式表示，用于标识云资源，便于对云资源进行分类和搜索。此处的标签仅用于凭证库的过滤和管理。一个凭证库最多添加20个标签。

图 5-1 添加标签



标签的设置说明如**表4-2**所示。

表 5-1 标签说明

参数	说明	举例
键	输入标签的键，同一个凭证库标签的键不能重复。标签的键为必选，无默认取值。键可以自定义，也可以选择预先在标签服务（TMS）创建好的标签。 键命名规则如下： ■ 长度不能超过128个字符。 ■ 可以包含任意语种的字母、数字和空格，以及_.:/=+-@字符，但首尾不能包含空格，且不能以_sys_开头。	Key_0001

版权所有 © 华为云计算技术有限公司

参数	说明	举例
值	输入标签的值，标签的值可以重复，标签的值非必选，并且可以为空。无默认取值。 标签值的命名规则如下： ■ 长度不能超过255个字符。 ■ 可以包含任意语种的字母、数字和空格，以及_.:/=+-@&字符。	Value_0001

c. 单击“确定”，完成标签的添加。添加成功后，标签将会展示在标签列表中。

- 编辑标签
  a. 单击左上角的“编辑标签”。
  b. 在右侧弹窗中修改标签的键和值，参数说明如表4-2所示。
  c. 单击“确定”，完成标签的编辑。编辑完成后，可以在标签列表中查看标签。
- 删除标签
  a. 单击左上角的“编辑标签”。
  b. 在右侧弹窗中，单击待删除标签右侧的“删除”。
  c. 单击“确定”，完成标签的删除。删除成功后，标签列表中将不存在该标签。

----结束

 版权所有 © 华为云计算技术有限公司