IAM 5.0 产品介绍

文档版本 01

发布日期 2025-11-06

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。

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 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。

说明

IAM新版控制台正在按照账号粒度逐步开放阶段，如果您还无法可见IAM新版控制台，您可以开通组织Organizations服务、资源访问管理RAM服务来提前使用IAM新版控制台进行身份策略的权限管理。本文档为与IAM新版控制台对应的新版资料，后续提到的IAM控制台如无特殊说明均指IAM新版控制台。要查看新旧控制台的差异详情，请参见**6 IAM新旧控制台功能差异说明**。

IAM 的优势

对华为云的资源进行精细访问控制

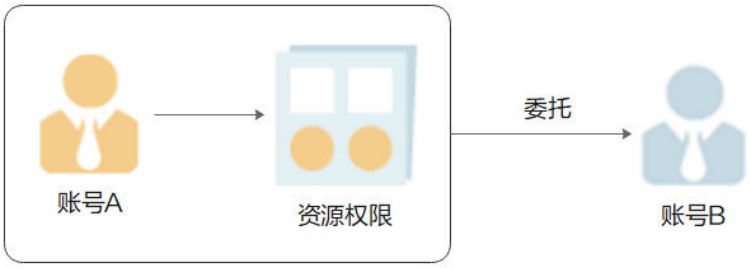
您注册华为云后，系统自动创建账号，账号是资源的归属以及使用计费的主体，账号根用户对账号所拥有的资源具有完全控制权限，可以访问华为云所有的云服务。

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，进行精细化的权限控制。

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提供的信任委托功能。

例如，您希望一家专业的代运维公司来帮您运维资源，您可以使用IAM的信任委托功能，将资源委托给代运维公司；当您不需要时，可以随时修改或者撤销对该运维公司的信任委托。下图中账号A即为委托方，账号B为被委托方。



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**。

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

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，账号根用户对账号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。

您不能在IAM中修改账号信息，而是需要到账号中心去修改账号信息，如果您需要删除账号，可以在账号中心进行注销。

说明

账号可以由账号名（Account Name）和账号ID（Account ID）标识，在IAM或其他云服务的资料中可能出现Domain Name和Domain ID，它们也标识账号名和账号ID。其中，Account Name和Domain Name是完全等价的，Account ID和Domain ID也是完全等价的。

IAM 用户

由账号管理员在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），根据账号管理员授予的权限使用资源。IAM用户使用云服务资源时不进行独立的计费，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：**忘记账号或IAM用户密码怎么办**。

图 2-1 IAM 用户登录

账号根用户

在创建账号的同时，系统会默认创建一个与账号同名的根用户。

从概念上来说，账号根用户也是一种IAM用户，它具备IAM用户概念模型下相同的能力。

从使用上来说，账号根用户会有一些额外的约束与限制。

约束1：账号根用户拥有默认的授权

账号根用户在被创建的同时会被授予默认的完全访问权限, 基于这些权限，根用户可以完全控制账号下的资源， 还可以分配其他IAM用户的使用权限。

约束2：账号根用户的权限不允许被修改

账号根用户不允许被绑定或者解绑权限，也不允许被加入或移除用户组，以保证账号根用户可以完全控制账号下的资源。

约束3：账号根用户不允许被删除

账号根用户不允许被删除， 以保证账号下至少有一个IAM用户可以完全控制账号下的资源。

说明

- 强烈建议您不要使用根用户来执行日常任务。
- 请您保护好根用户凭证，避免泄露。

账号与 IAM 用户的关系

从概念模型上来说

- 账号： 资源归属、资源使用计费的主体，账号不直接使用资源。
- IAM用户： 账号下资源的使用主体。

从使用习惯上来说

账号中的用户还分为账号根用户和IAM用户，它们都属于IAM用户的概念范畴。

- 账号根用户：创建账号时，默认创建的与账号同名的IAM用户， 有一些**额外的约束和限制**。
- IAM用户：创建账号后，手动创建的IAM用户，可以被修改权限和删除。

用户组

用户组是用户的集合，IAM可以通过用户组功能实现批量用户的授权。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，具有所有云服务和资源的操作权限。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 2-2 用户组与用户

信任委托

信任委托是您可以在账号中创建的一种具有特定权限的IAM身份。信任委托与IAM用户类似，均可以绑定身份策略，身份策略拥有决定该身份在华为云中能做什么和不能做什么的权限。但是，信任委托并非只与某个人唯一关联，而是旨在供任何需要它的人员进行切换代入。与IAM用户相比，信任委托没有与之关联的长期凭证（如密码或永久访问密钥），在您切换到一个信任委托时，它会为您的信任委托会话提供临时安全凭证。信任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：通过信任委托，您可以将自己账号中的资源操作权限委托给其他更专业的第三方账号，被委托的第三方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：基于云服务的业务需求，可能需要您创建云服务信任委托，将资源的操作权限委托给该服务，让该服务代替您进行一些资源运维工作。

其中，有一种特殊的云服务信任委托被称为服务关联委托，它由云服务代表您进行创建。普通的云服务信任委托由用户自己进行管理，而服务关联委托则由云服务进行管理，您可以查看但是不能编辑服务关联委托的权限。想要了解信任委托的更多情况，请参见**信任委托概述**。

此外，在IAM新版控制台的“委托”页签，同时展示了普通委托和信任委托两种类型的委托，它们之间的差异见信任委托概述中的**信任策略**。在IAM新版资料中，在广义上委托包含普通委托和信任委托，泛指把资源委托给其他人管理，而在狭义上委托即指普通委托，此时它有区别于信任委托。

IAM 身份

IAM身份是可以授予身份策略的IAM资源，包含IAM用户、用户组、委托和信任委托。

IAM 主体

主体（Principal），是可以对华为云资源发出操作请求的主体，包含IAM用户、委托和信任委托。主体访问API需要经过身份认证，主体也是一种资源，因此Principal URN遵从资源URN格式定义。

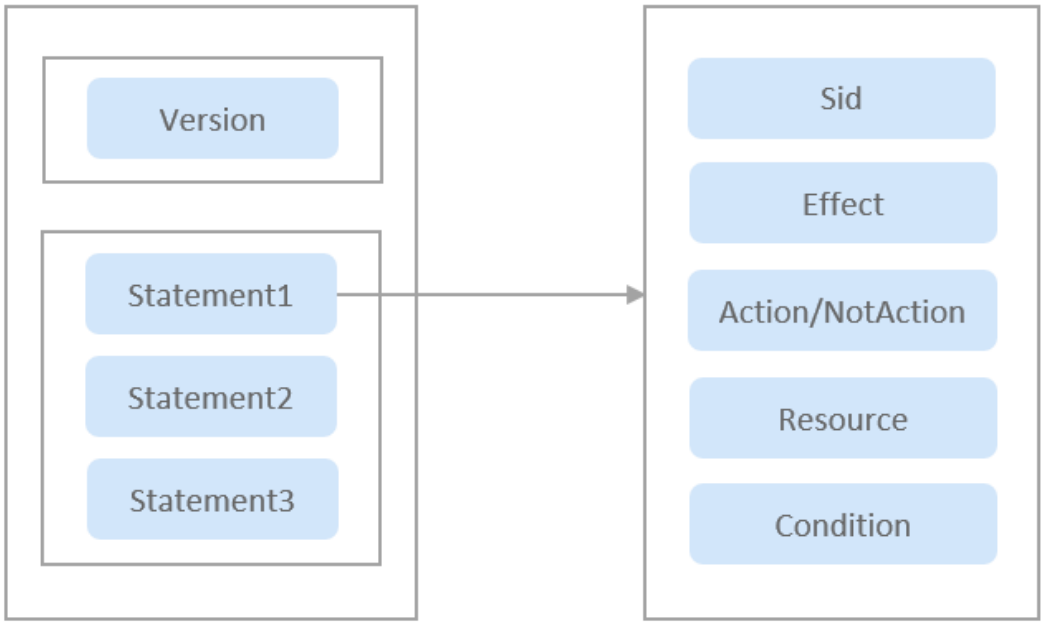
身份策略

身份策略包含多个元素定义的权限，可以精确到具体操作、资源、条件等。使用基于身份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。身份策略包含系统身份策略和自定义身份策略。

- 云服务在IAM预置了常用授权项集，称为**系统身份策略**。管理员给用户组授权时，可以直接使用这些系统身份策略，系统身份策略只能使用，不能修改。如果管理员在IAM控制台给用户、用户组或者信任委托授权时，无法找到特定服务的系统身份策略，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。
- 如果系统身份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**自定义身份策略**，并附加至用户、用户组、委托或信任委托，自定义身份策略是对系统身份策略的扩展和补充。目前支持可视化视图、JSON视图两种自定义身份策略配置方式。

身份策略结构**图2-3**所示，身份策略结构包含版本号Version和权限语句Statement两部分，其中Statement可以有多个，用于不同的权限控制。身份策略的Version为5.0，在Statement中，Sid表示Statement语句的标识，作用Effect包含Allow和Deny两种，分别表示允许执行和不允许执行。授权项Action/NotAction的格式为：{service name}:{resource type}:{action name}，资源Resource URN的格式为{service name}:{region id}:{account id}:{resource type}:{resource name}，条件Condition支持String、Number、Date、Bool、IP Address、Null六类条件运算符。同时身份策略支持40+的全局条件键，可以为用户访问华为云提供更加灵活与安全的控制方式。有关身份策略中各种元素的详情，请参见**JSON元素参考**。

图 2-3 身份策略模型结构



下面以一个具体的身份策略示例说明身份策略的模型结构：

```
{
    "Version": "5.0",
    "Statement": [{
        "Effect": "Deny",
        "Action": [
            "kms:cmk:decryptData"
        ],
        "Resource": [
            "*"
        ],
        "Condition": {
            "StringNotEquals": {
                "g:ResourceAccount": "xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx"
            }
        }
    }]
}
```

该身份策略表示拒绝用户使用指定用户以外的KMS密钥解密数据。身份策略详情请参见**身份策略语法**，更多示例请参见**自定义身份策略使用样例**。IAM的身份策略相对于策略，其授权项定义更加规范与细粒度，也支持更多的全局条件键，策略仅支持8个全局条件键，如果您仍需使用策略进行授权，请参见**权限管理**。

授权

授权指的是安全管理员将IAM权限附加到IAM身份（用户、用户组、信任委托、委托）上，使得主体（用户、委托、信任委托）被允许或者禁止访问华为云的资源。也就是说，授权描述的是IAM身份与权限之间的关系。在对IAM身份进行授权时，安全管理员可以直接给用户、用户组、信任委托和委托配置系统身份策略和自定义身份策略。身份策略授权与IAM旧版控制台中的角色和策略授权模型不同，不存在授权范围的概念，可以直接授予各种IAM身份。

```
{
    "Version": "5.0",
    "Statement": [{
        "Effect": "Allow",
        "Action": ["ecs:*:*"],
        "Resource": ["*"],
        "Condition": {
            "StringEquals": {
                "g:RequestedRegion": "cn-north-4"
            }
        }
    }]
}
```

如果想要在身份策略授权中达到类似控制授权范围的效果，则可以使用g:RequestedRegion条件键来实现。例如，将上述身份策略直接授予IAM用户上，表示仅允许IAM用户访问华北-北京四cn-north-4区域的ECS服务资源。如果您仍需使用角色与策略授权，授权方式和授权范围请参见**权限管理**。除此之外，由于系统兼容性原因，支持在IAM新版控制台中为委托授予系统身份策略和自定义身份策略，但是不支持在IAM旧版控制台中为信任委托授予系统角色、系统策略和自定义策略。IAM建议安全管理员在做权限管理时，尽量不要将委托和身份策略或者信任委托和角色与策略进行混用。

身份凭证

身份凭证是识别主体的依据，您通过控制台或者API访问华为云时，需要使用凭证来通过系统的鉴权认证。凭证包括密码、访问密钥、临时安全凭证，您可以在IAM中管理主体（IAM用户、委托和信任委托）的凭证。

身份凭证	对应的主体	安全性简要说明	详细介绍
用户名、密码	IAM用户	按需配置用户密码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	IAM用户	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
临时安全凭证	委托与信任委托	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。	临时安全凭证

MFA

Multi-Factor Authentication (MFA) 是一种非常简单的安全实践方法，它能够在用户名和密码之外再额外增加一层保护。启用MFA后，用户登录控制台时，系统将要求用户输入用户名和密码（第一安全要素），以及来自其MFA设备的验证码（第二安全要素）。这些多重要素结合起来将为您的账号和资源提供更高的安全保护。

URN

统一资源名称（Uniform Resource Name，URN），用于唯一标识云服务资源。

格式为：<service-name>:<region>:<account-id>:<type-name>:<resource-path>

- service-name：云服务简称，例如ecs。
- region：资源所在的区域，例如cn-north-1。如果是全局服务的资源，可以不填写或者用*填充。
- account-id：账号ID。“system”表示系统公共资源，例如系统身份策略。
- type-name：资源类型，需要填写目标云服务所支持的资源类型。可以参考**身份策略授权参考**中各服务的资源类型说明。
- resource-path：资源路径。可以参考**身份策略授权参考**中各服务的资源类型说明。

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、通过用户组批量管理用户权限、委托其他账号或者云服务管理资源、设置安全策略、访问分析。

须知

IAM为您提供的功能保证最终一致性，指您在IAM进行的操作，如创建用户和用户组、给用户和用户组授权等，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。建议您在进行其他操作前，确认已提交的策略修改已经生效。

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。

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身份信息来判断是否允许用户访问您账号中的资源。

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。

对用户直接进行权限管理

您也可以为每个用户进行单独的授权。可以直接将所需权限直接附加至用户，实现更灵活、更便捷的权限管理。

委托其他账号或者云服务管理资源

通过信任委托，您可以将自己的操作权限委托给其他更专业、高效的账号或者云服务，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和密码策略来提高用户信息和系统数据的安全性。

访问分析

IAM访问分析（IAM Access Analyzer）帮助您识别组织或账号中共享给外部主体的资源，未使用的密码和密钥，例如OBS桶策略、KMS密钥、IAM委托或信任委托，此类访问会带来安全风险。

IAM访问分析主要提供以下三个功能：

- 识别组织或账号中共享给外部主体的资源。

  通过访问分析功能，可以直观地了解组织或账号中共享给外部主体的资源，从而及时识别资源的访问风险。

- 识别组织或账号中未使用的访问。

  通过未使用的访问分析功能，可以了解组织或账号中IAM用户未使用的密码、访问密钥和权限，以及信任委托未使用的权限。

- 根据策略语法验证自定义策略。

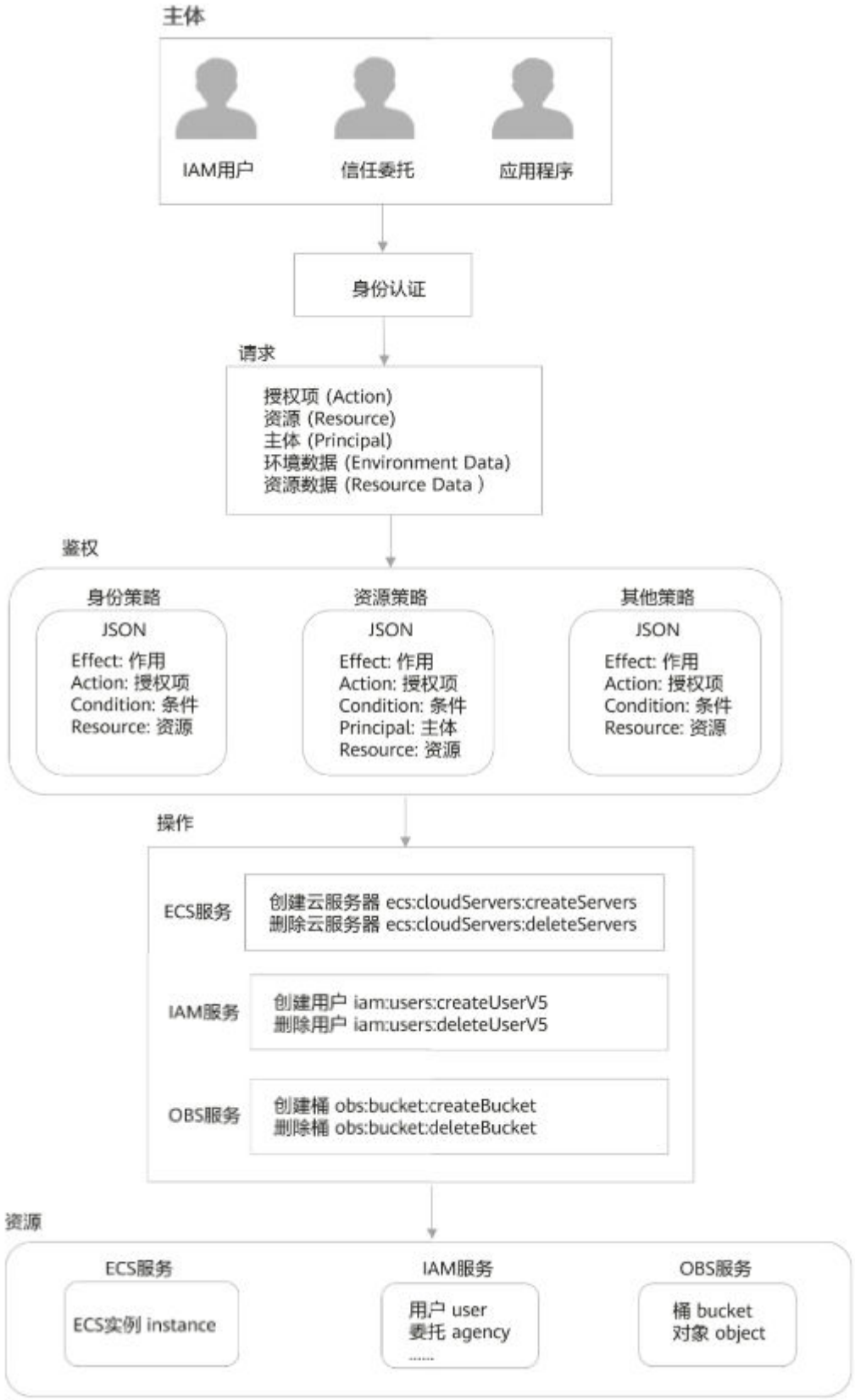
  通过策略检查功能来验证策略，并且提供检查结果。检查结果包括：安全、错误、建议、警告。

4 IAM 运行原理

IAM提供了为您账号进行身份认证和鉴权的基础设施。

用户登录控制台或者应用程序访问API时，IAM均会对其使用的凭证进行身份认证。IAM会将这些凭证与IAM主体进行匹配（例如，IAM用户、信任委托等），然后验证其是否有访问华为云的权限。对于一个鉴权请求，IAM会判断它是允许访问还是拒绝访问。例如，当您第一次登录华为云并进入控制台主页时，您还未访问任何云服务。当您选择进入某一个云服务时，该云服务将会为您发送一个鉴权请求到IAM。IAM将验证您的身份是否在授权的主体列表中，并评估任何可能生效的策略，然后给出最终的鉴权结果。一旦鉴权通过，您便能够在您的账号内执行这些操作，例如：创建新的ECS实例、创建新的IAM用户或者删除OBS桶等。下面的示例图描述了IAM认证和鉴权的流程：

图 4-1 IAM 认证和鉴权的流程



身份认证

主体使用凭证登录华为云时，IAM会对其进行身份认证，认证通过后才允许主体向华为云发送请求。每种类型的用户都要经过身份认证：

- IAM根用户：用于身份认证的凭证是您创建华为账号/华为云账号时的账号名与密码。
- IAM用户：用于身份认证的凭证是您的账号名、IAM用户名与密码。
- 联邦用户：您的身份提供商会对您进行身份验证并将您的凭证传递给华为云，您无需直接登录华为云。IAM Identity Center（外部身份源）和IAM旧版控制台都支持身份联邦身份认证。
- IAM Identity Center用户（本地身份源）： IAM Identity Center本地身份源中创建的用户使用华为云IAM Identity Center访问门户登录并认证您提供的用户名和密码。

建议您对所有用户均开启多因素认证（MFA）来提供您账号的安全性。要了解有关MFA的更多信息，请参考**什么是多因素认证**。

请求组成部分

当一个主体尝试访问华为云控制台、API或者CLI时，主体将会发送一个请求到华为云，这个请求会包含以下信息：

- 授权项（Action）：主体想要执行的操作对应的授权项。
- 资源（Resource）：主体想要执行的操作所关联的华为云资源。
- 主体（Principal）：发送请求的人员（IAM用户、信任委托或应用程序等）。
- 环境数据（Environment Data）：请求中有关IP、时间、用户代理等信息。
- 资源数据（Resource Data）：与华为云资源相关的数据，例如IAM用户和信任委托上的标签。

华为云将请求信息收集到**请求上下文**中，IAM会对其进行评估以便对该请求进行鉴权。

鉴权与策略基础知识

鉴权是指判断主体是否拥有完成其请求的权限。在鉴权期间，IAM使用请求上下文中的值来确定是允许还是拒绝请求。有多种策略可以影响请求的鉴权，使用IAM身份策略可以向您的IAM用户提供访问您账号内华为云资源的权限；而使用资源策略则可以进行跨账号授权，在进行跨账号访问时，其他账号中的资源策略必须允许您去访问这个资源，并且您发起访问的IAM主体必须被身份策略允许执行这个操作。

IAM检查应用于请求上下文的每个策略。IAM在策略评估逻辑中使用**显示拒绝**，这意味着如果一个策略中包含拒绝的授权项，那么IAM将拒绝整个请求并停止评估。由于在没有进行任何授权时，请求是默认被拒绝的，所以一个合适的策略需要允许请求中的每个部分，这样IAM才能最终允许您执行这个请求。单个账号内的鉴权遵循以下基本规则：

- 默认情况下，所有的请求都将被拒绝。（通常，始终允许账号根用户发起的访问该账号内资源的请求。）
- 任何策略（IAM身份策略或资源策略）中的显示允许都将覆盖该默认值。
- 如果存在服务控制策略（SCP）或者会话策略，它们会覆盖上一步中的显示允许，必须SCP策略或者会话策略也是允许，这个请求才能最终被允许，否则该请求将被

隐式拒绝。有关SCP策略的更多信息，请参考组织服务用户指南中的**服务控制策略概述**。

- 任何策略中的显示拒绝都将会覆盖所有策略中的允许。

想要了解更多信息，请参考**请求上下文**。

在进行身份认证之后，IAM通过附加在IAM身份上的各种策略来评估是否允许该请求。每个华为云服务都定义了它们支持的授权项，以及可以对资源进行的操作，例如创建、查看、编辑和删除该资源。例如IAM定义了几十种针对用户资源的授权项，一些基本授权项如下所示：

- 创建用户，其授权项为：iam:users:createUserV5
- 查看用户，其授权项为：iam:users:getUserV5
- 编辑用户，其授权项为：iam:users:updateUserV5
- 删除用户，其授权项为：iam:users:deleteUserV5

此外，您还可以在策略中指定条件，当请求满足指定条件时，才允许访问该资源。例如，您可能希望策略语句在特定日期之后生效、或者API请求中包含特定值时才允许访问。更多，请参考**全局条件键**。

在IAM允许请求后，该主体便可以使用您账号中的资源。资源是华为云服务中的对象，示例中包含：ECS实例、IAM用户和OBS存储桶等。如果主体触发的请求包含对未被允许的资源进行操作，则服务会拒绝该请求。例如，您有权限创建IAM用户，但是没有权限创建IAM用户组，那么您请求创建IAM用户组时，则会被拒绝。要了解哪些服务支持哪些授权项、资源和条件键，请参考请参见**身份策略授权参考**。

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）不被未经过认证、授权的主体或者个人获取，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5-1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	• 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	• 在创建用户、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
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、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。

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 IAM 新旧控制台功能差异说明

IAM新版控制台相比旧版控制台提供更精细化和更灵活的权限管控能力，同时删除部分功能，更聚焦于提升IAM访问控制的业务能力。以下按照IAM控制台功能模块划分，细化新旧版本控制台功能的区别。

用户

表 6-1 新旧版本控制台用户的区别

功能模块	对比项	旧版控制台	新版控制台
创建用户	批量创建	支持	不支持
	设置用户信息	用户名、描述、手机号、邮箱、外部身份源ID、设置访问方式、支持欢迎邮件设置密码、支持设置登录保护	仅用户名和描述即可
	创建方式	直接创建IAM用户	推荐创建IAM身份中心用户，也可以创建IAM用户
	授权方式	通过加入用户组授权	通过加入用户组授权或直接为用户附件身份策略授权
用户管理	批量删除	支持	支持
	批量编辑	支持（状态、访问方式、验证方式、登录密码、手机、邮箱）	支持（状态、登录密码）
	导出用户详细信息	支持（支持导出全部用户信息）	支持（支持导出全部或选中的部分用户信息）
	修改用户信息	仅用户状态和描述	支持修改用户名、状态和描述

功能模块	对比项	旧版控制台	新版控制台
	给用户添加标签	不支持	支持
	访问方式	支持修改“访问方式”为“编程访问或管理控制台访问”限制用户的访问方式	通过启用或关闭“管理控制台访问”限制能否访问控制台，通过是否为用户创建AKSK限制能否通过编程访问调用API
安全设置	登录凭证	重置登录密码、删除密码、最近一次修改密码时间	禁用控制台访问权限（删除密码）、重置密码、密码更新时间、密码过期时间、最近一次登录时间
	多因素认证设备	虚拟MFA、安全密钥	虚拟MFA、安全密钥
	登录保护	支持	不支持

用户组

新版控制台基本无变化，仅搜索能力变化和增强。在用户组列表页面支持根据用户组名称、描述和创建时间过滤用户组。

策略与授权

新版控制台支持更多的访问控制条件键、更加细粒度的权限管控能力。

表 6-2 新旧版本控制台策略的区别

对比项	旧版控制台	新版控制台
导航	权限管理包含授权管理和权限	仅身份策略
授权方式	支持IAM授权和企业项目授权	仅支持IAM授权，可以使用Condition条件键g:EnterpriseProjectId控制企业项目的授权范围。
能力	仅能在用户组和委托界面使用策略授权。开通企业项目后支持为用户直接进行策略授权，授权范围为指定企业项目	可以在策略界面直接将身份策略附加至IAM身份（用户、用户组、委托、信任委托）或从IAM身份分离

对比项	旧版控制台	新版控制台
授权对象	仅支持为用户组、委托绑定系统策略、系统角色和自定义策略进行授权。开通企业项目后支持为用户直接进行系统策略、自定义策略授权，授权范围为指定企业项目	支持为用户、用户组、委托、信任委托授予系统身份策略和自定义身份策略

如下策略基于源IP拒绝对华为云的访问。

```
{
   "Version": "5.0",
   "Statement": [{
      "Effect": "Deny",
      "Action": [
         "*:*:*"
      ],
      "Condition": {
         "NotIpAddress": {
            "g:SourceIp": [
               "192.0.2.0/24",
               "10.27.128.0/24"
            ]
         }
      }
   }]
}
```

如下策略仅允许用户名为TestUser开头的IAM用户查询企业路由实例详情。

```
{
   "Version": "5.0",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": ["er:instances:get"],
         "Resource": ["*"],
         "Condition": {
            "StringMatch": {
               "g:UserName": [
                  "TestUser*"
               ]
            }
         }
      }
   ]
}
```

项目

新版控制台不再支持“项目”功能，可以使用Condition条件键g:ProjectId控制项目的授权范围，配置示例如下所示。如果仍然希望在统一身份认证控制台中使用该功能，可以前往旧版控制台使用。

如下策略仅允许在 IAM 项目10a6c23c2a1044779794798beb067c94下创建虚拟私有云。

```
{
   "Version": "5.0",
   "Statement": [
      {
```



```
            "Effect": "Allow",
            "Action": ["vpc:vpcs:create"],
            "Resource": ["*"],
            "Condition": {
                "StringEquals": {
                    "g:ProjectId": "10a6c23c2a1044779794798beb067c94"
                }
            }
        }
    ]
}
```

如下策略仅允许查询IAM项目10a6c23c2a1044779794798beb067c94下的云服务器详情。

```
{
    "Version": "5.0",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": ["ecs:cloudServers:showServer"],
            "Resource": ["*"],
            "Condition": {
                "StringEquals": {
                    "g:ProjectId": "10a6c23c2a1044779794798beb067c94"
                }
            }
        }
    ]
}
```

委托

表 6-3 新旧版本控制台委托的区别

功能模块	对比项	旧版控制台	新版控制台
委托列表	查看委托列表	仅能查看老控制台创建的委托	可以查看老控制台创建的委托，及新控制台创建的信任委托
创建委托	创建委托	创建的委托不支持设置信任策略	创建的信任委托支持设置信任策略
	创建账号委托	输入账号名	输入账号ID
	委托时长表述	持续时间	最大会话持续时长
	更多选项	无	外部ID、启用MFA
	编辑方式	无	信任策略
	授权范围设置	配置策略并设置授权范围	无，创建完成后单独授权
委托详情	基本信息	显示委托类型和账号名	仅显示URN
	授权计数	有	无

身份提供商

新版控制台不再支持“身份提供商”功能，建议使用IAM身份中心的**外部身份源**功能。如果仍然希望在统一身份认证控制台中使用该功能，可以前往旧版控制台使用。

安全设置

新版控制台变化如下：

- 不再支持设置登录密码、手机号、邮箱。
- 不再支持敏感操作保护。
- 不再提供访问控制选项，合入登录验证策略页面，建议权限配置中condition条件键限制访问来源的IP。

我的凭证

新版控制台新增“登录凭证”和“多因素认证设备”功能。您可以使用“登录凭证”功能管理当前已登录控制台身份的密码，查看密码过期时间和上次修改密码时间。使用“多因素认证设备”功能，包括添加和解绑设备（包括虚拟MFA和安全密钥）。如果您是华为账号，请前往华为账号的账号与安全界面绑定华为账号的虚拟MFA，可以用于华为账号登录时的身份验证和华为账号的操作保护。

7 基于 IAM 进行权限管理

如果您需要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。IAM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，但是不允许在IAM中执行删除操作的权限。IAM服务支持的所有服务系统权限请参见：**系统身份策略**。

IAM 权限

如**表1**所示，包括了IAM的所有系统身份策略。

表 7-1 IAM 系统身份策略

系统身份策略名称	描述	策略类别
IAMFullAccessPolicy	统一身份认证服务的所有权限。	系统身份策略
IAMReadOnlyPolicy	统一身份认证服务的只读访问权限。	系统身份策略

表2列出了IAM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。

表 7-2 常用操作与系统权限的关系

操作	IAMFullAccessPolicy	IAMReadOnlyPolicy
创建IAM用户	√	×
查询IAM用户详情	√	√
修改IAM用户信息	√	×

操作	IAMFullAccessPolicy	IAMReadOnlyPolicy
查询IAM用户安全设置	√	√
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	√	×
创建自定义身份策略	√	×
修改自定义身份策略	√	×
删除自定义身份策略	√	×
查询权限详情	√	√
创建信任委托	√	×
查询信任委托	√	√
修改信任委托	√	×
切换角色	√	×
删除信任委托	√	×
为信任委托授权	√	×
移除信任委托权限	√	×
查询配额	√	√

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FullAccess权限。

表 7-3 访问密钥操作与系统权限的关系

操作	IAMFullAccessPolicy	IAMReadOnlyPolicy
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）	√	×

IAMFullAccessPolicy 策略内容

```
{
  "Version": "5.0",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "iam:*:*"
      ]
    }
  ]
}
```

IAMReadOnlyPolicy 策略内容

```
{
  "Version": "5.0",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "iam:*:get*",
        "iam:*:list*",
        "iam:*:check*",
        "iam:*:show*"
      ]
    }
  ]
}
```


8 基于属性的 ABAC 权限管理

在华为云统一身份认证服务（IAM）中，授权是确保正确主体拥有正确访问权限的关键。两种主要的授权策略是基于属性的访问控制（ABAC）和基于角色的访问控制（RBAC）。了解这两种模型的区别可以帮助您设计更安全、更高效的访问控制方案。

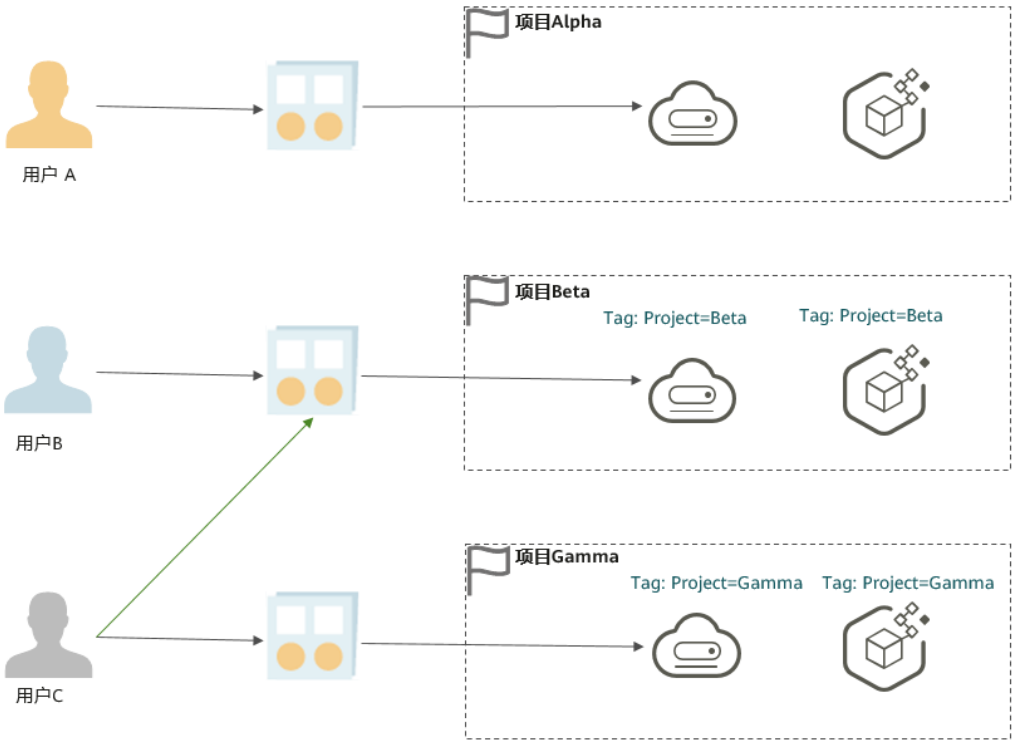
概念定义

- **基于属性的访问控制（ABAC）**：ABAC是一种附加到IAM身份（如IAM用户）和基于属性（Attributes）来定义权限的授权策略。ABAC 基于主体、资源、操作、环境等属性，通过策略实时评估多个属性组合来决策是否授权。例如，您可以规定只有当用户拥有“Project=Alpha”标签时，才能访问同样拥有标签为“Project=Alpha”的资源。
- **基于角色的访问控制（RBAC）**：RBAC是一种基于用户在组织中担任的职能或角色来定义权限的策略。在IAM中，这意味着为不同的工作职能创建不同的策略或利用华为云预制角色，并将这些策略附加到IAM身份（如IAM用户）并约束其授权范围(如某个项目)。例如，你可以为某容器管理员用户授予华为云预制的CCE Administrator角色, 并约束其授权仅在项目Alpha下生效。

例如, 您的员工分别需要在三个项目Alpha、Beta、Gamma上工作，且需要访问ECS资源，您可以选择ECS Administrator角色进行授权，并限制授权范围分别为项目Alpha，项目Beta及项目Gamma。这样您的员工将只能在授权范围内的项目中，根据您授权的角色权限来访问云服务资源。如果员工的工作发生变化，需要额外访问CCI提供的容器能力，或用户C需要访问归属于项目Beta的资源时，您必须创建新的角色授权关系，并更新授权范围，否则将无法满足调整后的资源访问诉求。

而基于ABAC授权时，您可以编写身份策略，允许特定身份访问带有特定标签的云服务资源(如标签Project=Beta或Gamma)，可以通过对身份或者资源的标签进行灵活的访问控制管理，而不需要反复的调整策略或授权关系。

图 8-1 示例



核心差异

表 8-1 核心差异

特性	基于角色的访问控制（RBAC）	基于属性的访问控制（ABAC）
授权关系	身份-角色-授权范围	身份-策略
授权基础	基于预定义的角色和职能	基于身份、资源、环境等的动态属性
策略数量	随着职能和资源增加，通常需要更多的策略	通常需要更少的策略，因为策略是基于属性而非具体主体
扩展性	新增资源或职能时，可能需要手动更新现有策略	权限可随新资源自动扩展，无需修改现有策略
权限粒度	通常授予对特定资源的访问权限	允许基于属性授权，支持更为丰富的条件控制属性
管理复杂度	在大型或快速变化的环境可能变得复杂	简化了新项目或人员变动时的权限管理

说明

1. IAM的策略是一种基于策略的角色(Policy-based role)，其授权也遵循身份-角色-授权范围的授权关系，而身份策略遵循身份-策略的授权关系。
2. IAM的身份策略支持完整的ABAC访问控制条件，包括基于身份，资源，环境等动态属性。相比策略而言，身份策略支持的访问控制条件键更多，详情请参见**全局条件键**，同时也支持更丰富的策略语法，详情请参见**JSON元素参考**。

ABAC 相对于 RBAC 的优势

- **动态响应变化与增长**：对于新资源的权限，只要属性匹配，便会自动授予，无需手动将策略分配给身份。这极大地简化了新项目启动或团队成员调动时的权限管理。
- **更细粒度的权限控制**：ABAC允许使用基于主体、资源、操作、环境上下文的属性，从而实现更细粒度的控制。
- **策略数量更少，管理更简单**：ABAC通常需要更少的策略。您无需为每个工作职能创建单独的策略，从而使策略更容易管理和维护。
- **与企业身份供应商集成**：ABAC允许您在使用外部身份供应商(IdP)时, 将员工在IdP上的属性映射至IAM的身份标签(通过IAM身份中心), 并在策略中基于这些标签进行访问控制。详情参考IAM身份中心的**ABAC概述和配置流程**。

9 安全

9.1 责任共担

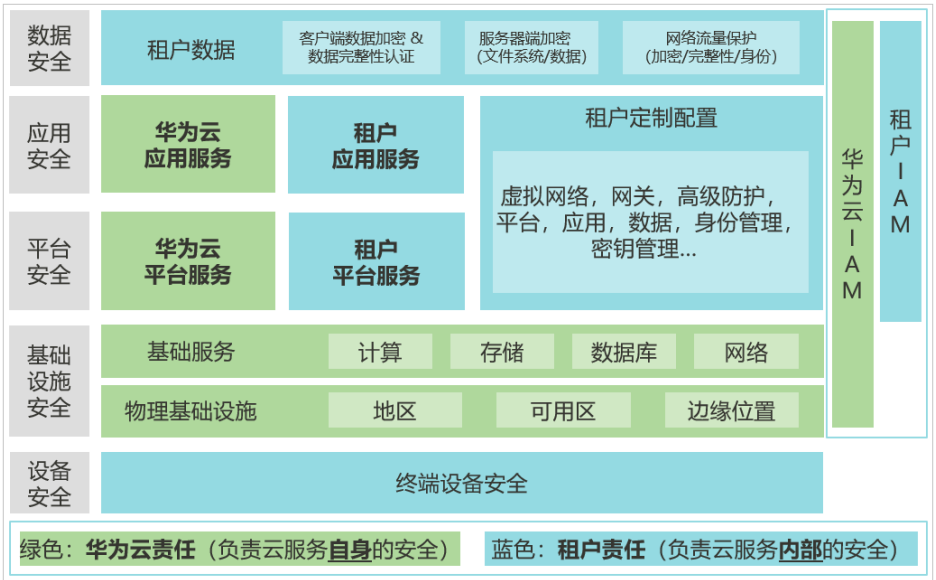
华为云秉承“将公司对网络和业务安全性保障的责任置于公司的商业利益之上”。针对层出不穷的云安全挑战和无孔不入的云安全威胁与攻击，华为云在遵从法律法规业界标准的基础上，以安全生态圈为护城河，依托华为独有的软硬件优势，构建面向不同区域和行业的完善云服务安全保障体系。

安全性是华为云与您的共同责任，如图9-1所示。

- **华为云**：负责云服务**自身**的安全，提供安全的云。华为云的安全责任在于保障其所提供的 IaaS、PaaS 和 SaaS 类云服务自身的安全，涵盖华为云数据中心的物理环境设施和运行其上的基础服务、平台服务、应用服务等。这不仅包括华为云基础设施和各项云服务技术的安全功能和性能本身，也包括运维运营安全，以及更广义的安全合规遵从。
- **租户**：负责云服务**内部**的安全，安全地使用云。 华为云租户的安全责任在于对使用的 IaaS、PaaS 和 SaaS 类云服务内部的安全以及对租户定制配置进行安全有效的管理，包括但不限于虚拟网络、虚拟主机和访客虚拟机的操作系统，虚拟防火墙、API 网关和高级安全服务，各项云服务，租户数据，以及身份账号和密钥管理等方面的安全配置。

《华为云安全白皮书》详细介绍华为云安全性的构建思路与措施，包括云安全战略、责任共担模型、合规与隐私、安全组织与人员、基础设施安全、租户服务与租户安全、工程安全、运维运营安全、生态安全。

图 9-1 华为云安全责任共担模型



9.2 身份认证与访问控制

9.2.1 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、访问密钥和临时安全凭证进行身份认证。详见**表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 9-1 IAM 身份凭证和安全性设计

访问凭证	对应的主体	安全性简要说明	详细介绍
用户名、密码	账号根用户与IAM用户	按需配置用户密码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	账号根用户与IAM用户	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

访问凭证	对应的主体	安全性简要说明	详细介绍
临时安全凭证	委托与信任委托	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。	临时安全凭证

登录保护与验证策略

如表2所示，除了要求用户登录出示凭证并验证合法性，IAM还支持登录保护和登录验证策略，防止用户信息被非法盗用。

表 9-2 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）。 验证设备支持虚拟MFA设备，详见多因素认证。	登录保护
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

9.2.2 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 9-3 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细粒度划分，身份策略明确定义了IAM服务允许或者拒绝的用户操作。例如拥有IAM ReadOnlyAccessPolicy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、网段登录IAM控制台。	登录验证策略

9.3 数据保护技术

9.3.1 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、授权的主体或者个人获取，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1**所示：

表 9-4 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	• 在创建用户或修改用户名称时，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	管理员权限可通过控制台或API修改	是 用户名是用户的身份标识信息
密码	在创建用户、重置密码时由用户在界面输入密码	控制台界面进行身份认证	是	否 用户可以选择使用AK/SK方式

类型	收集方式	用途	是否可以修改	是否必须
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或加盐SM3算法加密存储。
- SK：使用安全AES或SM4算法加密存储。

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。

9.3.2 用户侧

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。用户负责安全使用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。

9.4 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。为了减小由硬件故障、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。。

9.5 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支持云审计的关键操作**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**开通云审计服务**。开通云审计服务后，可**查看IAM的云审计日志**，云审计服务保存最近7天的操作日志。

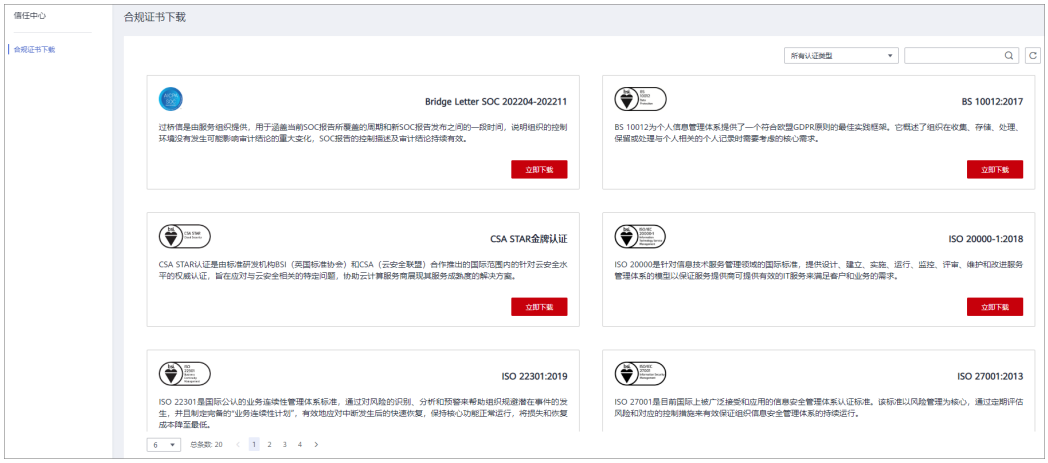
CTS支持**配置关键操作通知**。用户可将与IAM相关的高危敏感操作，作为关键操作加入到CTS的实时监控列表中进行监控跟踪。当用户使用IAM服务时，如果触发了监控列表中的关键操作，那么CTS会在记录操作日志的同时，向相关订阅者实时发送通知。

9.6 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 9-2 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 9-3 资源中心

10 约束与限制

IAM中的用户数、用户组数等有默认的配额， 其中“是否支持修改”列标示“√”的，表示该项资源的配额可以修改。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**。

资源分类	限制项	默认值	最大值	是否支持修改
用户	IAM用户数量	50	2000	√
	用户名的字符数量	64	-	x
	一个用户可绑定的身份策略数量	10	20	√
	用户可加入的用户组数量	10	-	x
	用户可创建的访问密钥（AK/SK）数量	2	-	x
	用户可绑定的虚拟MFA设备数量	1	-	x
用户组	用户组数量	20	2000	√
	用户组名的字符数量	128	-	x
	一个用户组中可添加的用户数量	账号下的IAM用户数	-	x
	一个用户组可绑定的身份策略数量	10	-	x
委托和信任委托	信任委托名称的字符数量	64	-	x
	委托和信任委托总和	50	5000	√
	一个委托或信任委托可绑定的权限数（包括系统身份策略和自定义身份策略）	10	20	√
身份策略	自定义身份策略数量	1500	5000	√
	自定义身份策略版本数量	5	-	x
	身份策略名称的字符数量	128	-	x

资源分类	限制项		默认值	最大值	是否支持修改
	自定义身份策略	字节数量	6144	-	x
		Statement	不限制，身份策略总字节数量不超过6144	-	x
		Action	不限制，身份策略总字节数量不超过6144	-	x
		Resource	不限制，身份策略总字节数量不超过6144	-	x
		Condition	不限制，身份策略总字节数量不超过6144	-	x

