统一身份认证服务(IAM2.0)
8.5.1
产品介绍

文档版本 01
发布日期 2025-09-23

华为云计算技术有限公司

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。

目 录

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，您只需要为您账号中的资源进行付费。

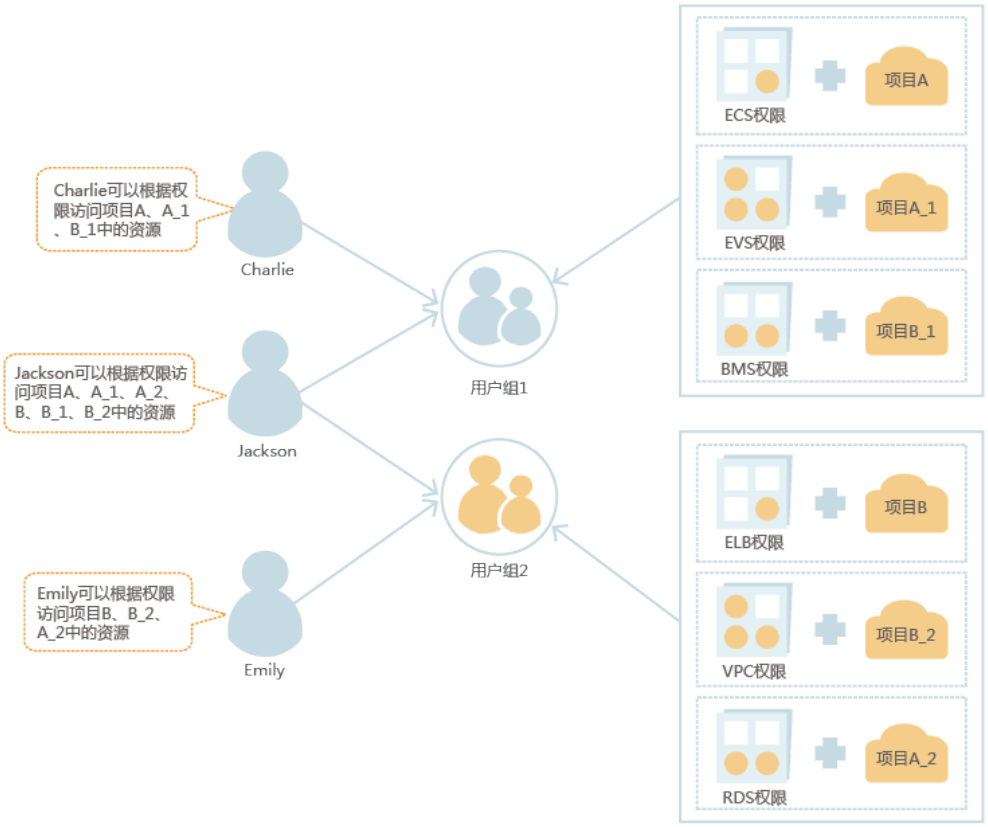
IAM 的优势

对华为云的资源进行精细访问控制

您注册华为云后，系统自动创建账号，账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账号时，避免分享账号的密码。

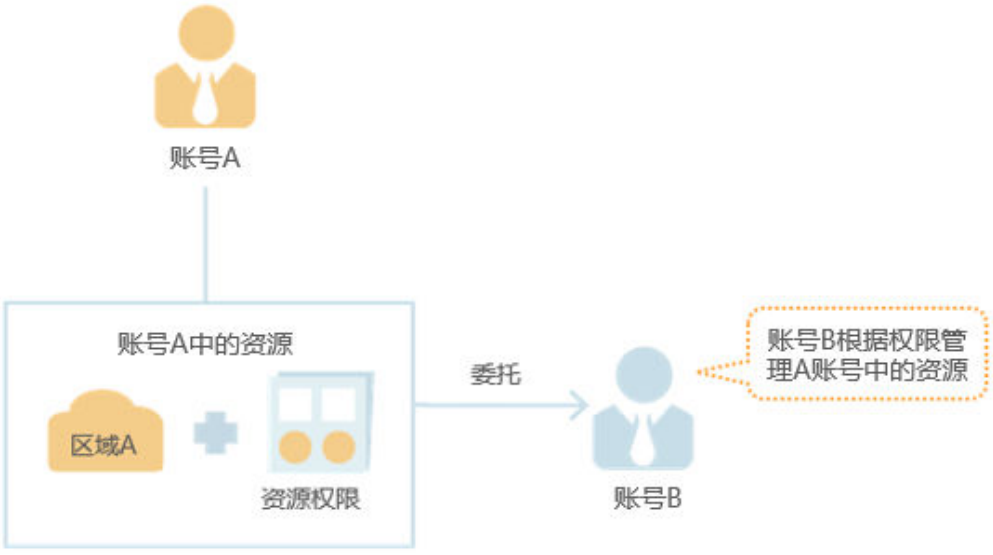
除了IAM外，还有企业管理服务同样可以进行资源权限管理，相对于IAM，企业管理对资源的控制粒度更为精细，同时还支持企业项目费用的管理，建议结合企业需求选择IAM或是企业管理进行资源权限管理，关于两者的详细区别，请参见：**IAM与企业管理的区别**。



跨账号的资源操作与授权

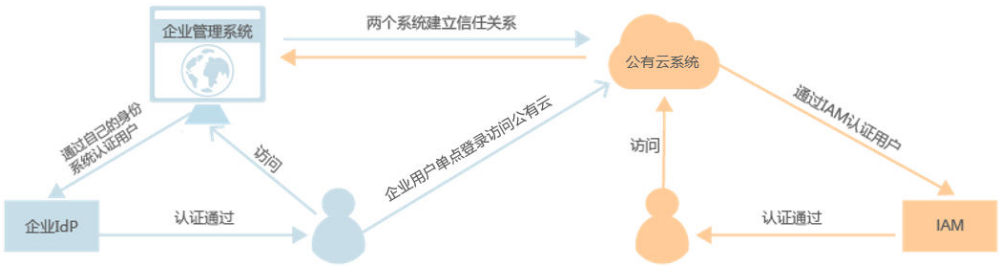
如果您在华为云购买了多种资源，其中一种资源希望由其它账号管理，您可以使用IAM提供的委托功能。

例如您希望将资源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账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销对代运维公司的授权。下图中账号A即为委托方，账号B为被委托方。



使用企业已有账号登录华为云

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账号直接登录华为云，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。详情请参考**如何进入IAM控制台**。
- **REST API**

  您可以使用IAM提供的REST API接口以编程方式访问IAM。详情请参考：**API参考**。

推荐您在使用IAM前，开通云审计服务CTS，方便查看、审计以及回溯IAM的关键操作记录。详情请参考：**IAM支持审计的关键操作**。

2 基本概念

本章为您介绍使用IAM服务时常用的基本概念：账号、IAM用户、账号与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。

账号

当您首次使用华为云时注册的账号，该账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。账号统一接收所有IAM用户进行资源操作时产生的费用账单。

账号不能在IAM中修改和删除，您可以在账号中心修改账号信息，如果您需要删除账号，可以在账号中心进行注销。

IAM 用户

由账号在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），根据账号授予的权限使用资源。IAM用户不进行独立的计费（无IAM的账单），由所属账号统一付费。

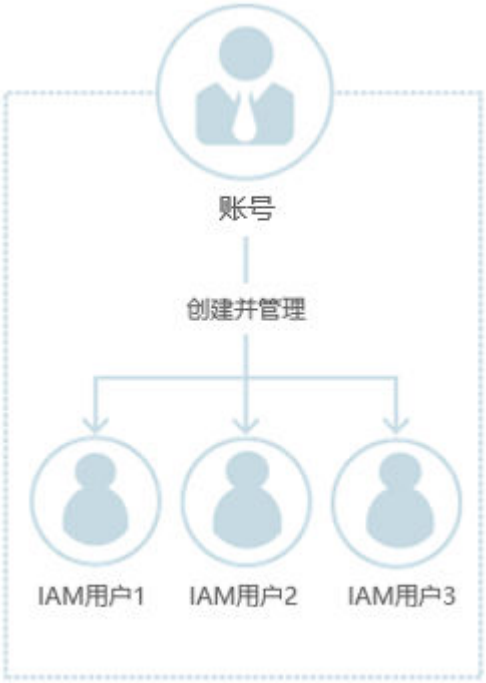
如果您忘记了IAM用户的登录密码，可以重置密码，重置方法请参见：**忘记账号密码**。

图 2-1 IAM 用户登录

账号与 IAM 用户的关系

账号与IAM用户可以类比为父子关系，账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用户由账号创建，只能拥有账号授予的资源使用权限，账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账号中，IAM用户不需要为资源付费。

图 2-2 账号与 IAM 用户



管理员

IAM的使用对象为管理员，管理员通常指的是：

- 账号：账号可以使用所有服务，包括IAM。
- admin用户组中的用户：IAM默认用户组admin中的用户，可以使用所有服务，包括IAM。
- 授予了“Security Administrator”权限的用户：具备该权限的用户为IAM管理员，可以使用IAM。

授权

授权是您将IAM用户完成具体工作需要的权限授予IAM用户，授权通过策略定义的权限生效。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，管理您账号中的ECS资源。

用户组

用户组是IAM用户的集合，IAM可以通过用户组功能实现用户的授权。您创建的IAM用户，加入特定用户组后，将具备对应用户组的权限。当某个IAM用户加入多个用户组时，此IAM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，包括但不仅限于创建用户组及用户、修改用户组权限、管理资源等。

图 2-3 用户组与用户

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。目前支持可视化视图、JSON视图两种自定义策略配置方式。

图 2-4 权限内容示例

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

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中管理账号以及账号下IAM用户的身份凭证。

- 密码：常见的身份凭证，密码可以用来登录控制台，还可以调用API接口。
- 访问密钥：即AK/SK（Access Key ID/Secret Access Key），调用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

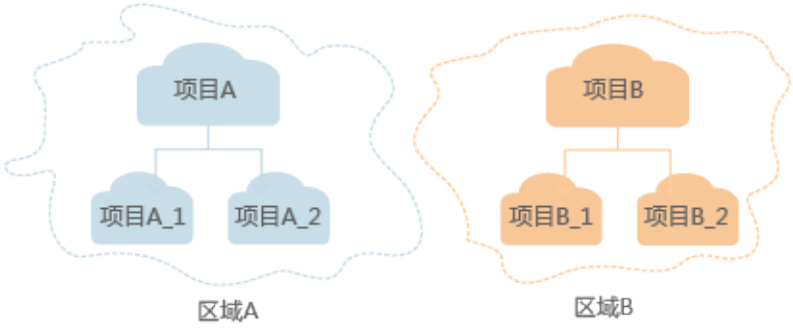
虚拟MFA（Multi-Factor Authentication，简称MFA），是一款能产生6位数字认证码的应用程序，遵循基于时间的一次性密码 （Time-Based One-Time Password，TOTP）标准。MFA设备可以基于硬件也可以基于软件，华为云目前仅支持基于软件的虚拟MFA，即虚拟MFA应用程序，可以在移动硬件设备（包括智能手机）上运行，获取认证码并进行身份认证。关于虚拟MFA的详细使用方法请参考：**虚拟MFA**。

项目

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，用户可以访问您账号中该

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 2-5 项目



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**》。

委托

委托根据委托对象的不同，分为委托其他账号和委托其他云服务。

- 委托其他账号：通过委托信任功能，您可以将自己账号中的资源操作权限委托给更专业、高效的其他账号，被委托的账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。

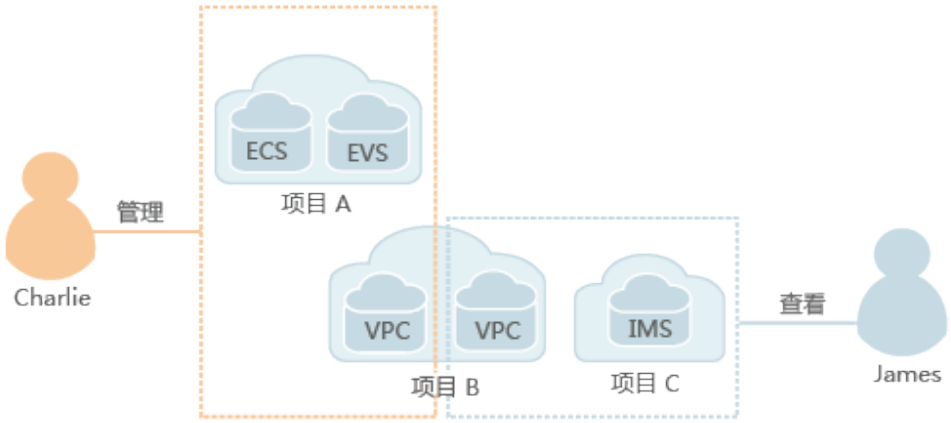
3 IAM 功能

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。**支持使用IAM授权的云服务请参见下方表格内容。

表格参数说明如下：

- 服务：使用IAM授权的云服务名称。
- 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。
- 企业项目：该服务是否支持基于企业项目授权。关于企业项目请参见《**企业管理服务用户指南**》

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	企业项目
弹性云服务器 ECS	除全局区域外的其他区域	√	√	√	√	√

服务	所属区域	控制台	API	服务委托	策略	企业项目
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	√	√
云手机服务器 CPH	除全局区域外的其他区域	√	√	x	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	√
专属主机 DeH	除全局区域外的其他区域	√	x	x	√	√

存储

服务	所属区域	控制台	API	委托	策略	企业项目
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	x
云服务器备份 CSBS	除全局区域外的其他区域	√	√	x	x	x
云硬盘备份 VBS	除全局区域外的其他区域	√	√	x	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	企业项目
虚拟私有云 VPC	除全局区域外的其他区域	√	√	x	√	√
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	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	√	√
VPC终端节点 VPCEP	除全局区域外的其他区域	√	√	x	x	x

容器

服务	所属区域	控制台	API	委托	策略	企业项目
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	√	√
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	√	√

数据库

服务	所属区域	控制台	API	委托	策略	企业项目
云数据库 RDS	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	企业项目
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	√	√
数据管理服务 DAS	除全局区域外的其他区域	√	x	x	x	x
云数据库（GeminiDB）	除全局区域外的其他区域	√	√	x	√	√

安全与合规

服务	所属区域	控制台	API	委托	策略	企业项目
Anti-DDoS流量清洗	除全局区域外的其他区域	√	√	x	x	x
DDoS防护 AAD	除全局区域外的其他区域	√	√	√	x	√
DDoS防护 CNAD	全局区域	√	√	x	√	x
Web应用防火墙 WAF	除全局区域外的其他区域	√	x	x	x	√
云防火墙 CFW	除全局区域外的其他区域	√	x	x	√	x
漏洞扫描服务 VSS	除全局区域外的其他区域	√	x	x	x	x
主机安全服务 HSS	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	x
SSL证书管理 SCM	全局区域	√	√	x	√	x
容器安全服务 CGS	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	企业项目
云堡垒机 CBH	除全局区域外的其他区域	√	√	x	√	x
数据安全中心 DSC	除全局区域外的其他区域	√	√	x	√	x

管理与监管

服务	所属区域	控制台	API	委托	细粒度策略	企业项目
统一身份认证服务 IAM	全局区域	√	√	x	√	x
云监控服务 CES	除全局区域外的其他区域	√	√	x	√	√
云审计服务 CTS	除全局区域外的其他区域	√	√	x	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	x

应用服务

服务	所属区域	控制台	API	委托	策略	企业项目
应用管理与运维平台 ServiceStage	除全局区域外的其他区域	√	√	x	x	x
分布式缓存服务 DCS	除全局区域外的其他区域	√	√	√	√	√
分布式消息服务 Kafka版	除全局区域外的其他区域	√	√	x	√	√
分布式消息服务 RabbitMQ版	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	企业项目
分布式消息服务 RocketMQ版	除全局区域外的其他区域	√	√	x	√	√
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	√
性能测试CodeArts PerfTest	除全局区域外的其他区域	√	√	x	x	x
API网关 APIG	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	√	√

专属云

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

迁移

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

智能边缘

服务	所属区域	控制台	API	委托	策略	企业项目
智能边缘云 IEC	全局区域	√	x	x	√	x

EI 企业智能

服务	所属区域	控制台	API	委托	细粒度策略	企业项目
ModelArts	除全局区域外的其他区域	√	√	√	√	√
数据治理中心 DataArts Studio	除全局区域外的其他区域	√	√	√	√	x
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	√
数据湖探索 DLI	除全局区域外的其他区域	√	√	x	x	√
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	√
内容审核 Moderation	除全局区域外的其他区域	√	√	x	√	x
对话机器人服务 CBS	除全局区域外的其他区域	√	√	x	x	x
华为HiLens	除全局区域外的其他区域	√	x	x	√	x
可信智能计算服务 TICS	除全局区域外的其他区域	√	x	x	√	x

企业应用

服务	所属区域	控制台	API	委托	策略	企业项目
云桌面 Workspace	除全局区域外的其他区域	√	√	x	×	x
企业集成平台 ROMA Connect	除全局区域外的其他区域	√	√	√	√	√

服务	所属区域	控制台	API	委托	策略	企业项目
云速建站 CloudSite	除全局区域外的其他区域	√	x	√	√	x

云通信

服务	所属区域	控制台	API	委托	策略	企业项目
语音通话 VoiceCall	除全局区域外的其他区域	√	√	√	x	x
消息&短信 MSGSMS	除全局区域外的其他区域	√	√	√	√	x
隐私保护通话 PrivateNumber	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	企业项目
媒体处理 MPC	除全局区域外的其他区域	√	√	√	x	x
视频点播 VOD	除全局区域外的其他区域	√	√	√	√	x

开发与运维

服务	所属区域	控制台	API	委托	策略	企业项目
软件开发生产线 CodeArts	除全局区域外的其他区域	√	x	x	√	√
需求管理CodeArts Req	除全局区域外的其他区域	√	√	x	√	x
CloudIDE	除全局区域外的其他区域	√	√	x	√	x

用户服务

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

其他

服务	所属区域	控制台	API	委托	策略	企业项目
消息中心	除全局区域外的其他区域	√	x	x	√	x

5 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，您可以在账号中给员工创建IAM用户，并授权控制他们对资源的访问范围。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服务支持的所有服务系统权限请参见：**系统权限**。

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5-1**所示，包括了IAM的所有系统权限。

表 5-1 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5-2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基础权限，不包含IAM的任何权限，因此下表中不进行解析。

表 5-2 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	√	×	√	×

访问密钥保护开启的情况下，仅管理员可以管理访问密钥。IAM用户如需创建、启用/停用或删除自己的访问密钥，需要管理员**关闭访问密钥保护**。访问密钥保护默认关闭。

若当前IAM用户要对其他IAM用户的访问密钥进行管理，则可以参考**表5-3**为当前IAM用户选择合适的系统权限。例如IAM用户A要为IAM用户B创建访问密钥，则IAM用户A需要拥有Security Administrator或者FullAccess权限。

表 5-3 访问密钥操作与系统权限的关系

操作	Security Administrator	Agent Operator	FullAccess	IAM ReadOnlyAccess
创建访问密钥（为其他IAM用户）	√	×	√	×
查询访问密钥列表（为其他IAM用户）	√	×	√	√
修改访问密钥（为其他IAM用户）	√	×	√	×
删除访问密钥（为其他IAM用户）	√	×	√	×

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:*: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"
        }
    ]
}
```

6 安全

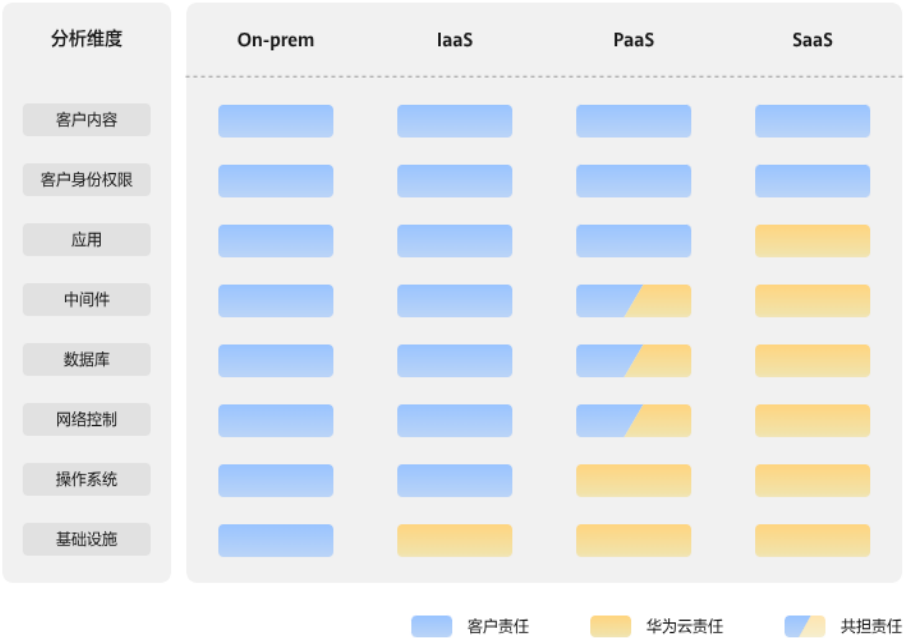
6.1 责任共担

华为云秉承“将公司对网络和业务安全性保障的责任置于公司的商业利益之上”。针对层出不穷的云安全挑战和无孔不入的云安全威胁与攻击，华为云在遵从法律法规业界标准的基础上，以安全生态圈为护城河，依托华为独有的软硬件优势，构建面向不同区域和行业的完善云服务安全保障体系。

与传统的本地数据中心相比，云计算的运营方和使用方分离，提供了更好的灵活性和控制力，有效降低了客户的运营负担。正因如此，云的安全性无法由一方完全承担，云安全工作需要华为云与您共同努力，如图6-1所示。

- **华为云**：无论在任何云服务类别下，华为云都会承担基础设施的安全责任，包括安全性、合规性。该基础设施由华为云提供的物理数据中心（计算、存储、网络等）、虚拟化平台及云服务组成。在PaaS、SaaS场景下，华为云也会基于控制原则承担所提供服务或组件的安全配置、漏洞修复、安全防护和入侵检测等职责。
- **客户**：无论在任何云服务类别下，客户数据资产的所有权和控制权都不会转移。在未经授权的情况，华为云承诺不触碰客户数据，客户的内容数据、身份和权限都需要客户自身看护，这包括确保云上内容的合法合规，使用安全的凭证（如强口令、多因子认证）并妥善管理，同时监控内容安全事件和账号异常行为并及时响应。

图 6-1 华为云安全责任共担模型



云安全责任基于控制权，以可见、可用作为前提。在客户上云的过程中，资产（例如设备、硬件、软件、介质、虚拟机、操作系统、数据等）由客户完全控制向客户与华为云共同控制转变，这也就意味着客户需要承担的责任取决于客户所选取的云服务。如图6-1所示，客户可以基于自身的业务需求选择不同的云服务类别（例如IaaS、PaaS、SaaS服务）。不同的云服务类别中，每个组件的控制权不同，这也导致了华为云与客户的责任关系不同。

- 在On-prem场景下，由于客户享有对硬件、软件和数据等资产的全部控制权，因此客户应当对所有组件的安全性负责。
- 在IaaS场景下，客户控制着除基础设施外的所有组件，因此客户需要做好除基础设施外的所有组件的安全工作，例如应用自身的合法合规性、开发设计安全，以及相关组件（如中间件、数据库和操作系统）的漏洞修复、配置安全、安全防护方案等。
- 在PaaS场景下，客户除了对自身部署的应用负责，也要做好自身控制的中间件、数据库、网络控制的安全配置和策略工作。
- 在SaaS场景下，客户对客户内容、账号和权限具有控制权，客户需要做好自身内容的保护以及合法合规、账号和权限的配置和保护等。

6.2 身份认证与访问控制

6.2.1 身份认证

华为云IAM服务要求访问请求方出示身份凭证，并进行身份合法性校验，同时提供登录保护和登录验证策略加固身份认证安全。

身份凭证及其安全性

IAM服务支持通过账号和IAM用户两种身份访问，并且均支持通过用户名密码、访问密钥和临时访问密钥进行身份认证。详见**表6-1**，每一种身份凭证，IAM都对其进行安全性设计，目的是保护用户数据，让用户更安全地访问IAM。

表 6-1 IAM 身份凭证和安全性设计

访问凭证	安全性简要说明	详细介绍
用户名、密码	按需配置用户密钥字符种类和最小长度，支持配置密码有效期策略和密码最短使用时间策略。	**密码策略**
访问密钥	华为云通过AK识别访问用户的身份，通过SK对请求数据进行签名验证，用于确保请求的机密性、完整性和请求者身份的正确性。	**访问密钥**
临时访问密钥	临时访问密钥除了具备访问密钥特性，还具备时效性，可对有效期进行设置，到期后无法重复使用，只能重新获取。	**临时访问密钥**

登录保护及登录验证策略

如**表6-2**所示，除了要求用户登录出示凭证并验证合法性，IAM还提供登录保护机制，支持登录验证策略，防止用户信息被非法盗用。

表 6-2 登录保护和登录验证策略

登录保护手段	简要说明	详细介绍
登录保护	除了在登录页面输入用户名和密码外（第一次身份验证），用户登录华为云还需要在登录验证页面输入验证码（第二次身份验证）。 验证设备支持手机、邮箱和虚拟MFA设备，详见**多因素认证**。	**登录保护**

登录保护手段	简要说明	详细介绍
登录验证策略	IAM支持**会话超时策略**，超过规定时长未操作界面需重新登录；支持**账号锁定策略**，登录失败次数过多触发账号锁定；支持**账号停用策略**，长时间未登录触发账号停用；支持**最近登录提示**，用户可查看上次登录时间。	**登录验证策略**

6.2.2 访问控制

IAM服务支持通过IAM细粒度授权策略和ACL进行访问控制。

表 6-3 IAM 的访问控制

访问控制方式	简要说明	详细介绍
IAM细粒度授权策略	将IAM服务本身的权限做了角色或者细粒度划分，角色和策略明确定义了IAM服务允许或者拒绝的用户操作。例如拥有IAM ReadOnlyAccess的用户和用户组，只拥有IAM服务数据的只读权限。IAM也支持**自定义策略**划分IAM服务权限。	**IAM权限**
ACL	设置访问控制策略，限制用户只能从特定IP地址区间、网段及VPC Endpoint登录 IAM 控制台或访问OpenAPI。	**访问控制**

6.3 数据保护技术

6.3.1 IAM 侧

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对用户数据的存储和传输进行加密保护，以防止个人数据泄露，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6-4**所示：

表 6-4 个人数据范围列表

类型	收集方式	用途	是否可以修改	是否必须
用户名	• 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	• 标识用户身份 • 控制台界面或API调用时进行身份认证	管理员权限可通过API修改	是 用户名是用户的身份标识信息
密码	• 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	控制台界面或API调用时进行身份认证	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	• 标识用户身份 • 控制台界面进行身份认证 • 接收消息	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	• 标识用户身份 • 控制台界面进行身份认证 • 接收消息	是	否
AK（Access Key ID）/SK（Secret Access Key）	在“我的凭证”页面或者在“统一身份认证>用户>安全设置>访问密钥”处创建生成AK/SK	API调用时进行身份认证	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

数据存储安全

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：使用加盐的SHA512算法进行加密存储。
- 邮箱、手机号、SK：使用安全AES算法进行加密存储。

数据传输安全

用户个人敏感数据（包括密码）将通过TLS 1.2进行传输中加密，所有华为云IAM的API调用都支持 HTTPS 来对传输中的数据进行加密。

6.3.2 租户侧

责任共担模式适用于华为云IAM中的数据保护。如该模式中所述，IAM负责服务自身的安全，提供安全的数据保护机制。租户负责安全使用IAM服务，包括使用时的安全参数配置，以及企业对自身权限的拆解和授予。

出于数据保护目的，建议您参考**安全使用IAM**的内容更规范地使用IAM服务，以便更加妥善地保护您的数据。

6.4 服务韧性

华为云数据中心按规则部署在全球各地，所有数据中心都处于正常运营状态，无一闲置。数据中心互为灾备中心，如一地出现故障，系统在满足合规政策前提下自动将客户应用和数据转离受影响区域，保证业务的连续性。为了减少由硬件故障、自然灾害或其他灾难带来的服务中断，华为云为所有数据中心提供灾难恢复计划。

华为云IAM作为基础身份认证服务，已面向全球用户服务，并在多个分区部署，具有更高的可用性、容错性和可扩展性。

6.5 审计与监控

云审计服务（Cloud Trace Service，以下简称CTS），是华为云安全解决方案中专业的日志审计服务，提供对各种云资源操作记录的收集、存储和查询功能，可用于支撑安全分析、合规审计、资源跟踪和问题定位等常见应用场景。

CTS可记录的IAM操作列表详见**IAM支持审计的关键操作**中的“CTS支持的IAM操作列表”。用户开通云审计服务并创建和配置追踪器后，CTS开始记录操作事件用于审计，开通方法参见**IAM支持审计的关键操作**。开通云审计服务后，可**在CTS事件列表查看云审计事件**，云审计服务保存最近7天的操作日志。

CTS支持**创建关键操作通知**。用户可将与IAM相关的高危敏感操作，作为关键操作加入到CTS的实时监控列表中进行监控跟踪。当用户使用IAM服务时，如果触发了监控列表中的关键操作，那么CTS会在记录操作日志的同时，向相关订阅者实时发送通知。

6.6 认证证书

合规证书

华为云服务及平台通过了多项国内外权威机构（ISO/SOC/PCI等）的安全合规认证，用户可自行**申请下载**合规资质证书。

图 6-2 合规证书下载

资源中心

华为云还提供以下资源来帮助用户满足合规性要求，具体请查看**资源中心**。

图 6-3 资源中心

7 约束与限制

本节介绍IAM在使用过程中的约束和限制。

配额

查看每个配额项目支持的默认配额，请参考**怎样查看我的配额**，登录控制台查询您的配额详情。如果需要扩大配额，可以**提交工单**申请提升配额。

表 7-1 配额

资源分类	限制项	默认配额限制	是否支持调整
用户	IAM用户数	50	是 **提交工单**申请提升配额
	用户名的字符数	64	否
	用户可加入的用户组数	10	否
	用户可创建的访问密钥（AK/SK）数	2	否
	用户可绑定的虚拟MFA设备数	1	否
	一个用户基于企业项目可绑定的权限数（包括系统权限和自定义策略）	500	是 **提交工单**申请提升配额
用户组	用户组数	20	是 **提交工单**申请提升配额
	用户组名的字符数	128	否
	一个用户组中可添加的用户数	账号下的IAM用户数	否

资源分类	限制项	默认配额限制	是否支持调整
	一个用户组基于IAM项目可绑定的权限数（包括系统权限和自定义策略）	200	是 提交工单申请提升配额
	一个用户组基于企业项目可绑定的权限数（包括系统权限和自定义策略）	500	是 提交工单申请提升配额
项目	项目数	10	是 提交工单申请提升配额
策略	策略名称的字符数	128	否
自定义策略	自定义策略个数	200	是 提交工单申请提升配额
	字符数	6144	否
	Statement	无限制	否
	Action	无限制	否
	Resource	无限制	否
	Condition	无限制	否
委托	委托数	50	是 提交工单申请提升配额
	委托名称的字符数	64	否
	一个委托可绑定的权限数（包括系统权限和自定义策略）	200	是 提交工单申请提升配额
身份提供商	数量	10	是 提交工单申请提升配额
	名称字符数	64	否
	账号中所有身份提供商的映射规则总数	10	是 提交工单申请提升配额
	联邦虚拟用户绑定的用户组数	100	否

资源分类	限制项	默认配额限制	是否支持调整
	联邦虚拟用户的用户名的字符数	255	否

命名限制

表 7-2 命名限制

限制项	说明
用户名	● 长度不能超过64个字符。 ● 只能包含如下字符：大小写字母、空格、数字或特殊字符(-_.)且不能以数字或空格开头。
用户组名	● 长度不能超过128个字符。 ● 只能包含如下字符：中文、大小写字母、数字、空格或特殊字符(-_)。
自定义策略名	● 长度不能超过128个字符。 ● 只能包含如下字符：大小写字母、中文、数字、空格或特殊字符(-_.,)。
项目名	● 长度不能超过53个字符。 ● 只能包含如下字符：大小写字母、数字或特殊字符(-_)。
委托名	长度不能超过64个字符。
身份提供商名	● 长度不能超过64个字符。 ● 只能包含如下字符：大小写字母、数字或特殊字符(-_)。

操作限制

表 7-3 操作限制

操作场景	限制项	限制说明
创建IAM用户	单次最多创建IAM用户数量	10个
	IAM用户名设置	不能与当前已创建的IAM用户同名。
	手机号和邮件地址	手机号和邮件地址只能绑定一个用户（IAM用户或账号），不可重复绑定。

操作场景	限制项	限制说明
	IAM用户密码	密码不能是用户名或者用户名的倒序，例如：用户名为A12345，则密码不能为A12345、a12345、54321A和54321a。
创建自定义策略	策略内容	• 授权项、条件键和资源类型均不区分大小写。 • 如果一个自定义策略中包含多个服务的授权语句，这些服务必须是同一属性，即都是全局级服务或者项目级服务。如果需要同时设置全局服务和项目级服务的自定义策略，请创建两条自定义策略。
创建委托	被委托的账号	被委托的账号只能是账号，不能是联邦用户、IAM用户。
配置安全设置	敏感操作	• 一个用户（IAM用户或账号）敏感操作进行二次验证的设备仅能绑定一个手机、邮件地址或虚拟MFA设备。 • 绑定虚拟MFA前需要先在智能设备上安装一个MFA应用程序，才能绑定虚拟MFA设备。 • 登录保护仅影响使用管理控制台访问华为云的IAM用户，对编程访问用户无影响。 • 目前“华为云”手机应用程序暂不支持通过手机、邮件地址进行二次身份验证。如需登录“华为云”手机应用程序，建议选择MFA验证方式。 • 如果您的华为云账号已升级为华为账号，将不支持在“安全设置”页面开启登录保护，请在“**华为账号中心**>账号与安全>安全验证>双重验证”中开启。 • 开启操作保护后，默认在敏感操作验证成功后的15分钟之内，进行敏感操作无需再次验证。

操作场景	限制项	限制说明
	登录验证操作	● 账号锁定策略对华为云账号、账号下的IAM用户均生效。 ● 账号被锁定时，账号不能为自己或IAM用户解锁，锁定时间结束后，才能重新登录。 ● 账号停用策略仅对账号下的IAM用户生效，对账号本身不生效。 ● USB KEY证书策略对账号以及账号下的IAM用户生效。
	密码策略	● 如果您的华为云账号已升级为华为账号，密码策略将对账号不生效。 ● 只有管理员可以设置密码策略，普通IAM用户只有查看权限，不能对其进行设置，如需使用，请联系IAM管理员为您操作或添加权限。 ● 密码设置策略对华为云账号、账号下的IAM用户均生效。 ● 密码有效期策略默认关闭。 ● 密码过期后，重新设置的新密码不允许与旧密码相同。 ● 密码最短使用时间策略默认关闭，对账号以及账号下的IAM用户生效。

操作场景	限制项	限制说明
	访问控制	• 访问控制策略最多可设置200条。 • 如果IAM用户或联邦用户通过代理访问华为云，需按照代理IP设置允许访问的IP地址区间/IP地址或网段；如果IAM用户或联邦用户通过公网访问华为云，请按照公网IP进行设置。 • 支持IPv4和IPv6类型的地址。 • 控制台访问（推荐）：仅对账号下的所有IAM用户和联邦用户（SP方式）登录控制台生效，对账号本身不生效。 • API访问：仅对账号下的所有IAM用户和联邦用户通过API网关访问API接口生效，修改后15分钟生效。 • “允许访问的IP地址区间”、“允许访问的IP地址区间或网段”和“允许访问的VPC Endpoint”，如果同时设置，只要满足其中一种即可允许访问。
创建项目	/	• 如果您已开通企业项目，将不支持创建IAM项目。 • IAM项目中的资源不能转移。
删除项目	/	预置项目不支持删除。 删除项目前，请先**提交工单**进行技术咨询。
联邦用户通过身份提供商功能访问华为云	联邦用户登录形式	IAM支持两种形式的联邦身份认证： • 浏览器页面单点登录（Web SSO）：浏览器作为通讯媒介，适用于普通用户通过浏览器访问华为云。 • 调用API接口：开发工具/应用程序作为通讯媒介，例如OpenStack Client、ShibbolethECP Client，适用于企业或用户通过API调用方式访问华为云。

操作场景	限制项	限制说明
	敏感操作保护	如果账号开启了敏感操作保护（登录保护或操作保护），对联邦用户不生效，即联邦用户在执行敏感操作时，不需要二次验证。
	永久访问密钥（AK/SK）	不支持创建永久访问密钥（AK/SK），支持通过用户或委托token来获取临时访问凭证（临时AK/SK和securitytoken），具体方法请参见：**获取临时AK/SK和securitytoken**。