

IAM 身份中心

# 产品介绍

文档版本 01  
发布日期 2023-06-30



版权所有 © 华为技术有限公司 2024。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



HUAWEI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。

# 安全声明

## 漏洞处理流程

华为公司对产品漏洞管理的规定以“漏洞处理流程”为准，该流程的详细内容请参见如下网址：

<https://www.huawei.com/cn/psirt/vul-response-process>

如企业客户须获取漏洞信息，请参见如下网址：

<https://securitybulletin.huawei.com/enterprise/cn/security-advisory>

---

## 目录

---

1 什么是 IAM 身份中心.....	1
2 应用场景.....	2
3 功能总览.....	4
4 权限管理.....	5
5 约束与限制.....	7
6 计费说明.....	9
7 基本概念.....	10
8 修订记录.....	11


# 1 什么是 IAM 身份中心

## 简介

IAM身份中心为用户提供基于华为云组织的多账号统一身份管理与访问控制。可以统一管理企业中使用华为云的用户，一次性配置企业的身份管理系统与华为云的单点登录，以及所有用户对组织下账号的访问权限。管理员集中创建用户，分配登录密码，并对其进行分组管理。允许用户使用特定用户名和密码登录统一的用户门户网站，访问为其分配的多个账号下的资源，无需多次登录。且通过一个应用中的安全验证后，再访问其他应用中的受保护资源时，不再需要重新登录验证。

## 如何访问 IAM 身份中心

通过管理控制台、基于HTTPS请求的API（Application Programming Interface）两种方式访问IAM身份中心。

- 管理控制台方式  
管理控制台是网页形式的，您可以使用直观的界面进行相应的操作。登录[管理控制台](#)，单击页面左上角的 ，选择“管理与监管 > IAM身份中心”。
- API方式  
如果用户需要将华为云上的IAM身份中心集成到第三方系统，用于二次开发，请使用API方式访问IAM身份中心，具体操作请参见[《IAM身份中心API参考》](#)。

# 2 应用场景

## 集中的身份管理，一次配置，即可安全访问多个账号的资源

大型企业在云上一般有多个账号，当前企业员工如需访问多个账号下的资源，需分别登录多个账号，或在多个账号下分别创建IAM用户来登录，维护成本高，操作效率低。通过IAM身份中心可以：

- 集中创建和管理用户：
  - 允许管理员集中创建用户，分配登录密码，并对其进行分组管理。
  - 允许用户使用特定用户名和密码登录统一的用户门户网站，访问为其分配的多个账号下的资源，无需多次登录。
- 连接到基于SAML 2.0协议的外部身份提供商系统，例如微软AD和Okta：
  - 允许管理员将IAM身份中心使用的SAML 2.0协议连接到外部身份提供商系统。
  - 支持通过SCIM协议自动化用户预置过程。管理员可以在外部身份提供商处管理用户，用户信息会自动同步到IAM身份中心，无需人工干预。
  - 外部身份提供商用户可使用现有账号密码登录其门户，然后自动跳转至华为云来访问华为云账号下的资源，无需IAM身份中心管理员重新分配密码。
- 多因素认证（MFA）：
  - 允许管理员对用户强制实施MFA，降低密码泄露的风险。
  - MFA设备支持基于TOTP协议的APP和基于FIDO2的硬件安全密钥设备。

## 支持细粒度授权，让用户集中、安全以及高效地分配每个账号资源的访问权限

大型企业在云上一般有多个账号，各个账号承载业务不同，登录的企业员工的职责也不同。需要针对不同账号配置不同员工的细粒度访问权限，确保企业的资源访问安全合规。

- 集中管理用户对多个账号资源的访问权限：
  - 允许管理员使用不超过20个IAM权限策略创建权限集，实现批量的账号权限配置。
  - 每个账号可以设置允许访问的用户和对应的权限集。
  - IAM身份中心会自动将账号的权限信息同步到IAM，无需管理员在单个账号中重复授权。
- 基于属性的访问控制机制：

- 允许管理员通过支持属性的自定义策略创建权限集。包括用户和资源的组织、标签、请求时间、源地址等20+全局级属性及其他云服务级属性。
- 允许管理员利用身份提供商定义的业务标签创建权限集。业务标签会在联邦登录过程中被自动转换为IAM的身份标签属性，用于控制访问权限。
- 管理员只需一次性为所有用户定义权限，后续属性变化后策略中的条件键匹配结果也将发生变化，即可自动授予、撤销或修改访问权限。

# 3 功能总览

---

## 集中身份管理

通过IAM身份中心可以创建和管理用户、用户组以及配置登录时的身份验证方式等。使用创建的用户登录后，可集中管理和访问华为云下多个账号的资源。IAM身份中心为每个组织提供统一的用户管理及登录门户。

## 访问权限管理

IAM身份中心可以统一配置用户对整个组织内的任意成员账号的访问权限。IAM身份中心管理员可以根据组织的结构，选择不同成员账号为其关联IAM身份中心用户/用户组以及权限集，用户的对成员账号资源的访问权限由权限集控制，且权限集可以随时修改和删除。

## 对接企业身份管理系统

IAM身份中心可配置基于满足条件（SAML 2.0协议）的企业身份管理系统进行单点登录（SSO），直接使用企业身份管理系统的用户，无需再创建用户，提升企业用户管理效率，降低安全风险。



# 4 权限管理

如果您需要对华为云上创建的IAM身份中心资源，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。IAM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。

通过IAM，您可以在账号中给员工创建IAM用户，并授权控制他们对华为云资源的访问范围。

如果华为账号已经能满足您的要求，不需要创建独立的IAM用户进行权限管理，您可以跳过本章节，不影响您使用IAM身份中心的其它功能。

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。

关于IAM的详细介绍，请参见[IAM产品介绍](#)。

## IAM 身份中心权限

默认情况下，管理员创建的IAM用户没有任何权限，需要将其加入用户组，并给用户组授予策略或角色，才能使得用户组中的用户获得对应的权限，这一过程称为授权。授权后，用户就可以基于被授予的权限对云服务进行操作。

IAM身份中心部署时不区分物理区域，为全局级服务。授权时，在全局级服务中设置权限，访问IAM身份中心时，不需要切换区域。

权限根据授权精细程度分为角色和策略。

- **角色**：IAM最初提供的一种根据用户的工作职能定义权限的粗粒度授权机制。该机制以服务为粒度，提供有限的服务相关角色用于授权。由于华为云各服务之间存在业务依赖关系，因此给用户授予角色时，可能需要一并授予依赖的其他角色，才能正确完成业务。角色并不能满足用户对精细化授权的要求，无法完全达到企业对权限最小化的安全管控要求。
- **策略**：IAM最新提供的一种细粒度授权的能力，可以精确到具体服务的操作、资源以及请求条件等。基于策略的授权是一种更加灵活的授权方式，能够满足企业对权限最小化的安全管控要求。例如：针对ECS服务，管理员能够控制IAM用户仅能对某一类云服务器资源进行指定的管理操作。多数细粒度策略以API接口为粒度进行权限拆分，权限的最小粒度为API授权项（action）。

如[表1](#)所示，包括了IAM身份中心的所有系统权限。

表 4-1 IAM 身份中心系统权限

系统角色/策略名称	描述	类别	依赖关系
IdentityCenter FullAccess	IAM身份中心管理员权限，拥有该权限的用户可以查看并使用IAM身份中心所有功能。	系统策略	无
IdentityCenter ReadOnlyAccess	IAM身份中心只读权限，拥有该权限的用户仅能查看IAM身份中心数据。	系统策略	无

表2列出了IAM身份中心常用操作与系统权限的授权关系，您可以参照该表选择合适的系统权限。

表 4-2 常用操作与系统权限的关系

操作	IdentityCenter FullAccess	IdentityCenter ReadOnlyAccess
创建用户	√	x
查看用户信息	√	√
修改用户信息	√	x
创建用户组	√	x
用户组添加/移除用户	√	x
删除用户组	√	x
查看用户组	√	√
创建权限集	√	x
修改权限集	√	x
删除权限集	√	x
查看权限集	√	√

## 相关链接

- [IAM产品介绍](#)
- [创建IAM用户并授权使用IAM身份中心](#)

# 5 约束与限制

## 使用约束

- IAM身份中心依赖组织云服务定义的组织来获取成员账号信息，所以使用IAM身份中心之前，必须先开通组织云服务并创建组织，以组织管理账号登录并使用IAM身份中心。如何开通组织云服务并创建组织请参见：[创建组织](#)。
- 中国站IAM身份中心无法管理国际站账号，国际站的IAM身份中心也无法管理中国站账号。

## 使用限制

IAM身份中心的使用限制如下表所示，如果默认配额无法满足业务需求，您可以申请扩大配额，具体请参见：[调整配额](#)。

表 5-1 IAM 身份中心的使用限制

限制项	默认配额	是否支持修改
IAM身份中心允许创建的用户数量	10万	是
IAM身份中心允许创建的用户组数量	10万	是
一个用户组内的用户数量	无限制	-
一个用户可以加入的用户组数量	1000	否
一个用户可以绑定的多因素认证（MFA）设备数量	2	否
IAM身份中心允许创建的权限集数	2000	是
一个权限集可以包含的权限策略数	18个系统策略+1个自定义身份策略+1个自定义策略	否
一个账号可以绑定的权限集数	50	是
自定义策略的最大字符数量	6144	否

限制项	默认配额	是否支持修改
可以配置的外部身份提供商 (IdP) 数量	1	否
访问控制属性功能可添加的属性数量	20	否

# 6 计费说明

IAM身份中心为免费服务，使用IAM身份中心的相关功能不收取任何费用。账号下资源自身的使用费用请参见各服务的计费说明。

# 7 基本概念

## 用户

指在IAM身份中心创建的用户，将IAM身份中心用户与组织下的多个账号关联并配置权限，然后使用IAM身份中心用户登录即可访问多个账号下的资源，无需重复登录。

## 用户组

指在IAM身份中心创建的用户组，IAM身份中心用户组是IAM身份中心用户的集合，可以通过用户组功能实现对多个用户的统一授权，方便统一权限管理。用户加入特定用户组后，将具备对应用户组的权限。当某个用户加入多个用户组时，此用户同时拥有多个用户组的权限，即多个用户组权限的全集。

## 权限集

权限集是管理员创建和维护的权限模板，它定义了一个或多个IAM策略的集合。权限集简化了IAM身份中心的用户和用户组对账号访问权限的分配，可以实现批量的账号权限配置，无需再进行单独的权限配置。

## 管理账号

组织中开通并创建IAM身份中心实例的账号即为管理账号（也称管理员），此账号统一管理所有IAM身份中心用户及其访问权限。

## 委托管理员

IAM身份中心默认由组织管理员账号使用和管理，组织中的成员账号如需使用IAM身份中心，需组织管理员将其设置为委托管理员。

此操作会将IAM身份中心的管理访问权限委托给此成员账号中的用户。对此委托管理员账号拥有足够权限的所有用户可以从该账号执行所有IAM身份中心管理任务，但以下任务除外：删除IAM身份中心、设置其他成员账号为委托管理员、管理向管理账号分配的任务，或管理在管理账号中预置的权限集。

## 用户门户

管理员开通IAM身份中心后，系统会自动生成唯一的用户门户URL，此管理员创建的所有IAM身份中心用户均需使用此URL登录并访问指定账号下的资源。

# 8 修订记录

发布日期	修订记录
2023-06-30	第一次正式发布。