

统一身份认证服务

产品介绍

文档版本

14

发布日期

2020-12-30



版权所有 © 华为技术有限公司 2021。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默示的声明或保证。

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。

目录

1 什么是 IAM.....	1
2 基本概念.....	4
3 IAM 功能.....	10
4 使用 IAM 授权的云服务.....	12
5 个人数据保护机制.....	19
6 权限管理.....	21
7 约束与限制.....	27
8 修订记录.....	29

1 什么是 IAM

统一身份认证（Identity and Access Management，简称IAM）是华为云提供权限管理的基础服务，可以帮助您安全地控制华为云服务和资源的访问权限。

IAM无需付费即可使用，您只需要为您帐号中的资源进行付费。

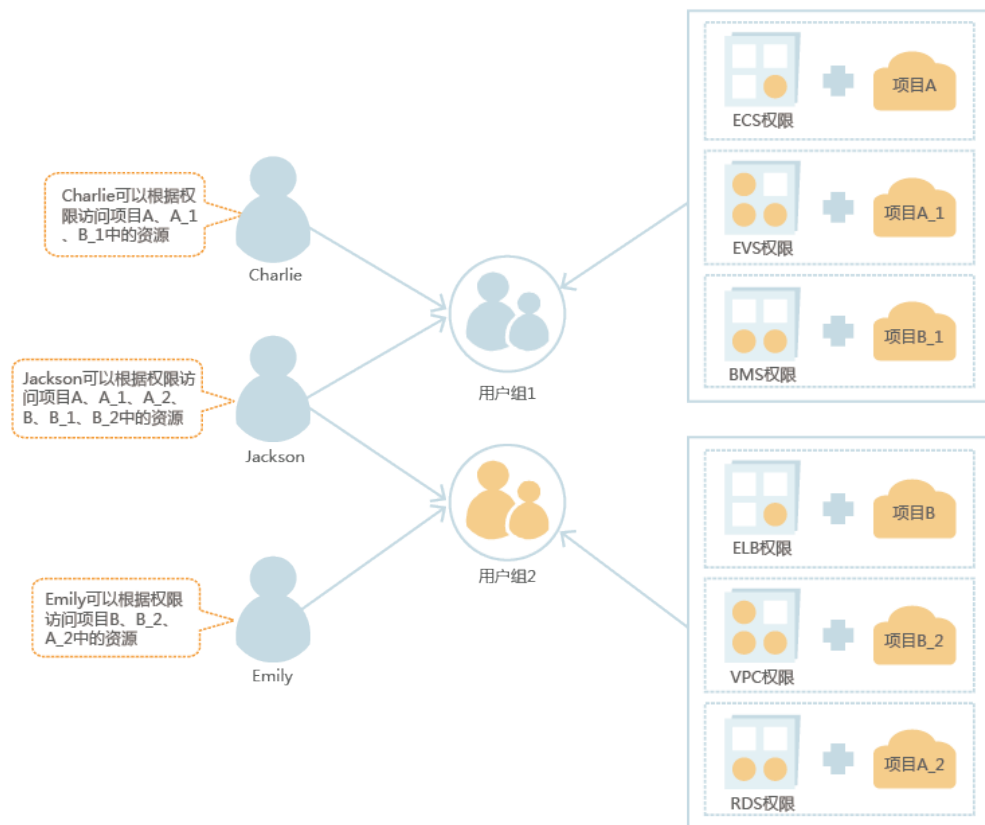
IAM 的优势

对华为云的资源进行精细访问控制

您注册华为云后，系统自动创建帐号，帐号是资源的归属以及使用计费的主体，对其所拥有的资源具有完全控制权限，可以访问华为云所有的云服务。

如果您在华为云购买了多种资源，例如弹性云服务器、云硬盘、裸金属服务器等，您的团队或应用程序需要使用您在华为云中的资源，您可以使用IAM的用户管理功能，给员工或应用程序创建IAM用户，并授予IAM用户刚好能完成工作所需的权限，新创建的IAM用户可以使用自己单独的用户名和密码登录华为云。IAM用户的作用是多用户协同操作同一帐号时，避免分享帐号的密码。

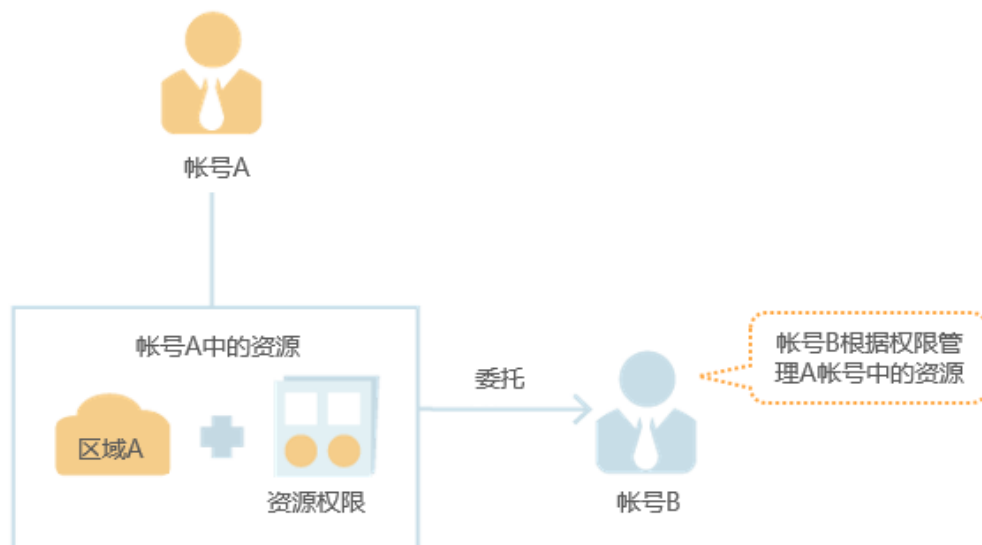
除了IAM外，还有企业管理服务同样可以进行资源权限管理，相对于IAM，企业管理对资源的控制粒度更为精细，同时还支持企业项目费用的管理，建议结合企业需求选择IAM或是企业管理进行资源权限管理，关于两者的详细区别，请参见：[IAM与企业管理的区别](#)。



跨帐号的资源操作与授权

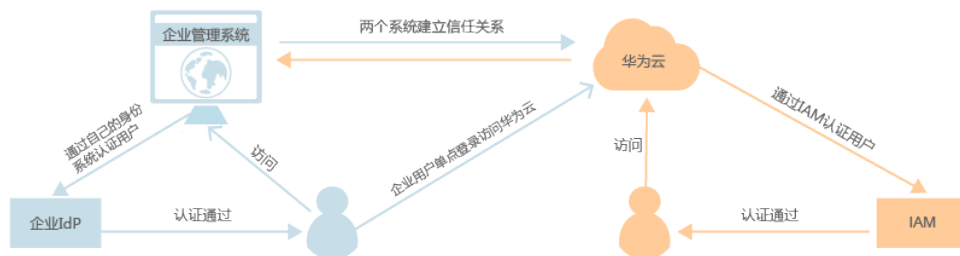
如果您在华为云购买了多种资源，其中一种资源希望由其它帐号管理，您可以使用IAM提供的委托功能。

例如您在华为云上购买的部分资源，希望委托给一家专业的代运维公司来运维，通过IAM的委托功能，代运维公司可以使用自己的帐号对您委托的资源进行运维。当委托关系发生变化时，您可以随时修改或撤消对代运维公司的授权。下图中帐号A即为委托方，帐号B为被委托方。



使用企业已有帐号登录华为云

当您希望本企业员工可以使用企业内部的认证系统登录华为云，而不需要在华为云中重新创建对应的IAM用户，您可以使用IAM的身份提供商功能，建立您所在企业与华为云的信任关系，通过联合认证使员工使用企业已有帐号直接登录华为云，实现单点登录。



IAM 访问方式

您可以通过以下任何一种方式访问IAM。

- **管理控制台**
您可以通过基于浏览器的可视化界面，即控制台访问IAM。
- **REST API**
您可以使用IAM提供的REST API接口以编程方式访问IAM。

2 基本概念

本章为您介绍使用IAM服务时常用的基本概念：帐号、IAM用户、帐号与IAM用户的关系、身份凭证、虚拟MFA、用户组、授权、权限、项目、委托、企业项目。

帐号

当您首次使用华为云时，需要使用手机号注册一个帐号，该帐号是您的华为云资源归属、资源使用计费的主体，对其所拥有的资源及云服务具有完全的访问权限，可以重置用户密码、分配用户权限等。帐号统一接收所有IAM用户进行资源操作时产生的费用账单。帐号在登录华为云控制台时，使用“帐号登录”方式登录。

如果您忘记了帐号的登录密码，可以重置密码，重置方法请参见：[忘记帐号密码](#)。

图 2-1 帐号登录



IAM 用户

由华为云帐号在IAM中创建的用户，是云服务的使用人员，具有独立的身份凭证（密码和访问密钥），根据帐号授予的权限使用资源。IAM用户不进行独立的计费，由所属账户统一付费。

如果您忘记了IAM用户的登录密码，可以重置密码，重置方法请参见：[忘记帐号密码](#)。

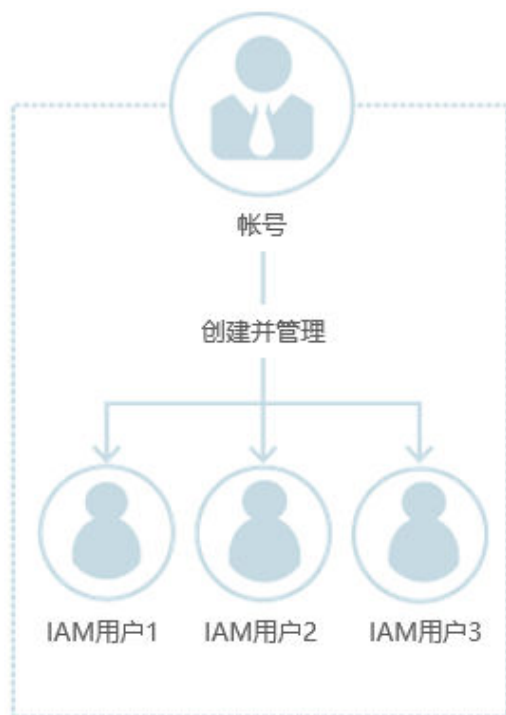
图 2-2 IAM 用户登录



帐号与 IAM 用户的关系

帐号与IAM用户可以类比为父子关系，帐号是资源归属以及计费的主体，对其拥有的资源具有所有权限。IAM用户由帐号创建，只能拥有帐号授予的资源使用权限，帐号可以随时修改或者撤销IAM用户的使用权限。IAM用户进行资源操作时产生的费用统一计入帐号中，IAM用户不需要为资源付费。

图 2-3 帐号与 IAM 用户



身份凭证

身份凭证是识别用户身份的依据，您通过控制台或者API访问华为云时，需要使用身份凭证来通过系统的鉴权认证。身份凭证包括密码和访问密钥，您可以在IAM中管理自己以及帐号中IAM用户的身份凭证。

- 密码：常见的身份凭证，密码可以用来登录华为云界面控制台，还可以调用华为云的API接口。
- 访问密钥：即AK/SK（Access Key ID/Secret Access Key），调用华为云API接口的身份凭证，不能登录控制台。访问密钥中具有验证身份的签名，通过加密签名验证可以确保机密性、完整性和请求双方身份的正确性。

虚拟 MFA

虚拟MFA（Multi-Factor Authentication，简称MFA），是一款能产生6位数字认证码的应用程序，遵循基于时间的一次性密码（TOTP）标准。MFA设备可以基于硬件也可以基于软件，华为云目前仅支持基于软件的虚拟MFA，即虚拟MFA应用程序，可以在移动硬件设备（包括智能手机）上运行，获取认证码并进行身份认证。关于虚拟MFA的详细使用方法请参考：[虚拟MFA](#)。

用户组

用户组是用户的集合，IAM通过用户组功能实现用户的授权。您创建的IAM用户，需要加入特定用户组后，才具备对应的权限，否则IAM用户无法访问您帐号中的任何资源或者云服务。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。

“admin”为系统缺省提供的用户组，具有所有云服务资源的操作权限。将IAM用户加入该用户组后，IAM用户可以操作并使用所有云资源，包括但不限于创建用户组及用户、修改用户组权限、管理华为云资源等。

图 2-4 用户组与用户



授权

授权是您将用户完成具体工作需要的权限授予用户，授权通过策略定义的权限生效，通过给用户组授予策略（包括系统策略和自定义策略），用户组中的用户就能获得策略中定义的权限，这一过程称为授权。用户获得具体云服务的权限后，可以对云服务进行操作，例如，管理您帐号中的ECS资源。

图 2-5 授权



权限

权限根据授权的精细程度，分为策略和角色。

- 角色：角色是IAM最初提供的一种粗粒度的授权能力，当前有部分云服务不支持基于角色的授权。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：策略是IAM最新提供的一种细粒度授权的能力，可以精确到具体操作、资源、条件等。使用基于策略的授权是一种更加灵活地授权方式，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的资源进行指定的管理操作。策略包含系统策略和自定义策略。
 - 云服务在IAM预置了常用授权项，称为**系统策略**。管理员给用户组授权时，可以直接使用这些系统策略，系统策略只能使用，不能修改。如果管理员在IAM控制台给用户组或者委托授权时，无法找到特定服务的系统策略，原因是该服务暂时不支持IAM，管理员可以通过**给对应云服务提交工单**，申请该服务在IAM预置权限。
 - 如果系统策略无法满足授权要求，管理员可以根据各服务支持的授权项，创建**自定义策略**，并通过给用户组授予自定义策略来进行精细的访问控制，自定义策略是对系统策略的扩展和补充。目前华为云支持可视化视图、JSON视图两种自定义策略配置方式。

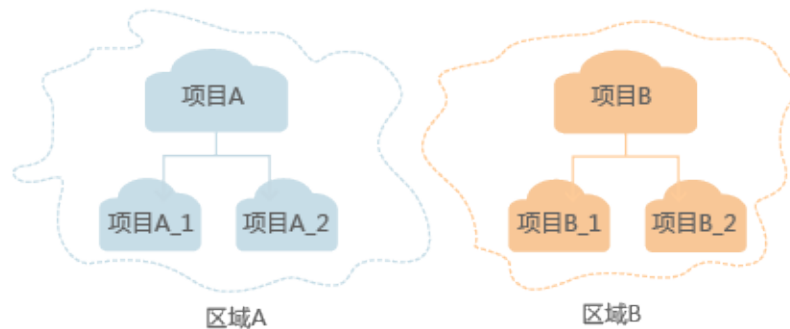
图 2-6 权限内容示例

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Action": [
        "apm:*:*"
      ],
      "Effect": "Allow"
    }
  ]
}
```

项目

华为云的区域默认对应一个项目，这个项目由系统预置，用来隔离物理区域间的资源（计算资源、存储资源和网络资源），以默认项目为单位进行授权，用户可以访问您帐号中该区域的所有资源。如果您希望进行更加精细的权限控制，可以在区域默认的项目中创建子项目，并在子项目中购买资源，然后以子项目为单位进行授权，使得用户仅能访问特定子项目中资源，使得资源的权限控制更加精确。

图 2-7 项目



委托

委托根据委托对象的不同，分为委托其他华为云帐号和委托其他云服务。

- 委托其他华为云帐号：通过委托信任功能，您可以将自己帐号中的资源操作权限委托给更专业、高效的其他华为云帐号，被委托的帐号可以根据权限代替您进行资源运维工作。
- 委托其他云服务：由于华为云各服务之间存在业务交互关系，一些云服务需要与其他云服务协同工作，需要您创建云服务委托，将操作权限委托给该服务，让该服务以您的身份使用其他云服务，代替您进行一些资源运维工作。

企业项目

企业项目是项目的升级版，针对企业不同项目间资源的分组和管理，是逻辑隔离。企业项目中可以包含多个区域的资源，且项目中的资源可以迁入迁出。

关于企业项目ID的获取及企业项目特性的详细信息，请参见《[企业管理服务用户指南](#)》。

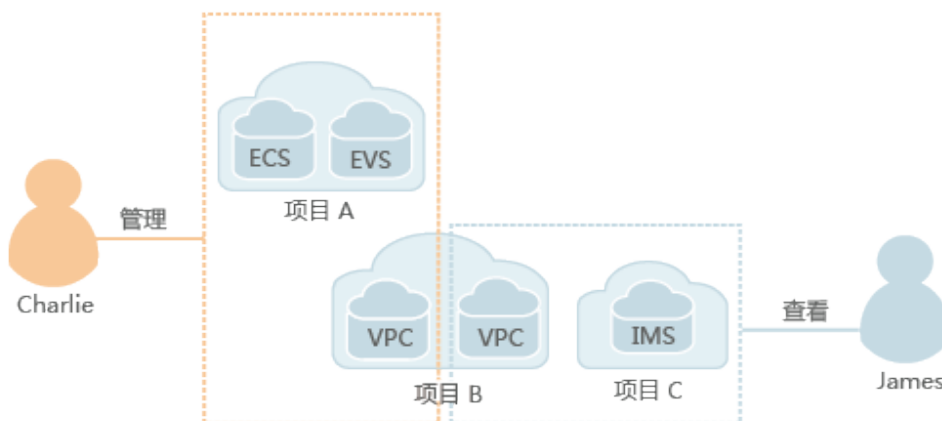
3 IAM 功能

IAM为您提供的主要功能包括：精细的权限管理、安全访问、敏感操作、通过用户组批量管理用户权限、区域内资源隔离、联合身份认证、委托其他账号或者云服务管理资源、设置账号安全策略。

精细的权限管理

使用IAM，您可以将账号内不同的资源按需分配给创建的IAM用户，实现精细的权限管理。例如：控制用户Charlie能管理项目B的VPC，而让用户James只能查看项目B中VPC的数据。

图 3-1 权限管理模型



安全访问

您可以使用IAM为用户或者应用程序生成身份凭证，不必与其他人员共享您的账号密码，系统会通过身份凭证中携带的权限信息允许用户安全地访问您账号中的资源。

敏感操作

IAM提供敏感操作保护功能，包括登录保护和操作保护，在您登录控制台或者进行敏感操作时，系统将要求您进行邮箱/手机/虚拟MFA的验证码的第二次认证，为您的账号和资源提供更高的安全保护。

通过用户组批量管理用户权限

您不需要为每个用户进行单独的授权，只需规划用户组，并将对应权限授予用户组，然后将用户添加至用户组中，用户就继承了用户组的权限。如果用户权限变更，只需在用户组中删除用户或将用户添加进其他用户组，实现快捷的用户授权。

区域内资源隔离

您可以通过在区域中创建子项目的功能，使得同区域下的各项目之间的资源相互隔离。

联合身份认证

如果您已经有自己的身份认证系统，您不需要在华为云中重新创建用户，可以通过身份提供商功能直接访问华为云，实现单点登录。

委托其他账号或者云服务管理资源

通过委托信任功能，您可以将自己的操作权限委托给更专业、高效的其他华为云账号或者云服务，这些账号或者云服务可以根据权限代替您进行日常工作。

设置账号安全策略

通过设置登录验证策略、密码策略及访问控制列表来提高用户信息和系统数据的安全性。

最终一致性

最终一致性是指您在IAM进行的操作，如创建用户和用户组、给用户组授权等，会由于IAM通过在华为云数据中心的各个服务器之间复制数据、实现多区域的数据同步时，可能导致已提交的修改延时生效。建议您在进行操作前，确认已提交的策略修改已经生效。

4 使用 IAM 授权的云服务

IAM为华为云其他服务提供认证和授权功能，在IAM中创建的用户，经过授权后可以根据权限使用系统中的其他服务。IAM支持的所有服务权限，请参见：[系统权限](#)。对于不支持使用IAM授权的服务，账号中创建的IAM用户无法使用该服务，请使用账号登录使用该服务。

- 服务：使用IAM授权的云服务名称。单击服务名，可以查看该服务支持的权限，以及不同权限间的区别。
- 所属区域：使用IAM授权时，该服务选择的授权区域。
 - 全局区域：服务部署时不区分物理区域，为全局级服务。在全局项目中进行授权，访问该服务时，不需要切换区域。
 - 其他区域：服务部署时通过物理区域划分，为项目级服务。在除全局区域外的其他区域中授权，仅在授权的区域生效，访问该服务时，需要先切换到对应区域。
- 控制台：该服务是否支持在IAM控制台进行权限管理。
- API接口：该服务是否支持调用API接口进行权限管理。
- 委托：您是否可以将操作权限委托给该服务，该服务可以以您的身份使用其他云服务，代替您进行日常工作。
- 策略：该服务是否支持通过策略进行权限管理。策略是以JSON格式描述一组权限集的语言，它可以精确地允许或拒绝用户对服务的资源类型进行指定的操作。

📖 说明

“√”表示支持，“x”表示暂不支持。

计算

服务	所属区域	控制台	API	服务委托	策略
弹性云服务器 ECS	除全局区域外的其他区域	√	√	√	√
云容器引擎 CCE	除全局区域外的其他区域	√	√	x	√
云容器实例 CCI	除全局区域外的其他区域	√	√	x	√

服务	所属区域	控制台	API	服务委托	策略
裸金属服务器 BMS	除全局区域外的 其他区域	√	√	√	√
弹性伸缩 AutoScaling	除全局区域外的 其他区域	√	√	x	√
云手机 CPH	除全局区域外的 其他区域	√	√	x	x
镜像服务 IMS	除全局区域外的 其他区域	√	√	√	√
函数工作流 FunctionGraph	除全局区域外的 其他区域	√	√	√	x

存储

服务	所属区域	控制台	API	委托	策略
云硬盘 EVS	除全局区域外的 其他区域	√	√	x	√
存储容灾服务 SDRS	除全局区域外的 其他区域	√	√	x	x
云服务器备份 CSBS	除全局区域外的 其他区域	√	√	x	x
云硬盘备份 VBS	除全局区域外的 其他区域	√	√	x	x
对象存储服务 OBS	全局区域	√	√	√	√
弹性文件服务 SFS	除全局区域外的 其他区域	√	√	x	√
内容分发网络 CDN	全局区域	√	√	x	√
云备份 CBR	除全局区域外的 其他区域	√	√	x	√

网络

服务	所属区域	控制台	API	委托	策略
虚拟私有云 VPC	除全局区域外的 其他区域	√	√	x	√

服务	所属区域	控制台	API	委托	策略
弹性负载均衡 ELB	除全局区域外的其他区域	√	√	x	√
云解析服务 DNS	全局区域	√	√	x	x
NAT网关	除全局区域外的其他区域	√	√	x	√
云专线 DC	除全局区域外的其他区域	√	x	x	x
虚拟专用网络 VPN	除全局区域外的其他区域	√	x	x	x
云连接 CC	除全局区域外的其他区域	√	x	x	x

数据库

服务	所属区域	控制台	API	委托	策略
云数据库 RDS	除全局区域外的其他区域	√	√	x	√
文档数据库服务 DDS	除全局区域外的其他区域	√	x	x	√
分布式数据库中间件 DDM	除全局区域外的其他区域	√	√	x	√
数据复制服务 DRS	除全局区域外的其他区域	√	√	x	x
数据管理服务 DAS	除全局区域外的其他区域	√	x	x	x

安全

服务	所属区域	控制台	API	委托	策略
Anti-DDoS流量清洗	除全局区域外的其他区域	√	√	x	x
DDoS高防服务	除全局区域外的其他区域	√	√	√	x
Web应用防火墙 WAF	除全局区域外的其他区域	√	x	x	x

服务	所属区域	控制台	API	委托	策略
漏洞扫描服务 VSS	除全局区域外的 其他区域	√	x	x	x
企业主机安全 HSS	除全局区域外的 其他区域	√	x	x	x
容器安全服务 CGS	除全局区域外的 其他区域	√	x	x	x
数据库安全服务 DBSS	除全局区域外的 其他区域	√	x	x	x
数据加密服务 DEW	除全局区域外的 其他区域	√	√	x	x
管理检测与响应 MDR	除全局区域外的 其他区域	√	x	x	x

迁移

服务	所属区域	控制台	API	委托	策略
主机迁移服务 SMS	-	x	x	x	x
对象存储迁移服 务 OMS	-	x	x	x	x
云数据迁移 CDM	除全局区域外的 其他区域	√	√	√	x

EI 企业智能

服务	所属区域	控制台	API	委托	细粒度策 略
ModelArts	除全局区域外的 其他区域	√	√	√	√
数据湖治理中心 DGC	除全局区域外的 其他区域	√	√	√	√
MapReduce服 务 MRS	除全局区域外的 其他区域	√	√	x	√
数据仓库服务 DWS	除全局区域外的 其他区域	√	√	√	√
表格存储服务 CloudTable	除全局区域外的 其他区域	√	√	x	x

服务	所属区域	控制台	API	委托	细粒度策略
数据湖探索 DLI	除全局区域外的其他区域	√	√	x	x
实时流计算服务 CS	除全局区域外的其他区域	√	√	√	√
数据接入服务 DIS	除全局区域外的其他区域	√	√	√	x
云搜索服务 CSS	除全局区域外的其他区域	√	√	√	x
图引擎服务 GES	除全局区域外的其他区域	√	√	√	x
数据湖工厂 DLF	除全局区域外的其他区域	√	√	x	x
推荐系统 RES	除全局区域外的其他区域	√	√	x	√
内容审核 Moderation	除全局区域外的其他区域	√	√	x	√
对话机器人服务 CBS	除全局区域外的其他区域	√	√	x	x

管理与部署

服务	所属区域	控制台	API	委托	细粒度策略
云监控	除全局区域外的其他区域	√	√	x	x
云审计服务 CTS	除全局区域外的其他区域	√	√	x	x
应用性能管理 APM	除全局区域外的其他区域	√	√	x	√
应用运维管理 AOM	除全局区域外的其他区域	√	√	x	√
云日志服务 LTS	除全局区域外的其他区域	√	√	x	√
标签管理服务 TMS	全局区域	√	√	x	x

应用服务

服务	所属区域	控制台	API	委托	策略
应用管理与运维平台 ServiceStage	除全局区域外的其他区域	√	√	x	x
分布式缓存服务 DCS	除全局区域外的其他区域	√	√	x	√
分布式消息服务 DMS	除全局区域外的其他区域	√	√	√	√
消息通知服务 SMN	除全局区域外的其他区域	√	√	x	x
微服务引擎 CSE	除全局区域外的其他区域	√	√	x	x
云性能测试服务 CPTS	除全局区域外的其他区域	√	√	x	x
区块链服务 BCS	除全局区域外的其他区域	√	√	x	x
API网关 APIG	除全局区域外的其他区域	√	√	x	x
应用编排服务 AOS	-	x	x	x	x
容器镜像服务 SWR	除全局区域外的其他区域	√	√	x	x
基因容器 GCS	除全局区域外的其他区域	√	√	x	√

视频

服务	所属区域	控制台	API	委托	策略
媒体处理 MPC	除全局区域外的其他区域	√	√	√	x
视频点播 VOD	除全局区域外的其他区域	√	√	√	x

云通信

服务	所属区域	控制台	API	委托	策略
联络中心	-	x	x	x	x

服务	所属区域	控制台	API	委托	策略
语音通话 RTC	除全局区域外的其他区域	√	√	√	x
消息短信 RTC	除全局区域外的其他区域	√	√	√	x
隐私保护通话 RTC	除全局区域外的其他区域	√	√	√	x

企业应用

服务	所属区域	控制台	API	委托	策略
企业集成平台 ROMA Connect	除全局区域外的其他区域	√	√	√	√

专属云

服务	所属区域	控制台	API	委托	策略
专属分布式存储 DSS	除全局区域外的其他区域	√	√	x	√

用户中心

服务	所属区域	控制台	API	委托	策略
账号中心 BSS	除全局区域外的其他区域	√	x	x	√
费用中心 BSS	除全局区域外的其他区域	√	x	x	√
资源中心 BSS	除全局区域外的其他区域	√	x	x	√
企业管理 EPS	全局区域	√	√	x	√
工单管理 Ticket	全局区域	√	√	x	x

5 个人数据保护机制

为了确保您的个人数据（例如用户名、密码、手机号码等）不被未经过认证、授权的实体或者个人获取，IAM通过加密存储个人数据、控制个人数据访问权限以及记录操作日志等方法防止个人数据泄露，保证您的个人数据安全。

收集范围

IAM收集及产生的个人数据如表1所示：

表 5-1 个人数据范围列表

类型	收集方式	是否可以修改	是否必须
用户名	<ul style="list-style-type: none"> 在创建用户时由用户在界面输入用户名 在调用API接口时输入用户名 	否	是 用户名是用户的身份标识信息
密码	<ul style="list-style-type: none"> 在创建用户、修改用户凭证、重置密码时由用户在界面输入密码 在调用API接口时输入密码 	是	否 用户可以选择使用AK/SK方式
邮箱	在创建用户、修改用户凭证、修改邮箱时由用户在界面输入邮箱	是	否
手机号	在创建用户、修改用户凭证、修改手机时由用户在界面输入手机号	是	否
AK (Access Key ID) /SK (Secret Access Key)	在“我的凭证”页面或者在IAM设置用户凭证时创建生成AK/SK	否 AK/SK不能直接修改，可以删除旧的AK/SK后重新创建AK/SK。	否 调用API接口时，需要使用AK/SK对请求进行签名

存储方式

IAM通过加密算法对用户个人敏感数据加密后进行存储。

- 用户名、AK：不属于敏感数据，明文存储
- 密码、邮箱、手机、SK：加密存储

访问权限控制

用户个人数据通过加密后存储在IAM数据库中，数据库的访问需要通过白名单的认证与授权。

二次认证

用户可以在“IAM>安全设置>敏感操作”中开启登录保护和操作保护，用户登录系统以及进行敏感操作时，需要二次认证（二次认证方式支持短信、邮箱，MFA验证码），有效保护用户敏感信息。

API 接口限制

- 用户调用API接口时，需要使用AK/SK进行认证。用户的AK/SK只能在首次创建时获取，如果没有获取或者遗失，只能重新创建AK/SK，保证使用AK/SK的为用户本人，有效防止个人数据泄露。
- IAM不提供批量查询和修改个人数据的API接口。

日志记录

用户个人数据的所有操作，包括增加、修改、查询和删除，IAM都会记录审计日志并上传至云审计服务（CTS），用户可以并且仅可以查看自己的审计日志。

6 权限管理

如果您需要针对统一身份认证服务，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。

通过IAM，您可以在华为云账号中给员工创建IAM用户，并授权控制他们对华为云资源的访问范围。例如您的员工中有负责进行项目规划的人员，您希望他们拥有IAM的查看权限，但是不希望他们拥有删除IAM用户、项目等高危操作的权限，那么您可以使用IAM为项目规划人员创建IAM用户，通过授予仅能查看IAM，但是不允许使用IAM的权限，控制他们对IAM控制台的使用范围。

IAM 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，IAM支持的API授权项请参见[权限及授权项说明](#)。

如表1所示，包括了IAM的所有系统权限。

表 6-1 IAM 系统权限

系统角色/策略名称	描述	类别	角色/策略内容
FullAccess	基于策略授权的所有服务的所有权限，拥有该权限的用户可以完成基于策略授权的所有服务的所有操作。	系统策略	FullAccess策略内容
IAM ReadOnlyAccess	统一身份认证服务的只读权限，拥有该权限的用户仅能查看统一身份认证服务数据。	系统策略	IAM ReadOnlyAccess策略内容
Security Administrator	统一身份认证服务的管理员权限，拥有该权限的用户拥有IAM支持的所有权限，包括创建、删除IAM用户等操作。	系统角色	Security Administrator角色内容
Agent Operator	统一身份认证服务的切换角色权限，拥有该权限的用户（被委托方）可以切换角色并访问委托方账号中的资源。	系统角色	Agent Operator角色内容
Tenant Guest	除统一身份认证服务外，其他所有服务的只读权限。	系统策略	Tenant Guest角色内容
Tenant Administrator	除统一身份认证服务外，其他所有服务的管理员权限。	系统策略	Tenant Administrator角色内容

表2列出了IAM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。

 说明

Tenant Guest、Tenant Administrator是统一身份认证服务提供的华为云基础权限，不包含IAM的任何权限，因此下表中不进行解析。

表 6-2 常用操作与系统权限的关系

操作	Security Administrator	Agent Operator	FullAccess	IAM ReadOnlyAccess
创建IAM用户	√	×	√	×
查询IAM用户详情	√	×	√	√
修改IAM用户信息	√	×	√	×
查询IAM用户安全设置	√	×	√	√

操作	Security Administrator	Agent Operator	FullAccess	IAM ReadOnlyAccess
修改IAM用户安全设置	√	×	√	×
删除IAM用户	√	×	√	×
创建用户组	√	×	√	×
查询用户组详情	√	×	√	√
修改用户组信息	√	×	√	×
添加用户到用户组	√	×	√	×
从用户组移除用户	√	×	√	×
删除用户组	√	×	√	×
为用户组授权	√	×	√	×
移除用户组权限	√	×	√	×
创建自定义策略	√	×	√	×
修改自定义策略	√	×	√	×
删除自定义策略	√	×	√	×
查询权限详情	√	×	√	√
创建委托	√	×	√	×
查询委托	√	×	√	√
修改委托	√	×	√	×
切换角色	×	√	√	×
删除委托	√	×	√	×
为委托授权	√	×	√	×
移除委托权限	√	×	√	×
创建项目	√	×	√	×
查询项目	√	×	√	√

操作	Security Administrator	Agent Operator	FullAccess	IAM ReadOnlyAccess
修改项目	√	×	√	×
删除项目	√	×	√	×
创建访问密钥	√	×	√	×
查询访问密钥	√	×	√	√
修改访问密钥	√	×	√	×
删除访问密钥	√	×	√	×
创建身份提供商	√	×	√	×
导入 Metadata 文件	√	×	√	×
查询 Metadata 文件	√	×	√	√
查询身份提供商	√	×	√	√
查询协议	√	×	√	√
查询映射	√	×	√	√
更新身份提供商	√	×	√	×
更新协议	√	×	√	×
更新映射	√	×	√	×
删除身份提供商	√	×	√	×
删除协议	√	×	√	×
删除映射	√	×	√	×
查询配额	√	×	√	×

FullAccess 策略内容

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Action": [
        "*"
      ],
    }
  ],
}
```

```
    "Effect": "Allow"  
  }  
]  
}
```

IAM ReadOnlyAccess 策略内容

```
{  
  "Version": "1.1",  
  "Statement": [  
    {  
      "Action": [  
        "iam:*:get*",  
        "iam:*:list*",  
        "iam:*:check*"  
      ],  
      "Effect": "Allow"  
    }  
  ]  
}
```

Security Administrator 角色内容

```
{  
  "Version": "1.0",  
  "Statement": [  
    {  
      "Action": [  
        "iam:agencies:*",  
        "iam:credentials:*",  
        "iam:groups:*",  
        "iam:identityProviders:*",  
        "iam:mfa:*",  
        "iam:permissions:*",  
        "iam:projects:*",  
        "iam:quotas:*",  
        "iam:roles:*",  
        "iam:users:*",  
        "iam:securitypolicies:*"  
      ],  
      "Effect": "Allow"  
    }  
  ]  
}
```

Agent Operator 角色内容

```
{  
  "Version": "1.0",  
  "Statement": [  
    {  
      "Action": [  
        "iam:tokens:assume"  
      ],  
      "Effect": "Allow"  
    }  
  ]  
}
```

Tenant Guest 角色内容

```
{  
  "Version": "1.1",  
  "Statement": [  
    {  
      "Action": [  
        "obs:*:get*",  
        "obs:*:list*",  
        "obs:*:delete*"  
      ],  
      "Effect": "Allow"  
    }  
  ]  
}
```

```
    "obs:*:head*",
  ],
  "Effect": "Allow"
},
{
  "Condition": {
    "StringNotEqualsIgnoreCase": {
      "g:ServiceName": [
        "iam"
      ]
    }
  },
  "Action": [
    "**:*:get*",
    "**:*:list*",
    "**:*:head*"
  ],
  "Effect": "Allow"
}
]
```

Tenant Administrator 角色内容

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Action": [
        "obs:*:*"
      ],
      "Effect": "Allow"
    },
    {
      "Condition": {
        "StringNotEqualsIgnoreCase": {
          "g:ServiceName": [
            "iam"
          ]
        }
      },
      "Action": [
        "**:*:*"
      ],
      "Effect": "Allow"
    }
  ]
}
```

7 约束与限制

IAM中的用户数、用户组数等有限定的配额，其中“是否支持修改”列标示“√”的，表示该限制项可以修改。如果当前资源配额无法满足业务需要，您可以申请扩大配额，具体方法请参见：[如何修改配额](#)。

限制项	限制值	是否支持修改
IAM用户数	50	√
用户组数	20	√
一个用户组中可添加的用户数	账号下的IAM用户数	x
委托数	50	√
用户可加入的用户组数	10	x
用户可创建的访问密钥（AK/SK）数	2	x
用户可绑定的虚拟MFA设备数	1	x
自定义策略数	200	√
委托可绑定策略数	10	x
一个项目内用户组可绑定的策略数（包括系统策略和自定义策略）	25	x
项目数	10	√
用户名的字符数	32	x
用户组名的字符数	64	x
策略名称的字符数	64	x
自定义策略	字符数	x
	Statement	8个/策略

限制项		限制值	是否支持修改
	Action	100个/Statement Action数组	x
	Resource	10个/Statement Resource数组	x
	Condition	10个/statement Condition数组	x
委托名称的字符数		64	x
身份提供商	数量	10	√
	名称字符数	64	x

8 修订记录

表 8-1 修订记录

日期	修订记录
2020-12-30	第十四次正式发布。 根据登录界面词条变更刷新 基本概念 章节截图。
2020-10-27	第十三次正式发布。 根据登录方式变更刷新 基本概念 章节截图。
2020-09-30	第十二次正式发布。 新增 权限管理 章节。
2020-06-11	第十一次正式发布。 约束与限制 中“用户可加入的用户组数”限制值减少至10。
2020-06-08	第十次正式发布。 基本概念 中增加HUAWEI ID说明，并更新登录界面截图。
2020-01-19	第九次正式发布。 <ul style="list-style-type: none"> • 优化基本概念中“权限”的概念。 • 约束与限制中新增“项目数”的限制。
2019-11-20	第八次正式发布。 约束与限制 中“自定义策略数”限制值增加至200。
2019-06-26	第七次正式发布。 使用IAM授权的云服务 中新增各服务的跳转链接。
2019-06-05	第六次正式发布。 优化 什么是IAM 、 基本概念 和 IAM功能 章节。
2019-03-05	第五次正式发布。 新增 约束与限制 章节。

日期	修订记录
2019-02-20	第四次正式发布。 新增 基本概念 章节。
2019-01-15	第三次正式发布。 新增 使用IAM授权的云服务 章节。
2018-08-10	第二次正式发布。 本次变更说明如下： 新增 个人数据保护机制 章节。
2018-03-30	第一次正式发布。