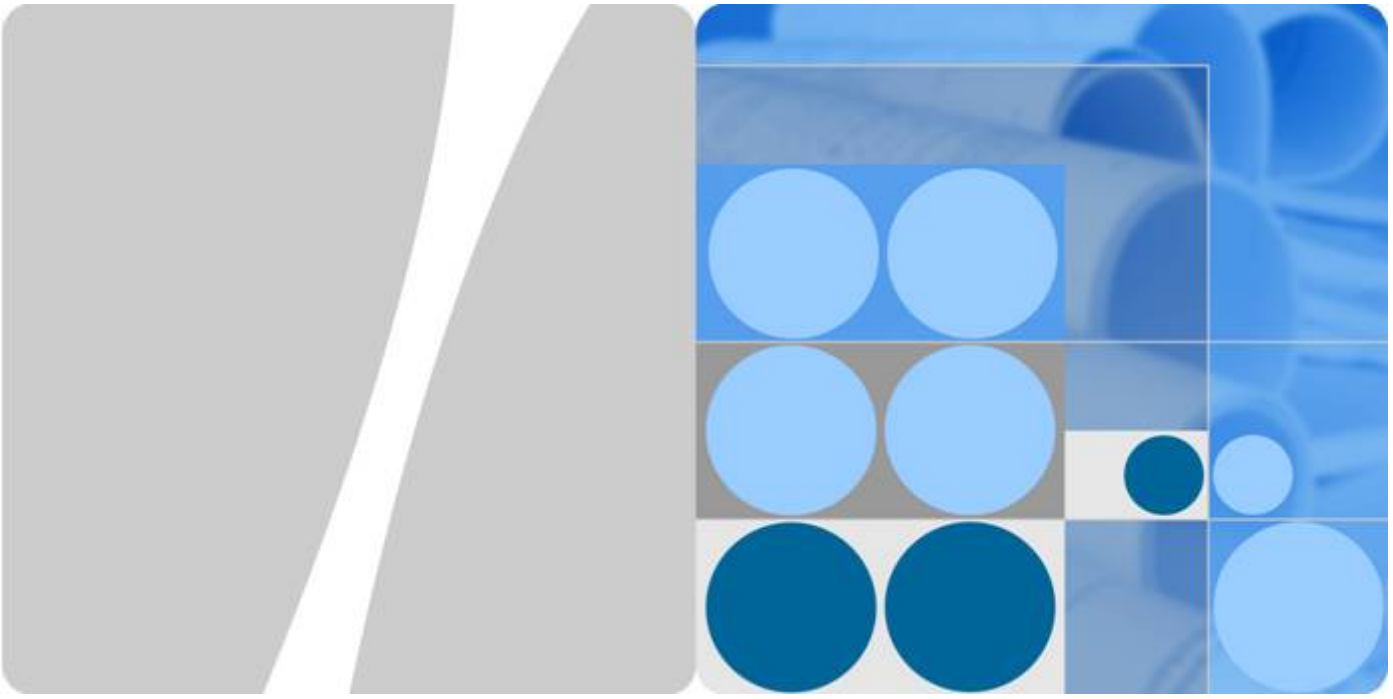


统一身份认证

用户指南

发布日期　2021-11-30

目 录

1 产品简介

1.1 什么是 IAM

统一身份认证（Identity and Access Management，简称IAM）是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。

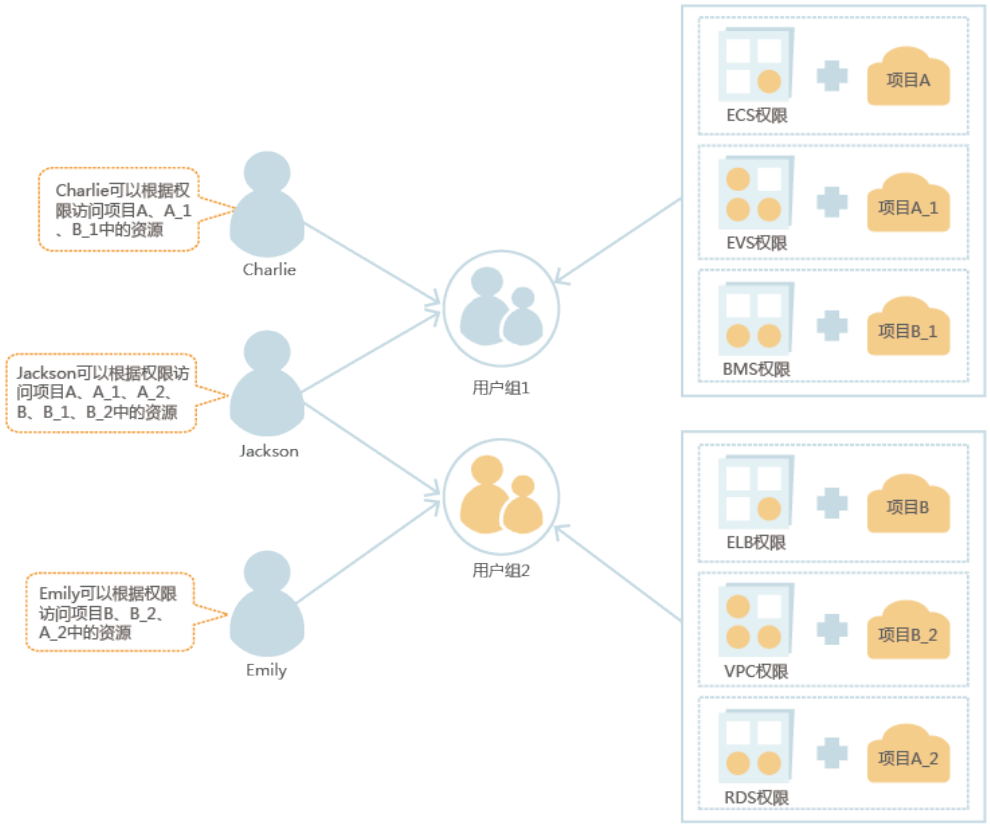
IAM 的优势

对资源进行精细访问控制

您注册后，系统自动创建账号，账号是对其所拥有的资源具有完全控制权限，可以访问系统中所有的云服务。

如果您创建了多种资源，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云服务平台。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。

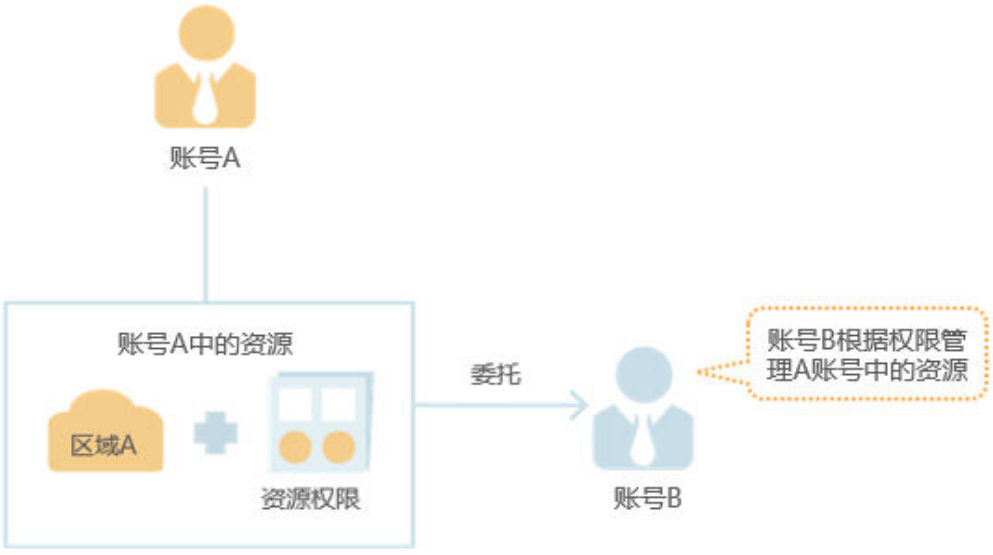
除了IAM外，还有企业管理服务同样可以进行资源权限管理，相对于IAM，企业管理对资源的控制粒度更为精细，同时还支持企业项目费用的管理，建议结合企业需求选择IAM或是企业管理进行资源权限管理。



跨账号的资源操作与授权

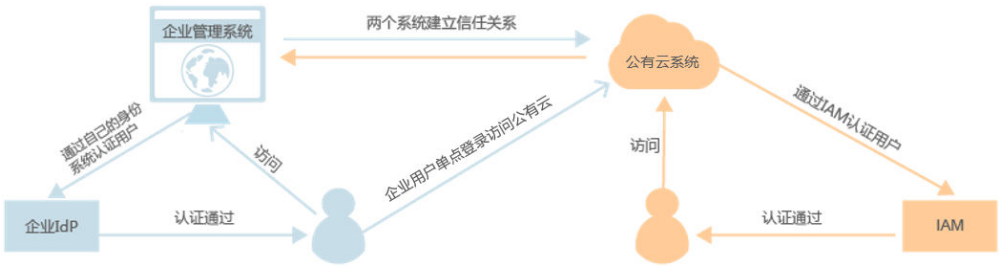
如果您创建了多种资源，其中一种资源希望由其它账号管理，您可以使用IAM提供的委托功能。

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消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云服务平台

当您希望本企业员工可以使用企业内部的认证系统登录云服务平台，而不需要在云服务平台上重新创建对应的IAM用户，您可以使用IAM的身份提供商功能，建立您所在企业与云服务平台的信任关系，通过联合认证使员工使用企业已有账号直接登录云服务平台，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。

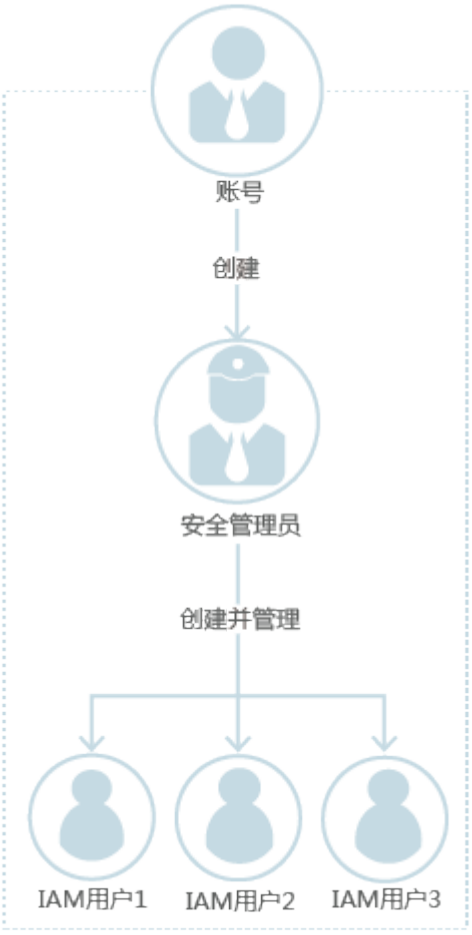
1.2 基本概念

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

当您首次使用云服务平台时注册的账号，该账号是您的资源归属，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。

图 1-1 账号管理模型



IAM 用户

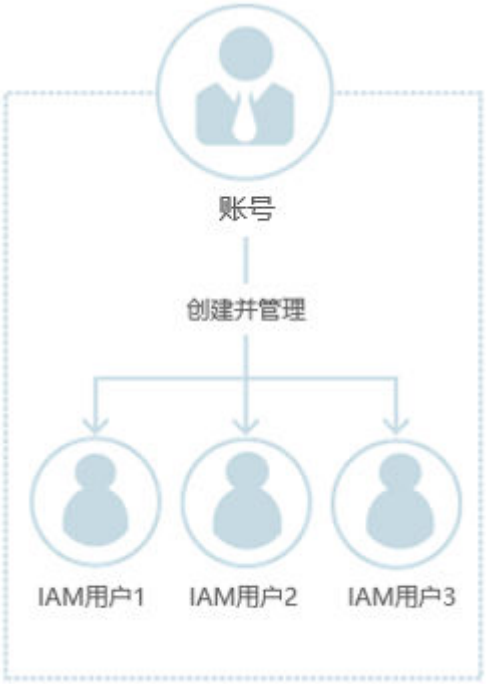
由账号在IAM中创建的用户，是云服务的使用人员，具有独立的身份凭证（密码和访问密钥），根据账号授予的权限使用资源。

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：常见问题>密码凭证类>忘记密码怎么办。

账号与 IAM 用户的关系

账号与IAM用户可以类比为父子关系。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。

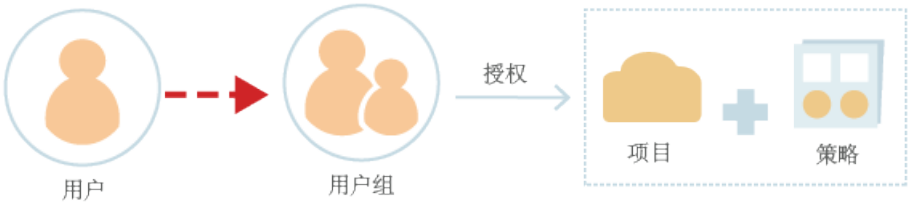
图 1-2 账号与 IAM 用户



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，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IAM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，管理您账号中的ECS资源。

图 1-3 授权



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 1-4 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。
  - 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 1-5 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访问云服务平台时，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。

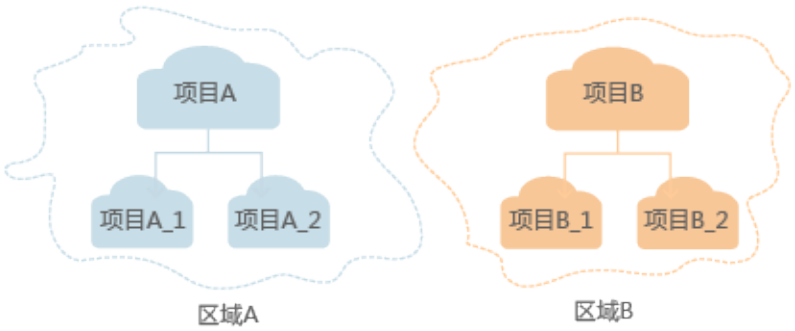
虚拟 MFA

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，云服务平台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。

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，并在子项目中创建资源，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 1-6 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。

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：由于云服务平台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。

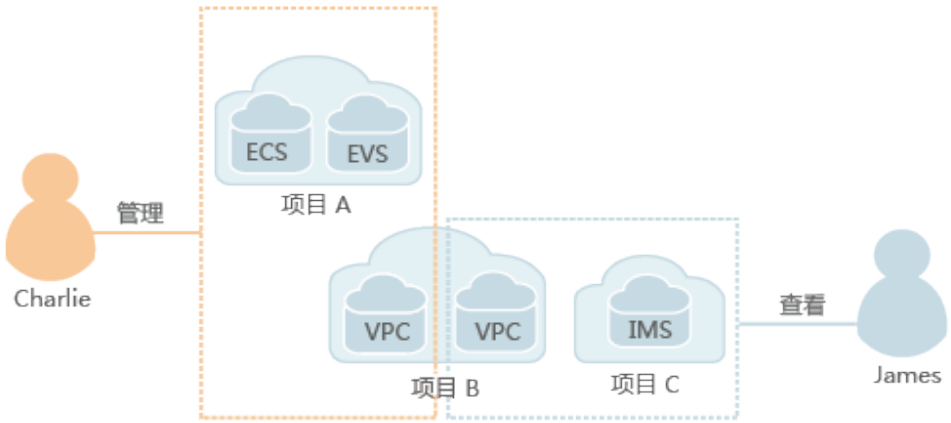
1.3 IAM 功能

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 1-7 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，您不需要在云服务平台上重新创建用户，可以通过身份提供商功能直接访问本系云服务平台，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通过在云服务平台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。

1.4 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1-1**所示：

表 1-1 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、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。

1.5 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：权限集。

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“IAM API参考>权限和授权项”。

如表1所示，包括了IAM的所有系统权限。

表 1-2 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

系统角色/策略名称	描述	类别	角色/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基础权限，不包含IAM的任何权限，因此下表中不进行解析。

表 1-3 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	√	×	√	√
修改IAM用户安全设置	√	×	√	×
删除IAM用户	√	×	√	×
创建用户组	√	×	√	×

操作	Security Administrator	Agent Operator	FullAccess	IAM ReadOnlyAccess
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	√	×	√	√
修改项目	√	×	√	×
删除项目	√	×	√	×
创建身份提供商	√	×	√	×

操作	Security Administrator	Agent Operator	FullAccess	IAM ReadOnlyAccess
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 1-4 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）	√	×	√	×

操作	Security Administrator	Agent Operator	FullAccess	IAM ReadOnlyAccess
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"
    }
  ]
}
```

2 快速入门

2.1 入门前必读

您可以通过本手册了解：

- 为什么要创建IAM用户
- 如何基于企业项目职能创建用户组
- 如何为用户组授权
- 如何为企业员工创建IAM用户
- 新创建的IAM用户如何登录云服务平台

前提条件

请确保您已拥有账号，若您还没有账号，请先进行注册。

示例场景

A公司是一家负责网站开发的公司，公司中有三个职能团队。为了方便A公司统一创建、分配资源并管理用户，A公司的人员不需要每人都注册账号，而是由公司的管理员注册一个账号，在这个账号下创建IAM用户并分配权限，然后将创建的IAM用户分发给公司的人员使用。

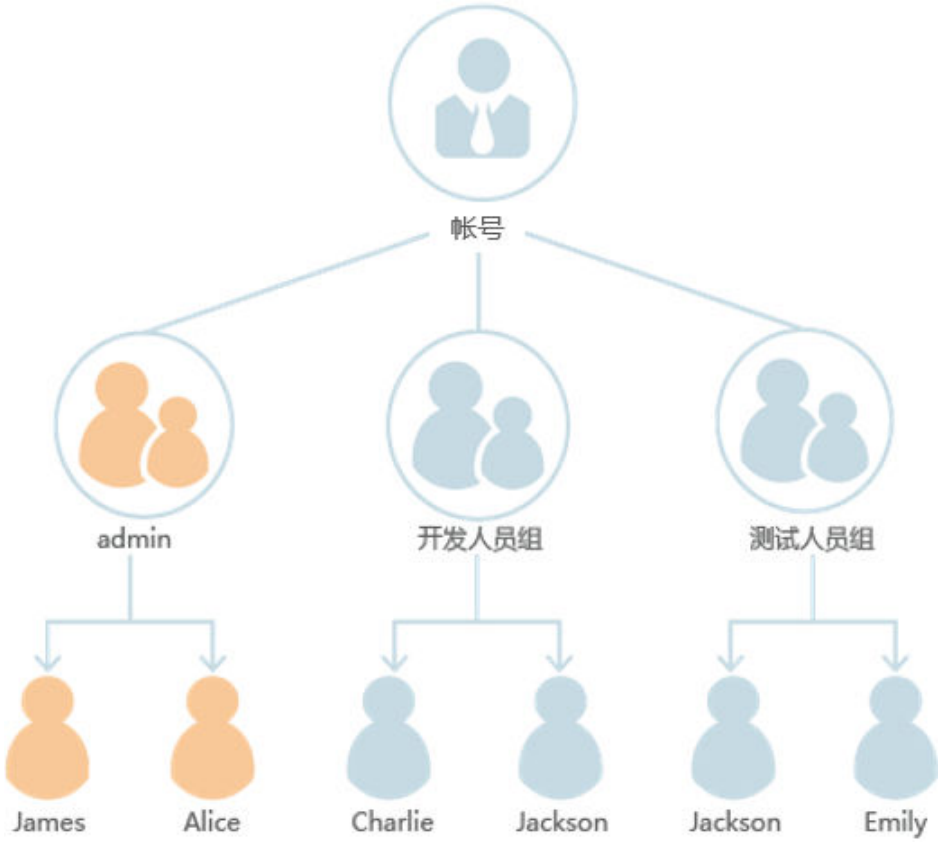
本文以A公司使用IAM创建用户及用户组为例，帮助您快速了解，企业如何使用IAM完成服务权限的配置。

A公司人员组成

- 负责管理公司的人员以及资源的管理团队（对应**图2-1**中的“admin”），进行权限分配，资源调配等。团队成员包括James和Alice。
- 负责开发公司网站的开发团队（对应**图2-1**中的“开发人员组”）。团队成员包括Charlie和Jackson。

- 对开发团队开发出的网站进行测试的测试团队（对应图2-1中的“测试人员组”）。团队成员包括Jackson和Emily。其中Jackson同时负责开发及测试，因此他需要同时加入“开发人员组”及“测试人员组”，以分别获得两个用户组的权限。

图 2-1 用户管理模型



A公司业务组成

- admin组主要负责公司人员权限分配，需要使用IAM服务。
- 开发人员组在网站开发过程中，需要使用弹性云服务器（ECS）、弹性负载均衡（ELB）、虚拟私有云（VPC）、关系型数据库（RDS）、云硬盘（EVS）以及对象存储服务（OBS）。
- 测试人员主要负责网站的功能及性能测试，需要使用应用性能管理（APM）。

用户管理流程

1. A公司的管理员使用注册的账号登录云服务平台，创建“开发人员组”及“测试人员组”，并给用户组授权。操作步骤请参见：**步骤1：创建用户组并授权**。
2. A公司的管理员给三个职能团队中的成员创建IAM用户，并让他们使用新创建的用户登录云服务平台。操作步骤请参见：**步骤2：创建IAM用户并登录**。

2.2 步骤 1：创建用户组并授权

A公司的团队分为管理组（admin）、开发人员组和测试人员组。由于系统默认内置了admin组，用于拥有账号所有资源的使用及管理权限，因此A公司的团队只需要在IAM中再创建开发人员组及测试人员组即可。

创建用户组

步骤1 A公司管理员登录控制台，并选择“统一身份认证服务”。

步骤2 在统一身份认证服务，左侧导航窗格中，单击“用户组”>“创建用户组”。

步骤3 在“创建用户组”界面，输入“用户组名称”，单击“确定”，完成用户组创建。

步骤4 按照**步骤2**和**步骤3**的方法，创建“测试人员组”。

----结束

给用户组授权

A公司的开发人员需要使用的云服务为ECS、RDS、ELB、VPC、EVS和OBS，需要为“开发人员组”授予这六个服务的管理员权限。测试人员需要使用云服务APM，需要为“测试人员组”授予此服务的权限。完成用户组的授权后，用户组中的用户才可以使用这些云服务。**如需查看所有云服务的系统权限，请参见：权限集**。

步骤1 确定所需权限。

需要设置的权限如**表1**所示。其中“作用范围”由该服务的物理部署位置决定。对于项目级服务，如果在某个区域的项目中设置策略，则策略只在该项目中生效。

表 2-1 所需权限

用户组	使用的服务	所属区域	设置策略或角色
开发人员组	ECS	除全局区域外的其他区域	ECS Admin
	RDS	除全局区域外的其他区域	RDS Admin
	ELB	除全局区域外的其他区域	ELB FullAccessELB Admin
	VPC	除全局区域外的其他区域	VPC Administrator
	EVS	除全局区域外的其他区域	EVS Admin
	OBS	全局区域	OBS Buckets Viewer
测试人员组	APM	除全局区域外的其他区域	APM Admin

步骤2 在用户组列表中，单击新建用户组“开发人员组”，右侧的“权限配置”。

图 2-2 权限配置

步骤3 设置区域级项目的权限。

1. 由表1可知，除OBS外，其它服务都是项目级服务。在作用范围中选择“区域级项目”，并在下拉框中选择项目。
2. 勾选需要授予用户组的权限，单击“确定”。

步骤4 设置全局服务的权限。

1. 在作用范围中选择“全局服务”。
2. 在全局服务中搜索并选择“OBS Buckets Viewer”，单击“确定”，完成全局服务的授权。

步骤5 参考2-5的方法，给“测试人员组”授予“APM Admin”的权限。

----结束

2.3 步骤 2：创建 IAM 用户并登录

上一个章节已完成用户组的创建，本节将描述A公司使用已注册的账号，给公司成员创建IAM用户并加入用户组的操作，使得他们拥有独立的用户和密码，可以独立登录云服务平台并使用权限范围内的资源。

创建 IAM 用户

步骤1 在统一身份认证服务，左侧导航窗格中，单击“用户”>“创建用户”。

步骤2 配置基本信息。在“创建用户”界面填写“用户信息”和“访问方式”。如需一次创建多个用户，可以单击“添加用户”进行批量创建，每次最多可创建10个用户。

图 2-3 配置用户信息

说明

- 用户可以使用此处设置的用户名、邮件地址或手机号任意一种方式登录云服务平台。
- 当用户忘记密码时，可以通过此处绑定的邮箱或手机自行重置密码，如果用户没有绑定邮箱或手机号码，只能由管理员重置密码。

表 2-2 用户信息

用户信息	说明
用户名	必填。IAM用户登录云服务平台的用户名，此处以“James”和“Alice”为例。
邮件地址	“凭证类型”选择“首次登录时设置”时必填，选择其他时选填。IAM用户绑定的邮件地址，可作为登录凭证，也可由IAM用户自己绑定。
手机号	选填。IAM用户绑定的手机号，可作为IAM用户的登录凭证，也可由IAM用户自己绑定。
描述	选填。记录IAM用户相关信息。
外部身份ID	选填。IAM SSO类型的联邦用户单点登录中，与当前实体IAM用户对接的，企业自身用户的身份ID值。 为IAM用户配置IAM SSO类型的联邦用户单点登录时，“外部身份ID”为必填参数（不超过128个字符）。

- 编程访问：为IAM用户启用**访问密钥或密码**，支持用户通过API、CLI、SDK等开发工具访问云服务。
- 管理控制台访问：为IAM用户启用**密码**，支持用户登录管理控制台访问云服务。

  说明

  - 如果IAM用户**仅需登录管理控制台访问云服务**，建议访问方式选择**管理控制台访问**，凭证类型为**密码**。
  - 如果IAM用户**仅需编程访问云服务**，建议访问方式选择**编程访问**，凭证类型为**访问密钥**。
  - 如果IAM用户**需要使用密码作为编程访问的凭证**（部分API要求），建议访问方式选择**编程访问**，凭证类型为**密码**。
  - 如果IAM用户使用部分云服务时，需要在其**控制台验证访问密钥**（由IAM用户输入），建议访问方式选择**编程访问和管理控制台访问**，凭证类型为**密码和访问密钥**。例如IAM用户在控制台使用云数据迁移CDM服务创建数据迁移，需要通过访问密钥进行身份验证。

表 2-3 配置凭证类型和登录保护

凭证类型与登录保护		说明
访问密钥		创建用户完成后即可下载本次创建的所有用户的访问密钥（AK/SK）。 **一个用户最多拥有两个访问密钥。**
密码	自定义	自定义用户密码，并选择用户首次登录时是否需要重置密码。 如果您是用户的使用主体，建议您选择该方式，设置自己的登录密码，且无需勾选首次登录时重置密码。

凭证类型与登录保护		说明
	自动生成	系统自动生成IAM用户的登录密码，创建完用户即可下载excel形式的密码文件。将密码文件提供给用户，用户使用该密码登录。 **仅在创建单个用户时适用。**
	首次登录时设置	系统通过邮件发一次性登录链接给用户，用户登录控制台并设置密码。 如果您不是用户的使用主体，建议选择该方式，同时输入用户的邮件地址和手机，用户通过邮件中的一次性链接登录云服务平台，自行设置密码。该链接**7天**内有效。
登录保护	开启登录保护（推荐）	开启登录保护后，IAM用户登录时，除了在登录页面输入用户名和密码外（第一次身份验证），还需要在登录验证页面输入验证码（第二次身份验证），该功能是一种安全实践，建议开启登录保护，多次身份认证可以提高账号安全性。 您可以选择通过手机、邮箱、虚拟MFA进行登录验证。
	不开启	创建完成后，如需开启登录保护，请参见：用户指南>IAM用户>查看或修改IAM用户信息。

步骤3 单击“下一步”，将用户加入到用户组（可选）。

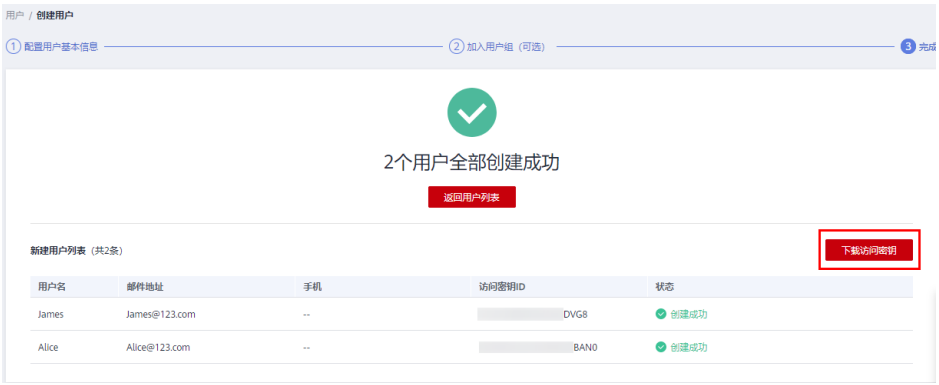
- 将用户加入用户组，用户将具备用户组的权限，这一过程即给用户授权。
- 如需创建新的用户组，可单击“创建用户组”，填写用户组名称和描述（可选），创建成功后即可将用户加入到新创建的用户组中。

说明

“admin”为系统缺省提供的用户组，具有管理人员以及所有云服务资源的操作权限。A公司人员与用户组对应关系请参见：**图2-1**。

步骤4 单击“创建用户”，IAM用户创建完成，用户列表中显示新创建的IAM用户。如果“访问方式”选择了“编程访问”且**表2 配置凭证类型**凭证类型勾选了“访问密钥”，可在此页面下载访问密钥。

图 2-4 用户创建成功



步骤5 参考**步骤1**-**步骤4**的方法，创建用户Charlie、Jackson和Emily，并加入对应的用户组。

----结束

IAM 用户登录

通过前面章节，A公司在名为“A-Company”的账号中创建了名为James、Alice、Charlie、Jackson和Emily的IAM用户。完成IAM用户创建后，A公司管理员需要将账号名、IAM用户名及初始密码告知对应的员工，这些员工就可以使用自己的用户名及密码访问云服务平台。

步骤1 在登录页面，单击登录下方的“IAM用户登录”，在“IAM用户登录”页面，输入“账号名”、“用户名/邮箱”和“密码”。

步骤2 单击“登录”，登录云服务平台。

----结束

3 用户指南

3.1 使用前必读

IAM 的使用对象

IAM的使用对象为管理员：

- 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。

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：**开通云审计服务**。

账号

账号是资源的归属，对其所拥有的资源具有完全控制权限，可以访问所有云服务。

IAM 用户

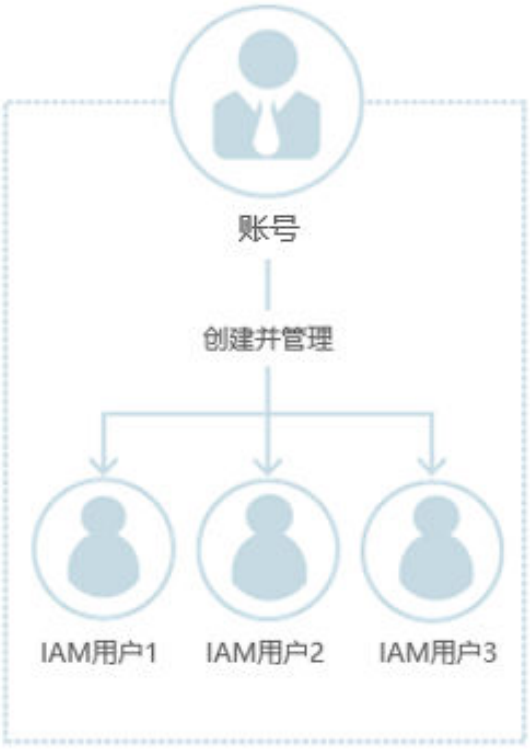
由管理员在IAM中创建的用户，IAM用户可以使用账号名、IAM用户名和密码登录系统，并根据权限使用所属账号中的资源。IAM不拥有资源，IAM用户的权限和资源由所属账号统一控制。

账号与 IAM 用户的关系

账号与IAM用户可以类比为父子关系，账号对其拥有的资源具有完全控制权限。

IAM用户由管理员创建，权限由管理员分配，管理员可以随时修改或者撤销IAM用户的权限。

图 3-1 账号和 IAM 用户的关系



用户组

用户组是权限控制的最小单位，您可以使用用户组来为IAM用户授权。默认情况下，新创建的IAM用户没有任何权限，需要将其加入用户组，并给用户组授权，用户组中的用户将获得用户组的权限。授权后，IAM用户就可以基于权限对云服务进行操作。

“admin”为缺省用户组，具有所有云服务资源的操作权限。将用户加入该用户组后，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 3-2 用户组

权限

IAM预置了各服务的常用权限，例如管理员权限、只读权限，您可以直接使用这些权限。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。

- 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。

3.2 IAM 用户

3.2.1 创建 IAM 用户

如果您是**管理员**，在云服务平台创建了多种资源，例如弹性云服务器、云硬盘、裸金属服务器等，您需要将资源分配给企业中不同的员工或者应用程序使用，为了避免分享自己的账号密码，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。

默认情况下，**新创建的IAM用户没有任何权限**，管理员需要为其授予权限，或将其加入用户组，并**给用户组授权**，用户组中的用户将获得用户组的权限。IAM用户拥有权限后，IAM用户就可以基于权限对云服务进行操作。

“admin”为缺省用户组，具有所有云服务资源的操作权限。将用户加入该用户组后，用户可以操作并使用所有云服务资源，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。

说明

如果删除并重新创建同名用户，则需要重新授权。

操作步骤

步骤1 管理员登录IAM控制台。

步骤2 在左侧导航窗格中，选择“用户”，单击右上方的“创建用户”。

步骤3 在“创建用户”页面配置“用户信息”。如需一次创建多个用户，可以单击“添加用户”进行批量创建，每次最多可创建10个用户。

表 3-1 用户信息

参数	描述
用户名	自定义，不可与账号、或账号中其他IAM用户重复。
邮件地址	自定义，不可与账号、或账号中其他IAM用户重复。可用于IAM用户身份验证、重置密码。
手机号	自定义。可用于IAM用户身份验证、重置密码。
外部身份ID	IAM SSO类型的联邦用户单点登录中，与当前实体IAM用户对接的，企业自身用户的身份ID值。 为IAM用户配置**基于SAML协议的联邦身份认证**时，“外部身份ID”为必选参数（不超过128个字符）。

步骤4 选择“访问方式”。

表 3-2 访问方式

访问方式	说明
编程访问	支持用户通过API、CLI、SDK等开发工具访问云服务。
管理控制台访问	支持用户登录管理控制台访问云服务。此时凭证类型“密码”为必选项。

步骤5 选择“凭证类型”。

表 3-3 配置凭证类型

凭证类型		说明
访问密钥		创建用户完成后即可下载本次创建的所有用户的访问密钥（AK/SK）。 **一个用户最多拥有两个访问密钥。**
密码	自定义	自定义用户密码，并选择用户首次登录时是否需要重置密码。 如果您是用户的使用主体，建议您选择该方式，设置自己的登录密码，且无需勾选首次登录时重置密码。
	自动生成	系统自动生成IAM用户的登录密码，创建完用户即可下载excel形式的密码文件。将密码文件提供给用户，用户使用该密码登录。 **仅在创建单个用户时适用。**
	首次登录时设置	系统通过邮件发一次性登录链接给用户，用户登录控制台并设置密码。 如果您不是用户的使用主体，建议选择该方式，同时输入用户的邮件地址和手机，用户通过邮件中的一次性链接登录云服务平台，自行设置密码。该链接**7天**内有效。

表 3-4 配置建议

管理控制台访问	编程访问	访问凭证	建议访问方式	建议凭证类型
勾选	不勾选	无特殊要求。	管理控制台	密码
不勾选	勾选	无特殊要求。	编程访问	访问密钥
不勾选	勾选	**需要使用密码作为编程访问的凭证**（部分API要求）。	编程访问	密码
勾选	勾选	需要在**控制台验证访问密钥**（由IAM用户输入）。 例如：例如IAM用户在控制台使用云数据迁移CDM服务创建数据迁移，需要通过访问密钥进行身份验证。	编程访问和管理控制台	密码和访问密钥

步骤6 选择“登录保护”设置。仅访问方式勾选管理控制台访问时，可以开启。

- 开启登录保护（推荐）：开启登录保护后，IAM用户登录时，除了在登录页面输入用户名和密码外（第一次身份验证），还需要在登录验证页面输入验证码（第二次身份验证），该功能是一种安全实践，建议开启登录保护，多次身份认证可以提高安全性。

  您可以选择通过手机、邮箱、虚拟MFA进行登录验证。

- 不开启：创建完成后，如需开启登录保护，请参见：登录保护。

步骤7 单击“下一步”，（可选）勾选要加入的用户组，将用户加入到用户组。加入用户组后，用户将具备用户组的权限。

说明

- 如需创建新的用户组，可单击“创建用户组”，创建完成并勾选该用户组，用户将加入到新创建的用户组中。
- 如果该用户是管理员，可以将用户加入默认用户组“admin”中。
- 一个用户最多可以同时加入10个用户组。

步骤8 单击“创建用户”，IAM用户创建完成，用户列表中显示新创建的IAM用户。

- 如果“5>凭证类型”勾选了“访问密钥”，可在此页面下载访问密钥。
- 如果“5>凭证类型”勾选了“密码>自动生成”，可在此页面下载密码。

图 3-3 创建成功

----结束

后续操作

- 如果管理员在创建IAM用户时，没有将其加入任何用户组，**新创建的IAM用户没有任何权限**，管理员可以在IAM控制台为其授予权限。授权后，用户即可根据权限使用账号中的云服务资源。详情请参考**给IAM用户授权**。
- IAM用户的登录方式与账号的登录方式不同，详情请参见**IAM用户登录**。

3.2.2 给 IAM 用户授权

如果管理员在**创建IAM用户**时，没有将其加入任何用户组，**新创建的IAM用户没有任何权限**，管理员可以在IAM控制台为其授予权限。授权后，用户即可根据权限使用账号中的云服务资源。

约束与限制

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）上限为500个。

操作步骤

步骤1 管理员登录IAM控制台。

步骤2 管理员在用户列表中，单击新建的用户，右侧的“授权”。

步骤3 在授权页面，选择授权方式和权限。

- **继承所选用户组的策略**：将IAM用户加入用户组，用户将拥有所选用户组的所有权限。

  选择“继承所选用户组的策略”，请勾选用户需要加入的用户组。

- **直接给用户授权（适用于企业项目授权）**：直接给IAM用户授予云服务权限。该授权方式仅在您开通企业项目后支持。

  选择“直接给用户授权”，请勾选需要授予用户的权限，并单击页面右下角“下一步”，进入“选择授权范围”页面，参考3继续完成操作。

说明

- 如果将IAM用户加入默认用户组“admin”，则IAM用户为管理员，可以对所有云服务执行任意操作。
- 当某个用户加入多个用户组时，此用户同时拥多个用户组的权限，即取多个用户组权限的全集。
- **所有使用IAM授权的云服务的系统策略，请参见：权限集。**
- 如果您开通了企业管理，将不能创建IAM项目，请谨慎操作。

步骤4 （如授权方式选择“继承所选用户组的策略”，无需执行此步骤）在“设置最小授权范围”页面，选择授权IAM用户使用的企业项目。

步骤5 单击“确定”，完成IAM用户授权。

授权完成后，管理员可以在“权限管理>授权管理”页面查看、修改该IAM用户的权限。

----结束

3.2.3 IAM 用户登录

管理员创建IAM用户后，这个新建的IAM用户可以登录云服务平台。登录方式包括登录页面的“IAM用户登录”，以及IAM控制台提供的“IAM用户登录链接”。

登录方法 1：系统登录页面

步骤1 在系统的登录页面，单击登录下方的“IAM用户登录”，在“IAM用户登录”页面，输入账号名，IAM用户名/邮箱和密码。

- 账号名：IAM用户所属的账号。如果不知道账号名，请向**管理员**获取。
- IAM用户名/邮箱：在IAM创建用户时，输入的**IAM用户**名/邮箱。如果不知道用户名及初始密码，请向**管理员**获取。
- 密码：IAM用户的密码。

步骤2 单击“登录”，完成登录。

说明

- 如果创建IAM用户时，IAM用户没有加入任何用户组，则IAM用户不具备任何权限，不能对云服务进行操作，需要联系管理员参考**创建用户组并授权**和**用户组添加/移除用户**给IAM用户授权。
- 如果创建IAM用户时，IAM用户加入了默认用户组“admin”，则IAM用户为管理员，可以对所有云服务执行任意操作。

----结束

登录方法 2：IAM 用户专属链接

此方法需要向管理员获取专属登录链接，获取后建议您保存该链接，方便后续快速登录。使用IAM用户专属链接登录时，系统会自动识别用户的账号名，用户仅需要填写用户名和密码，方便用户快速登录。

步骤1 管理员在IAM控制台，复制“IAM用户登录链接”，并将链接发送给用户。

步骤2 用户在浏览器中打开复制的地址，输入“用户名/邮箱”和“密码”，单击“登录”，完成登录。

----结束

3.2.4 查看或修改 IAM 用户信息

管理员在IAM用户列表中，单击用户名，或者单击右侧的“安全设置”，可以查看或修改IAM用户的基本信息、所属用户组、安全设置，并查看或删除授权记录。

管理员单击搜索框右侧的“  ”，可以修改用户列表展示项目，用户名、状态、操作为默认展示项目。可选项目：外部身份ID、描述、最近一次登录时间、创建时间、访问方式、MFA（状态）、密码使用时长、访问密钥状态。

基本信息

只能修改IAM用户的基本信息，不能修改账号的基本信息。用户名称、用户ID、创建时间仅支持查看，不支持修改。

- 状态：修改IAM用户的状态，IAM用户的状态默认为启用，如果需要停止使用该IAM用户，可以将IAM用户的状态设置为“停用”。停用后，该IAM用户将无法通过任一方式访问云服务平台，包括管理控制台访问和编程访问。
- 访问模式：修改iam用户的访问方式。

  说明

  - 请参考如下说明，修改访问模式：
    - 如果IAM用户**仅需登录管理控制台访问云服务**，建议访问方式选择**管理控制台访问**，凭证类型为**密码**。
    - 如果IAM用户**仅需编程访问云服务**，建议访问方式选择**编程访问**，凭证类型为**访问密钥**。
    - 如果IAM用户**需要使用密码作为编程访问的凭证**（部分API要求），建议访问方式选择**编程访问**，凭证类型为**密码**。
    - 如果IAM用户使用部分云服务时，需要在其**控制台验证访问密钥**（由IAM用户输入），建议访问方式选择**编程访问和管理控制台访问**，凭证类型为**密码和访问密钥**。例如IAM用户在控制台使用云数据迁移CDM服务创建数据迁移，需要通过访问密钥进行身份验证。
  - 如果当前IAM用户的访问模式为**编程访问**或**编程访问和管理控制台访问**，取消编程访问可能会使IAM用户无法访问云服务，请谨慎修改。
- 描述：修改IAM用户的描述信息。

所属用户组

所属用户组表示用户具备的权限，**通过修改IAM用户的所属用户组可以修改用户的权限**。如需修改用户所属用户组权限，请参见：查看或修改用户组。

只能修改IAM用户的所属用户组，账号属于默认用户组“admin”，不能修改。

- 单击“加入到用户组”，在“配置用户组”中选择需要加入的用户组。一个用户可以加入一个或是多个用户组。用户加入用户组后，拥有用户组的所有权限。
- 单击IAM用户所属用户组右侧的“移除”，单击“是”，退出选中的用户组，用户将不再拥有该用户组权限。

安全设置

管理员可以该页面修改IAM用户的多因素认证设备、登录凭证、登录保护和访问密钥。IAM用户如需修改自己的手机号、邮件地址、虚拟MFA设备，请参考**安全设置概述**。

- 多因素认证设备，只能修改IAM用户的多因素认证设备，不能修改账号的多因素认证设备。
  - 修改用户的手机、邮件地址。

    说明

    修改IAM用户绑定手机号和邮件地址不可与账号、其他IAM用户重复。
  - 虚拟MFA设备：给用户重置虚拟MFA设备。更多有关多因素认证以及MFA的介绍，详情请参见：**多因素认证与虚拟MFA**。
- 登录凭证：修改IAM用户的登录密码，详情请参见：**修改IAM用户密码**。
- 登录保护：修改IAM用户的登录验证方式，支持虚拟MFA、手机和邮箱。

  登录保护表示用户登录控制台时，除了在登录页面输入用户名和密码（第一次身份认证），还需要在“登录验证”页面输入验证码（第二次身份验证），该功能默认关闭。
- 访问密钥：管理IAM用户的访问密钥，详情请参见：**管理IAM用户访问密钥**。

授权记录

管理员可以查看或删除IAM用户所拥有的权限。如需修改该IAM用户的权限，请参考**所属用户组**。

图 3-4 IAM 用户授权记录

如需查看账号下所有授权记录，请参考：**查看授权记录**。

说明

删除授权记录，将删除该IAM用户所属用户组的权限，该用户组中所有IAM用户不再拥有该权限，请谨慎操作。

3.2.5 删除 IAM 用户

注意

请谨慎删除IAM用户，删除后该IAM用户将无法登录，该用户的IAM用户名、IAM密码、访问密钥、及其所有IAM授权关系将被清除且不可恢复。

- 请排查要删除的用户是否有其他服务或场景在使用，若无法确定，建议先使用"停用"功能，以免业务运行失败后无法回退。如需暂时停用IAM用户，请参考**基本信息**。
- 如需将IAM用户从某个用户组移除，请参见：**用户组添加/移除用户**。

操作步骤

步骤1 进入IAM控制台，在左侧导航栏选择“用户”页签。

步骤2 单击需要删除的IAM用户操作列的“删除”，确认弹窗中删除用户的信息，单击“是”，删除成功。

----结束

批量删除 IAM 用户

步骤1 进入IAM控制台，在左侧导航栏选择“用户”页签。

步骤2 在用户列表中，勾选需要删除的用户。勾选完成后，单击用户列表上方的“删除”。

步骤3 弹窗中单击“是”，完成所选IAM用户删除。

----结束

3.2.6 修改 IAM 用户密码

如果IAM用户忘记了登录密码，并且没有绑定邮件地址或者手机，可以由管理员在IAM中重置密码。

管理员在IAM用户列表中，单击右侧的“安全设置”，在“安全设置”页签，单击“登录凭证>登录密码”右侧的，重置IAM用户的登录密码。

说明

- IAM提供的安全设置功能，适用于管理员重置IAM用户的密码。
- IAM用户可以在**账号设置**页面修改自己的密码。。

- 通过邮件地址设置：用户通过邮件中的一次性链接登录控制台时，自行设置密码。
- 自动生成：系统自动生成随机密码，创建用户成功后可以下载并将新密码发送给用户。
- 自定义：管理员自定义用户的密码，并将新密码发送给用户。

3.2.7 管理 IAM 用户访问密钥

访问密钥即AK/SK（Access Key ID/Secret Access Key），是您通过开发工具（API、CLI、SDK）访问云服务平台时的身份凭证，不能登录控制台。系统通过AK识别访问用

户的身份，通过SK进行签名验证，通过加密签名验证可以确保请求的机密性、完整性和请求者身份的正确性。

如果IAM用户不能登录控制台，在需要使用访问密钥或者访问密钥遗失的情况下，可以由管理员在IAM中管理IAM用户的访问密钥。

管理员在IAM用户列表中，单击右侧的“安全设置”，新增或者删除用户的访问密钥。

说明

- 企业联邦用户不能创建访问密钥，但可以创建临时访问凭证（临时AK/SK和SecurititytToken）。
- IAM提供的“安全设置”功能，适用于管理员管理IAM用户的访问密钥。在我的凭证中也可以管理访问密钥，我的凭证适用于所有用户在可以登录控制台的情况下，自行管理访问密钥。
- 账号和IAM用户的访问密钥是单独的身份凭证，即账号和IAM用户仅能使用自己的访问密钥进行API调用。

- 新增访问密钥并下载
  a. 单击“新增访问密钥”。

     说明

     每个用户最多可以拥有2个访问密钥，有效期为永久。为了安全性，建议管理员定期给用户更换访问密钥。

  b. 若开启操作保护，则管理员需输入验证码或密码。
  c. 单击“确定”，生成并下载访问密钥后，将访问密钥提供给用户。
- 删除访问密钥
  a. 单击“删除”。
  b. 若开启操作保护，则管理员需输入验证码或密码。
  c. 单击“确定”。
- 启用、停用访问密钥

  新创建的访问密钥默认为启用状态，如需停用该访问密钥，步骤如下：
  a. 在“访问密钥”页签中，在需要停用的访问密钥右侧单击“停用”。
  b. 若开启操作保护，则需输入验证码或密码。然后单击“是”，停用访问密钥。

  启用访问密钥方式与停用类似，请参考以上步骤。

3.3 用户组及授权

3.3.1 创建用户组并授权

管理员可以创建用户组，并给用户组授予策略或角色，然后将用户加入用户组，使得用户组中的用户获得相应的权限。IAM预置了各服务的常用权限，例如管理员权限、只读权限，管理员可以直接使用这些系统权限给用户组授权，授权后，用户就可以基于权限对云服务进行操作。详情请参见**给IAM用户授权**。**如需查看所有云服务的系统权限，请参见：权限集**。

前提条件

在创建用户组前，建议管理员提前了解并规划以下内容：

- 了解权限的**基本概念及分类**。
- **所有使用IAM授权的云服务的系统策略，请参考：权限集**。

创建用户组

步骤1 管理员登录IAM控制台。

步骤2 在统一身份认证服务，左侧导航窗格中，选择“用户组”页签，单击右上方的“创建用户组”。

步骤3 在“创建用户组”界面，输入“用户组名称”。

步骤4 单击“确定”，用户组创建完成，用户组列表中显示新创建的用户组。

说明

您最多可以创建20个用户组，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：**如何申请扩大配额?**。

----结束

给用户组授权

以下步骤仅适用于给用户组**新增权限**。如需**移除权限**，请参见：**移除用户组权限**。

步骤1 在用户组列表中，单击新建用户组右侧的“授权”。

步骤2 在用户组选择策略页面中，勾选需要授予用户组的权限。单击“下一步”。

如果系统策略不满足授权要求，可以单击权限列表右上角的“新建策略”创建自定义策略，并勾选新创建的策略来进行精细的权限控制，自定义策略是对系统策略的扩展和补充。详情请参考**创建自定义策略**。

步骤3 选择权限的作用范围。系统会根据您所选择的策略，自动推荐授权范围方案，便于为用户选择合适的授权作用范围，**表1**为IAM提供的所有授权范围方案。

表 3-5 授权范围方案

可选方案	方案说明
所有资源	授权后，IAM用户可以根据权限使用账号中所有资源，包括企业项目、区域项目和全局服务资源。
指定企业项目资源	选择指定企业项目，IAM用户可以根据权限使用该企业项目中的资源。**仅开通企业项目后可选。** 如果您暂未开通企业项目，将不支持基于企业项目授权，了解企业项目请参考：《企业管理用户指南》。
指定区域项目资源	选择指定区域项目，IAM用户可以根据权限使用该区域项目中的资源。 如果选择作用范围为“区域项目”，且所勾选的策略包含全局服务权限，系统自动将全局服务权限的作用范围设置为**所有资源**，勾选的区域项目权限的作用范围仍为指定区域项目。

可选方案	方案说明
全局服务资源	IAM用户可以根据权限使用全局服务。全局服务部署时不区分物理区域。访问全局级服务时，不需要切换区域，如对象存储服务（OBS）、内容分发网络（CDN）等。 如果选择作用范围为“全局服务”，且所勾选的策略包含项目级服务权限，系统自动将项目权限作用范围设置为**所有资源**，勾选的全局服务权限的作用范围仍为全局服务。

步骤4 单击“确定”，完成用户组授权。

----结束

说明

- 当一个用户被加入多个用户组，将会拥有所有已加入用户组的权限。

3.3.2 用户组添加/移除用户

管理员创建用户组并授权后，将用户加入用户组中，使用户具备用户组的权限，实现用户的授权。给已授权的用户组中添加或者移除用户，快速实现用户的权限变更。

用户组添加用户

步骤1 管理员在用户组列表中，单击新建的用户组，例如“开发人员组”，右侧的“用户管理”。

图 3-5 用户管理

步骤2 在“可选用户”中选择需要添加至用户组中的用户。

图 3-6 选择用户

步骤3 单击“确定”，完成用户授权。

----结束

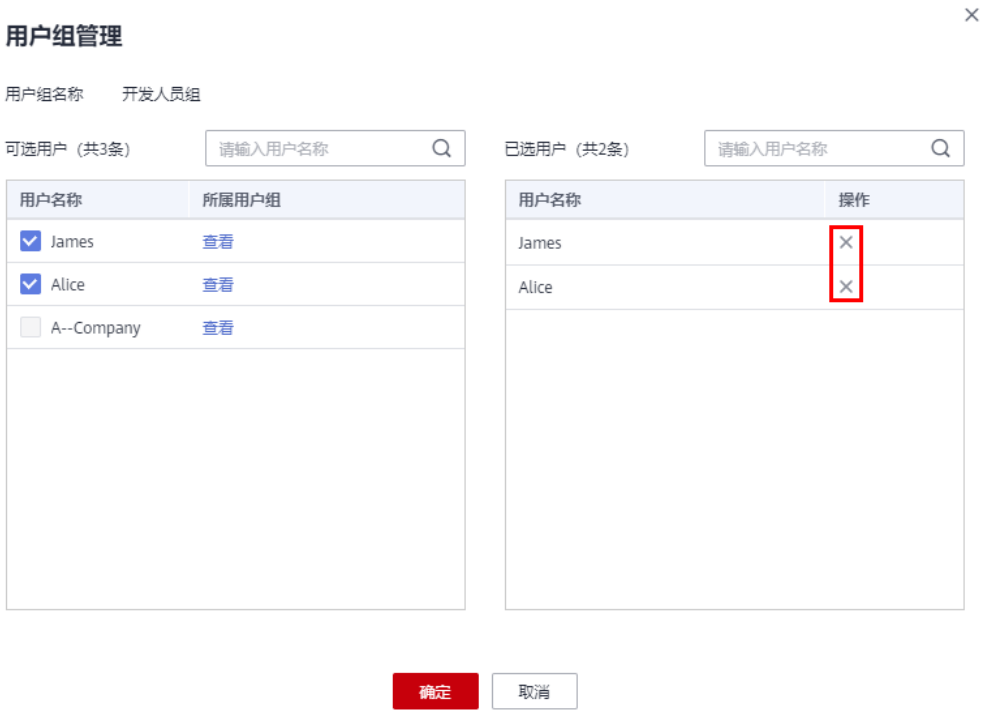
用户组移除用户

步骤1 管理员在用户组列表中，单击新建的用户组，例如“开发人员组”，右侧的“用户管理”。

图 3-7 用户管理

步骤2 在“已选用户”中，单击用户名称右侧的删除图标，单击“确定”，完成移除用户。

图 3-8 移除用户组中的用户



----结束

3.3.3 删除用户组

操作步骤

当您需要删除用户组，请参考以下操作：

步骤1 进入IAM控制台，在左侧导航栏选择“用户组”页签。

步骤2 在用户组列表中，单击用户组右侧的“删除”。

步骤3 在弹窗中选择“是”，删除勾选的用户组。

----结束

3.3.4 查看或修改用户组

查看用户组信息

管理员在用户组列表中，单击用户组左侧的 ，可以查看用户组的基本信息、权限和包含用户。

修改用户组权限

您可以进入用户组详情，在“授权记录”页签查看或修改用户组已经拥有的权限。

说明

- 修改用户组权限，将影响该用户组中所有用户的权限，请谨慎操作。
- 无法修改默认管理员用户组**admin**的权限。

1. 单击用户组的名称，例如“开发人员组”，进入用户组详情页面，在“授权记录”页签查看用户组已拥有的权限。
2. 单击需要修改权限右侧的“删除”。
3. 在确认弹窗中，单击“是”，删除当前授权。
4. 单击“授权记录”页签中的“授权”，进入给用户组授权页面。
5. 在授权页面选择对应的权限、作用范围，单击“确定”，完成用户组权限修改。
6. 单击“返回”，跳转至“用户组>授权记录”页签，确认修改后的用户组权限。

修改用户组名称和描述

管理员在用户组列表中，单击用户组右侧的“编辑”，修改用户组名称和描述。

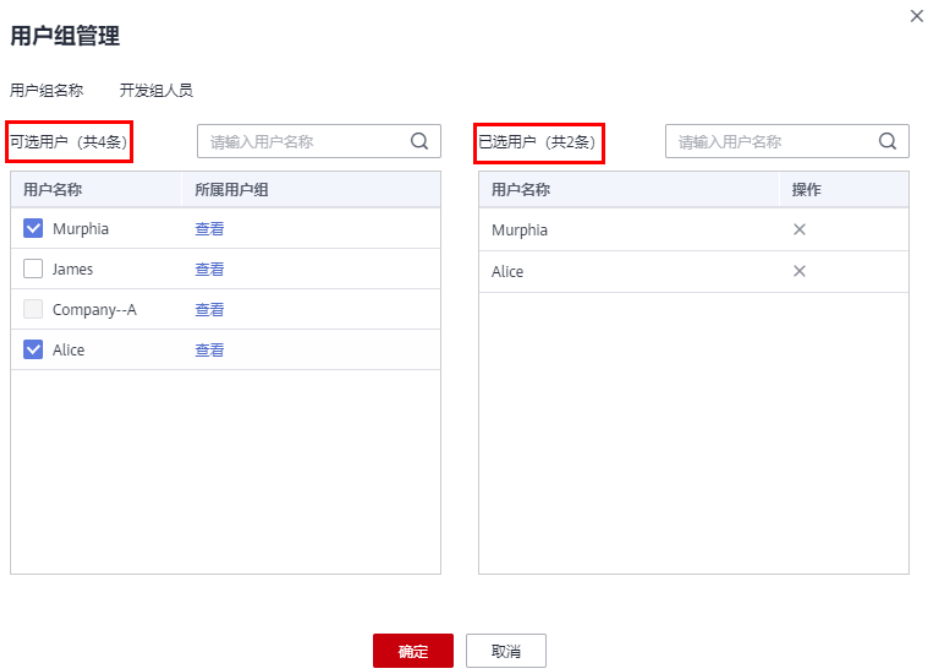
说明

如果该用户组名称已配置在身份提供商的身份转换规则中，修改用户组名称将导致对应身份转换规则失效，请谨慎操作。

修改用户组中的用户

步骤1 管理员在用户组列表中，单击用户组右侧的“用户管理”。

图 3-9 修改用户组中的用户



步骤2 在“可选用户”中选择需要添加的用户。

步骤3 在“已选用户”中选择移除对应用户。

----结束

说明

系统缺省用户组“admin”，只能修改其中包含的用户，不能修改描述信息与权限。

3.3.5 移除用户组权限

操作步骤

当您需要移除用户组中的某个权限，请参考以下操作：

步骤1 进入IAM控制台，在左侧导航栏选择“用户组”页签。

步骤2 单击用户组名称，进入用户组详情页面。

步骤3 在“授权记录”页签下，单击需要移除权限最右侧的“删除”。

步骤4 在弹窗中，单击“是”，移除用户组权限。

----结束

3.3.6 依赖角色的授权方法

由于云服务平台各服务之间存在业务交互关系，个别服务的角色依赖其他服务的角色实现功能。因此管理员在基于角色授权时，对于有依赖则需要授予依赖的角色才会生效。策略不存在依赖关系，不需要进行依赖授权。

操作步骤

步骤1 管理员登录IAM控制台。

步骤2 在用户组列表中，单击新建用户组右侧的“授权”。

步骤3 在授权页面进行授权时，管理员在权限列表的搜索框中搜索需要的角色。

步骤4 选择角色，系统将自动勾选依赖角色。

图 3-10 选择角色

步骤5 单击勾选权限下方的 ，查看角色的依赖关系。

图 3-11 查看角色的依赖关系

例如“DNS Administrator”，角色内容中存在“Depends”字段，表示存在依赖关系。给用户组授予“DNS Administrator”角色时，还需要在同项目同时授予“Tenant Guest”和“VPC Administrator”角色，“DNS Administrator”才能生效。

步骤6 单击“确定”，完成依赖角色的授权。

----结束

3.4 权限管理

3.4.1 权限基本概念

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。

权限的分类

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。由于云服务平台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。

  策略根据创建的对象，分为**系统策略**和**自定义策略**。

策略-系统策略

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。**如需查看所有云服务的系统策略，请参见：权限集**。

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。

策略-自定义策略

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IAM支持可视化视图、JSON视图两种自定义策略配置方式。

3.4.2 角色

角色是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。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。

由于云服务平台各服务之间存在业务依赖关系，因此给用户或用户组授予角色时，需要将依赖的其他角色一并授予该用户或用户组，保证权限生效。具体请参见：**依赖角色的授权方法**。

角色内容

给用户组选择角色时，单击角色前面的 ，可以查看角色的详细内容，以“DNS Administrator”为例，说明角色的内容。

图 3-12 DNS Administrator 角色内容


```
{
  "Version": "1.0",
  "Statement": [
    {
      "Action": [
        "DNS:Zone:*",
        "DNS:RecordSet:*",
        "DNS:PTRRecord:*"
      ],
      "Effect": "Allow"
    }
  ],
  "Depends": [
    {
      "catalog": "BASE",
      "display_name": "Tenant Guest"
    },
    {
      "catalog": "VPC",
      "display_name": "VPC Administrator"
    }
```

```
  ]
}
```

参数说明

表 3-6 参数说明

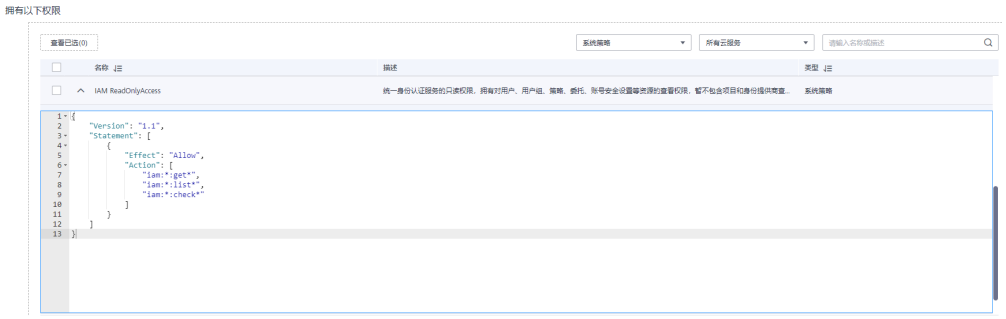
参数		含义	值
Version		角色的版本	1.0：代表基于角色的访问控制。
Statement： 角色的授权语句	Action：授权项	操作权限	格式为：服务名:资源类型:操作 "DNS:Zone:*"：表示对DNS的Zone所有操作。其中“DNS”为服务名；“Zone”为资源类型；“*”为通配符，表示对Zone资源类型可以执行所有操作。
	Effect：作用	定义Action中的操作权限是否允许执行	• Allow：允许执行。 • Deny：不允许执行。 **说明** 当同一个Action的Effect既有Allow又有Deny时，遵循Deny优先的原则。
Depends： 角色的依赖关系	catalog	依赖的角色所属服务	服务名称。例如：BASE、VPC。
	display_name	依赖的角色名称	角色名称。 **说明** 给用户组授予示例的“DNS Administraor”角色时，必须同时勾选该角色依赖的角色“Tenant Guest”和“VPC Administrator”，“DNS Administraor”才会生效。 了解更多角色依赖关系，请参考：权限集。

3.4.3 策略

3.4.3.1 策略内容

给用户组选择策略时，单击策略前面的 ，可以查看策略的详细内容，以系统策略“IAM ReadOnlyAccess”为例。

图 3-13 IAM ReadOnlyAccess 策略内容




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

3.4.3.2 策略语法

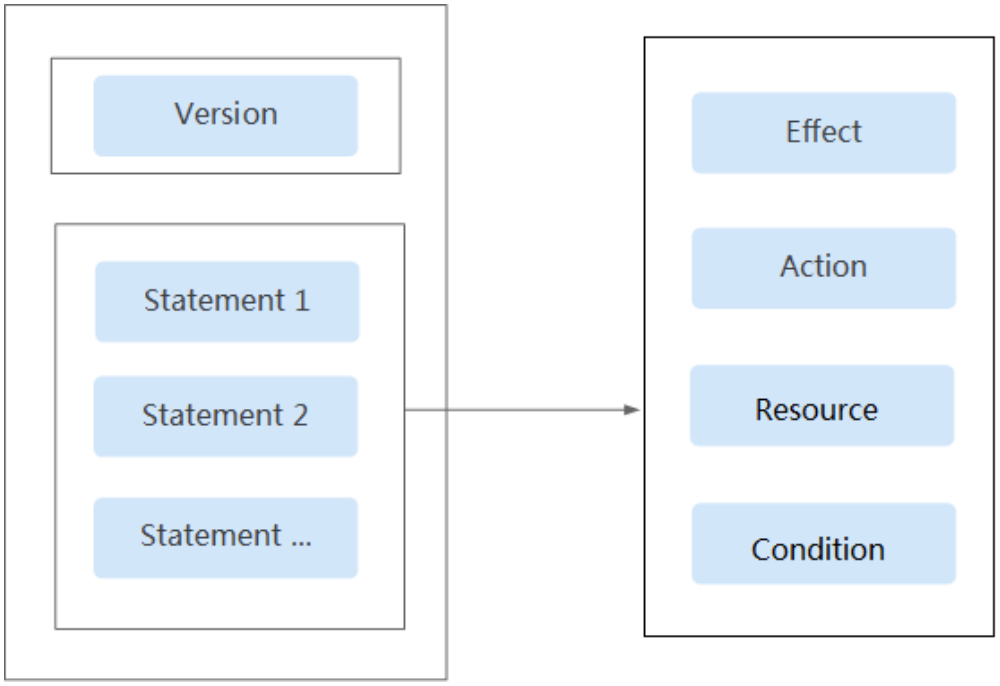
下面以OBS的自定义策略为例，说明策略的语法。

```
{
   "Version": "1.1",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
            "obs:bucket:ListAllMyBuckets",
            "obs:bucket:HeadBucket",
            "obs:bucket:ListBucket",
            "obs:bucket:GetBucketLocation"
         ],
         "Condition": {
            "StringEndWithIfExists": {
               "g:UserName": [
                  "specialCharacter"
               ]
            },
            "Bool": {
               "g:MFAPresent": [
                  "true"
               ]
            }
         },
         "Resource": [
            "obs:*:*:bucket:*"
         ]
      }
   ]
}
```

策略结构

策略结构包括Version（策略版本号）和Statement（策略权限语句）两部分，其中Statement可以有多个，表示不同的授权项。

图 3-14 策略结构



策略参数

策略参数包含Version和Statement两部分，下面介绍策略参数详细说明。了解策略参数后，您可以根据场景自定义策略，如**自定义策略使用样例**。

表 3-7 策略参数说明

参数		含义	值
Version		策略的版本。	1.1：代表基于策略的访问控制。
Statement： 策略的授权语句	Effect：作用	定义Action中的操作权限是否允许执行。	• Allow：允许执行。 • Deny：不允许执行。 **说明** 当同一个Action的Effect既有Allow又有Deny时，遵循Deny优先的原则。
	Action：授权项	操作权限。	格式为“服务名:资源类型:操作”。授权项支持通配符号*，通配符号*表示所有。 示例： "obs:bucket:ListAllMybuckets"：表示查看OBS桶列表权限，其中obs为服务名，bucket为资源类型，ListAllMybuckets为操作。 您可以在对应服务“API参考”资料中查看该服务所有授权项。

参数		含义	值
	Condition：条件	使策略生效的特定条件，包括**条件键**和**运算符**。	格式为“条件运算符:{条件键：[条件值1,条件值2]}”。 如果您设置多个条件，同时满足所有条件时，该策略才生效。 示例: "StringEndWithIfExists": {"g:UserName": ["specialCharacter"]}：表示当用户输入的用户名以"specialCharacter"结尾时该条statement生效。
	Resource:资源类型	策略所作用的资源。	格式为“服务名:region:domainId:资源类型:资源路径”，资源类型支持通配符号*，通配符号*表示所有。 示例： ● "obs:*:*:bucket:*": 表示所有的OBS桶。 ● "obs:*:*:object:my-bucket/my-object/*": 表示my-bucket桶my-object目录下的所有对象。

- **条件键**

  条件键表示策略语句的 Condition 元素中的键值。根据适用范围，分为全局条件键和服务条件键。

  – 全局级条件键（前缀为g:）适用于所有操作，IAM提供两种全局条件键：**通用全局条件键**和**其他全局条件键**。

    ▪ 通用全局条件键：在鉴权过程中，云服务不需要提供用户身份信息，IAM将自动获取并鉴权。详情请参见：**通用全局条件键**。

    ▪ 其他全局条件键：在鉴权过程中，IAM通过云服务获取条件信息并鉴权。

  – 服务级条件键（前缀为服务缩写，如obs:）仅适用于对应服务的操作，详情请参见对应云服务的用户指南。

表 3-8 通用全局条件键

全局条件键	类型	说明
g:CurrentTime	时间	接收到鉴权请求的时间。以 ISO 8601 格式表示，例如：2012-11-11T23:59:59Z
g:DomainName	字符串	账号名称
g:MFAPresent	布尔值	是否使用MFA多因素认证方式获取Token

全局条件键	类型	说明
g:MFAAge	数值	通过MFA多因素认证方式获取的Token的生效时长。该条件需要和g:MFAPresent一起使用
g:ProjectName	字符串	项目名称
g:ServiceName	字符串	服务名称
g:UserId	字符串	IAM用户ID
g:UserName	字符串	IAM用户名

- **运算符**

  运算符与条件键、条件值一起构成完整的条件判断语句，当请求信息满足该条件时，策略才能生效，详情请参见：**运算符**。运算符可以增加后缀“IfExists”，表示对应请求值为空或满足条件的请求值均使策略生效，如“StringEqualsIfExists”表示请求值为空或请求值等于条件值均使策略生效。

  表 3-9 运算符（字符串型运算符，如未增加说明，不区分大小写。）

运算符	类型	说明
StringEquals	字符串	请求值等于条件值（区分大小写）
StringNotEquals	字符串	请求值不等于条件值（区分大小写）
StringEqualsIgnoreCase	字符串	请求值等于条件值
StringNotEqualsIgnoreCase	字符串	请求值不等于条件值
StringLike	字符串	请求值包含条件值
StringNotLike	字符串	请求值不包含条件值
StringStartWith	字符串	请求值以条件值开头
StringEndWith	字符串	请求值以条件值结尾
StringNotStartWith	字符串	请求值不以条件值开头
StringNotEndWith	字符串	请求值不以条件值结尾
StringEqualsAnyOf	字符串	可配置多个条件值，请求值与任意一个条件值相同（区分大小写）
StringNotEqualsAnyOf	字符串	可配置多个条件值，请求值与所有条件值都不同（区分大小写）

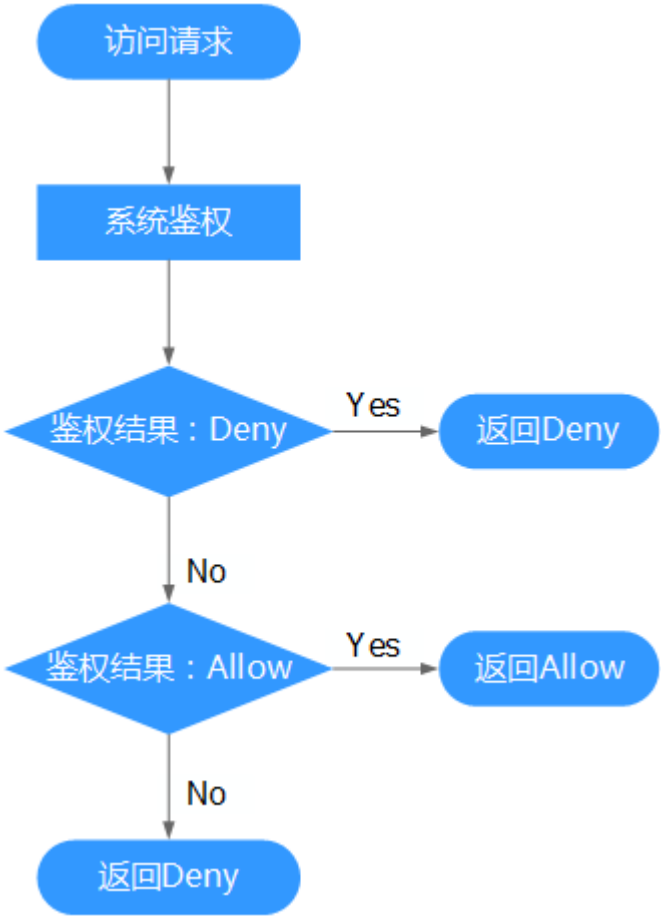
运算符	类型	说明
StringEqualsIgnoreCaseAnyOf	字符串	可配置多个条件值，请求值与任意一个条件值相同
StringNotEqualsIgnoreCaseAnyOf	字符串	可配置多个条件值，请求值与所有条件值都不同
StringLikeAnyOf	字符串	可配置多个条件值，请求值包含任意一个条件值
StringNotLikeAnyOf	字符串	可配置多个条件值，请求值不包含所有条件值
StringStartWithAnyOf	字符串	可配置多个条件值，请求值以任意一个条件值开头
StringEndWithAnyOf	字符串	可配置多个条件值，请求值以任意一个条件值结尾
StringNotStartWithAnyOf	字符串	可配置多个条件值，请求值不以任意一个条件值开头
StringNotEndWithAnyOf	字符串	可配置多个条件值，请求值不以任意一个条件值结尾
NumberEquals	数值	请求值等于条件值
NumberNotEquals	数值	请求值不等于条件值
NumberLessThan	数值	请求值小于条件值
NumberLessThanEquals	数值	请求值小于或等于条件值
NumberGreaterThan	数值	请求值大于条件值
NumberGreaterThanEquals	数值	请求值大于或等于条件值
NumberEqualsAnyOf	数值	可配置多个条件值，请求值与任意一个条件值相同
NumberNotEqualsAnyOf	数值	可配置多个条件值，请求值与所有条件值都不同
DateLessThan	时间	请求值早于条件值
DateLessThanEquals	时间	请求值早于或等于条件值
DateGreaterThan	时间	请求值晚于条件值
DateGreaterThanEquals	时间	请求值晚于或等于条件值
Bool	布尔值	请求值等于条件值

运算符	类型	说明
IpAddress	IP地址	请求值在条件值所设置的IP地址范围内
NotIpAddress	IP地址	请求值不在条件值所设置的IP地址范围内
IsNullOrEmpty	空值	请求值为null或者空字符串
IsNull	空值	请求值为null
IsNotNull	空值	请求值不为null

3.4.3.3 策略鉴权规则

用户在发起访问请求时，系统根据用户被授予的访问策略中的action进行鉴权判断。鉴权规则如下：

图 3-15 系统鉴权逻辑图



1. 用户发起访问请求。
2. 系统在用户被授予的策略中寻找请求对应的action，优先寻找Deny指令。如果找到一个适用的Deny指令，系统将返回Deny决定。
3. 如果没有找到Deny指令，系统将寻找适用于请求的任何Allow指令。如果找到一个Allow指令，系统将返回Allow决定。

4. 如果找不到Allow指令，最终决定为Deny，鉴权结束。

3.4.4 查看授权记录

如果您需要查看当前账号下的所有授权关系，可以进入“权限管理>授权管理”页面。IAM权限管理为您呈现账号中的所有授权关系，支持使用**“策略名”**、**“用户名/用户组名/委托名”**、**“项目区域”**、**“企业项目（已开启企业项目）”**“**主体类型**”为过滤条件查看指定授权关系。

- 如果您已开通并使用企业项目，可以选择IAM项目视图、企业项目视图，分别查看IAM项目、企业项目的授权关系。
- 如果您暂未开通企业项目，将自动显示IAM项目视图。

IAM 项目视图

在IAM项目视图下，您可以选择如下过滤条件查看对应授权记录。

- **策略名**：权限的名称。单击权限名称可以查看权限详情。

  如需查看指定权限的授权记录，选择过滤条件为“策略名”，输入指定权限名称，查看该权限的授权记录。如需查看所有云服务的系统权限，请参见：**权限集**。
- **用户名/用户组名/委托名**：IAM用户、用户组、委托的名称。

  如需查看指定IAM用户/用户组/委托的IAM项目授权记录，选择过滤条件为“用户名”、“用户组名”或“委托名”，输入指定对应名称，查看其授权记录。

  说明

  基于IAM项目授权，最小授权单位为用户组。查看IAM项目视图下指定IAM用户授权记录时，将显示该IAM用户所属用户组的授权记录。
- **项目区域**：IAM项目或区域名称，即权限的作用范围。查看IAM项目授权情况，请选择：
  - 全局服务：查看所有全局服务授权记录。
  - 所有项目：查看基于所有项目授权的授权记录。基于“所有项目”授权，权限对所有项目都生效，包括全局服务和所有项目（包括未来创建的项目）。
  - 指定项目：查看基于默认区域、子项目授权的授权记录。
- **主体类型**：授权对象类型，可以选择用户、用户组、委托3种。IAM项目视图下，可以选择主体类型为“用户组”、“委托”，如果选择“用户”，筛选结果为空。
- **企业项目**：企业项目的名称。如果您在IAM用户视图下，选择“企业项目”为过滤条件，并输入企业项目名称，将自动切换至企业项目视图。

企业项目视图

在企业项目视图下，您可以选择如下过滤条件查看对应授权记录。

- **策略名**：权限的名称。单击权限名称可以查看权限详情。

  如需查看指定权限的授权记录，选择过滤条件为“策略名”，输入指定权限名称，查看该权限的授权记录。如需查看企业项目支持的云服务权限，请参见：企业管理用户指南中的“云服务权限说明”章节。
- **用户名/用户组名/委托名**：IAM用户、用户组、委托的名称。

如需查看指定IAM用户/用户组的企业项目授权记录，选择过滤条件为“用户名”、“用户组名”，输入指定对应名称，查看其授权记录。

说明

- 企业项目不支持委托功能，请选择过滤条件为“用户名”、“用户组名”。
- 基于企业项目授权，最小授权单位为用户，查看企业项目视图下指定IAM用户授权记录时，显示该IAM用户及其所属用户组的授权记录。

- **企业项目**：企业项目的名称，即权限的作用范围。查看指定企业项目的授权记录，选择区域过滤条件为“企业项目”，输入企业项目名称，查看基于该企业项目的所有授权记录。
- **主体类型**：授权对象类型，可以选择用户、用户组、委托3种。企业项目视图下，可以选择主体类型为“用户”、“用户组”；如果选择“委托”，筛选结果为空。
- **项目区域**：IAM项目或区域。如果您在企业项目视图下，选择“项目区域”为过滤条件，并选择指定项目，将自动切换至**IAM项目视图**。

3.4.5 自定义策略

3.4.5.1 创建自定义策略

如果系统策略不满足授权要求，管理员可以创建自定义策略，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IAM支持以下两种方式创建自定义策略：

- 可视化视图：通过可视化视图创建自定义策略，无需了解JSON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。
- JSON视图：通过JSON视图创建自定义策略，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。

可视化视图配置自定义策略

步骤1 登录IAM控制台。

步骤2 在统一身份认证服务，左侧导航窗格中，选择“权限管理>策略”页签，单击右上方的“创建自定义策略”。

步骤3 输入“策略名称”。

图 3-16 输入策略名称

步骤4 “策略配置方式”选择“可视化视图”。

步骤5 在“策略内容”下配置策略。

1. 选择“允许”或“拒绝”。
2. 选择“云服务”。

   说明

   - 此处只能选择一个云服务，如需配置多个云服务的自定义策略，请在完成此条配置后，单击“添加权限”，创建多个服务的授权语句；或使用**JSON视图配置自定义策略**。
   - 暂不支持一个自定义策略同时包含全局级云服务和项目级云服务。如果需要同时设置全局级服务和项目级服务的自定义策略，请创建两条自定义策略，便于授权时设置最小授权范围。
3. 选择“操作”，根据需求勾选产品权限。
4. （可选）选择资源类型，如选择“特定资源”可以单击“通过资源路径指定”来指定需要授权的资源。

表 3-10 资源类型

类型	说明
特定资源	授予IAM用户特定资源的相应权限。如授予IAM用户以TestBucket命名开头的桶相应权限，需将bucket设置为通过资源路径指定，添加资源路径：OBS:*:*:bucket:TestBucket*。 **说明** - 指定桶资源： 【格式】OBS:*:*:bucket:*桶名称* 对于桶资源，IAM自动生成资源路径前缀“**obs:*:*:bucket:**”。通过**桶名称**指定具体的资源路径，支持通配符*。例如：obs:*:*:bucket:*表示任意OBS桶。 - 指定对象资源： 【格式】OBS:*:*:object:*桶名称/对象名称* 对于对象资源，IAM自动生成资源路径前缀“**obs:*:*:object:**”。通过**桶名称/对象名称**指定具体的资源路径，支持通配符*。例如：obs:*:*:object:my-bucket/my-object/*表示my-bucket桶下my-object目录下的任意对象。
所有资源	授予IAM用户所有资源的相应权限。

5. （可选）添加条件，单击“添加条件”，选择“条件键”，选择“运算符”，根据运算符类型填写相应的值。

表 3-11 条件参数

参数名称	参数说明
条件键	条件键表示策略语句的 Condition 元素中的键值。分为全局条件键和服务级条件键。全局级条件键（前缀为g:）适用于所有操作，详情请参见：**全局级请求条件**；服务级条件键（前缀为服务缩写，如obs:）仅适用于对应服务的操作，详情请参见对应云服务的用户指南。
运算符	与条件键、条件值一起使用，构成完整的条件判断语句。
值	与条件键、运算符一起使用，当运算符需要某个关键字时，需要输入关键字的值，构成完整的条件判断语句。

图 3-17 添加请求条件

表 3-12 全局级请求条件

全局条件键	条件类型	说明
g:CurrentTime	时间	接收到鉴权请求的时间。以 ISO 8601 格式表示，例如：2012-11-11T23:59:59Z。
g:DomainName	字符串	账号名称。
g:MFAPresent	布尔值	是否使用MFA多因素认证方式获取Token。
g:MFAAge	数值	通过MFA多因素认证方式获取的Token的生效时长。该条件需要和g:MFAPresent一起使用。
g:ProjectName	字符串	项目名称。
g:ServiceName	字符串	服务名称。

全局条件键	条件类型	说明
g:UserId	字符串	IAM用户ID。
g:UserName	字符串	IAM用户名。

步骤6 （可选）在“策略配置方式”选择JSON视图，将可视化视图配置的策略内容转换为JSON语句，您可以在JSON视图中对策略内容进行修改。

说明

如果您修改后的JSON语句有语法错误，将无法创建策略，可以自行检查修改内容或单击界面弹窗中的“重置”，将JSON文件恢复到未修改状态。

步骤7 （可选）如需创建多条自定义策略，请单击“添加权限”；也可在已创建的策略最右端单击“+”，复制此权限。

步骤8 输入“策略描述”（可选）。

步骤9 单击“确定”，自定义策略创建完成。

步骤10 将新创建的自定义策略授予用户组，使得用户组中的用户具备自定义策略中的权限。

说明

给用户组授予自定义策略与系统策略操作一致，详情请参考：**创建用户组并授权**。

----结束

JSON 视图配置自定义策略

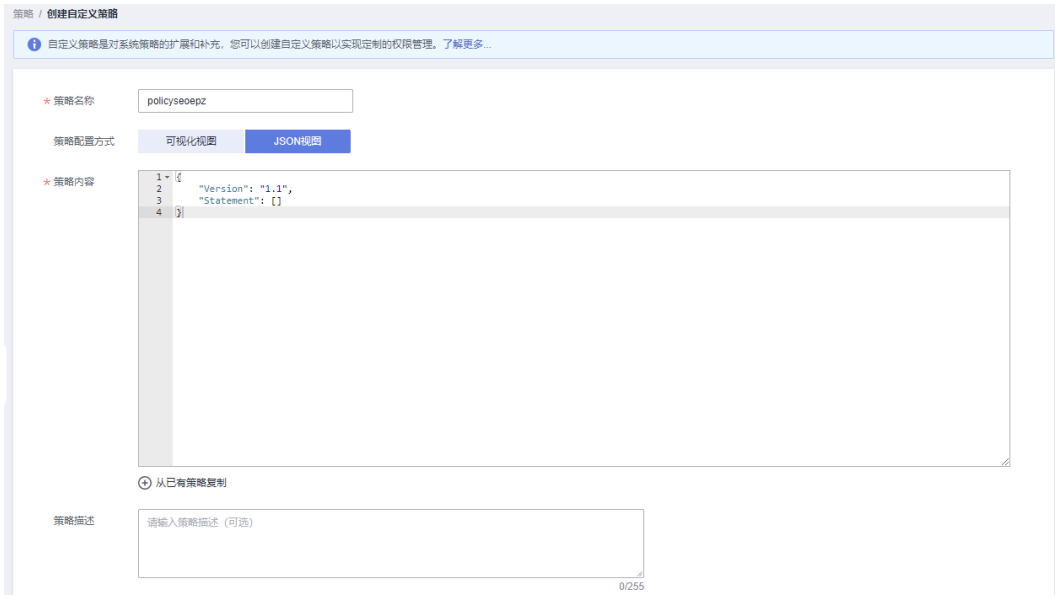
步骤1 登录IAM控制台。

步骤2 在统一身份认证服务，左侧导航窗格中，选择“权限管理>策略”页签，单击右上方的“创建自定义策略”。

图 3-18 创建自定义策略

步骤3 输入“策略名称”。

图 3-19 输入策略名称



步骤4 “策略配置方式”选择“JSON视图”。

步骤5 （可选）在“策略内容”区域，单击“从已有策略复制”，例如选择“EVS Admin”作为模板。

说明

此处可以同时选择多个服务的策略，这些策略的作用范围必须一致，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，便于授权时设置最小授权范围。

步骤6 单击“确定”。

步骤7 修改模板中策略授权语句。

- 作用（Effect）：允许（Allow）和拒绝（Deny）。
- 权限集（Action）：写入各服务API授权项列表（如所示）中“授权项”中的内容，例如："evs:volumes:create"，来实现细粒度授权。

说明

自定义策略版本号（Version）固定为1.1，不可修改。

步骤8 （可选）输入“策略描述”。

步骤9 单击“确定”后，系统会自动校验语法，如跳转到策略列表，则自定义策略创建成功；如提示“策略内容错误”，请按照语法规范进行修改。

步骤10 将新创建的自定义策略授予用户组，使得用户组中的用户具备自定义策略中的权限。

说明

给用户组授予自定义策略与系统策略操作一致，详情请参考：**创建用户组并授权**。

----结束

3.4.5.2 修改、删除自定义策略

本章为您介绍如何修改和删除已创建的自定义策略。

修改自定义策略

修改自定义策略名称、描述和内容。

1. 管理员在IAM控制台左侧导航窗格中，选择“权限管理>策略”页签。
2. 在指定策略的操作列中单击“编辑”，或者单击需要修改的策略名称，进入策略详情页。
3. 可根据需要修改“策略名称”和“策略描述”。
4. 按**可视化视图配置自定义策略**方式修改策略。
5. 单击“确定”完成修改。

删除自定义策略

说明

如果当前自定义策略已被授权给用户组或委托，则无法删除。移除该用户组或委托中的自定义策略后，才可删除自定义策略。

1. 管理员在IAM控制台左侧导航窗格中，选择“权限管理>策略”。
2. 在指定策略的操作列中单击“删除”。
3. 单击“确定”完成删除。

3.4.5.3 自定义策略使用样例

配合较高权限系统策略使用

如果您给IAM用户授予较高权限的系统策略，例如“FullAccess”，但不希望IAM用户拥有某个服务的权限，例如云审计服务。您可以创建一个自定义策略，并将自定义策略的Effect设置为Deny，然后将较高权限的系统策略和自定义策略同时授予用户，根据Deny优先原则，则授权的IAM用户除了云审计服务，可以对其他所有服务执行所有操作。

以下策略样例表示：拒绝IAM用户使用云审计服务。

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

说明

- Action为授权项，格式为：服务名:资源类型:操作。

  "cts:*:*"：表示对云审计的所有操作。其中cts为服务名；“*”为通配符，表示对所有的资源类型可以执行所有操作。
- Effect为作用，Deny表示拒绝，Allow表示允许。

配合单个服务系统策略使用

- 如果您给IAM用户授予单个服务系统策略，例如“BMS FullAccess”，但不希望用户拥有BMS FullAccess中的创建裸金属服务器权限（bms:servers:create），可

以创建一条相同Action的自定义策略，并将自定义策略的Effect设置为Deny，然后将系统策略BMS FullAccess和自定义策略同时授予用户，根据Deny优先原则，则用户可以对BMS执行除了创建裸金属服务器外的所有操作。

以下策略样例表示：拒绝IAM用户创建裸金属服务器。

```
{
   "Version": "1.1",
   "Statement": [
      {
         "Effect": "Deny",
         "Action": [
               "bms:servers:create"
         ]
      }
   ]
}
```

- 如果您给IAM用户授予“OBS ReadOnlyAccess”权限，但不希望部分用户查看指定OBS资源（例如，不希望用户名以“TestUser”开头的用户查看以“TestBucket”命名开头的桶），可以再创建一条自定义策略来指定特定的资源，并将自定义策略的Effect设置为Deny，然后将OBS ReadOnlyAccess和自定义策略同时授予用户。根据Deny优先原则，则用户可以对以“TestBucket”命名开头之外的桶进行查看操作。

  以下策略样例表示：拒绝以TestUser命名开头的用户查看以TestBucket命名开头的桶。

```
{
      "Version": "1.1",
      "Statement": [
            {
                  "Effect": "Deny",
                  "Action": [
                        "obs:bucket:ListAllMybuckets",
                        "obs:bucket:HeadBucket",
                        "obs:bucket:ListBucket",
                        "obs:bucket:GetBucketLocation"
                  ],
                  "Resource": [
                     "obs:*:*:bucket:TestBucket*"
                  ],
                  "Condition": {
                     "StringStartWith": {
                        "g:UserName": [
                           "TestUser"
               ]
            }
         }
            }
      ]
}
```

说明

当前仅部分服务支持资源级授权，例如OBS 对象存储服务；对于不支持资源级别授权的服务，若自定义策略中含有资源类型，则无法创建成功。

完全使用自定义策略

您也可以不使用系统策略，只创建自定义策略，实现IAM用户的指定服务授权。

- 以下策略样例表示：仅允许IAM用户使用ECS、EVS、VPC、ELB、AOM

```
{
      "Version": "1.1",
      "Statement": [
            {
```

```
                "Effect": "Allow"
                "Action": [
                        "ecs:*:*",
                        "evs:*:*",
                        "vpc:*:*",
                        "elb:*:*",
                        "aom:*:*"
                ]
        }
    ]
}
```

- 以下策略样例表示：允许特定IAM用户（以TestUser命名开头）删除特定OBS对象（my-bucket桶my-object目录下的所有对象）。

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "obs:object:DeleteObject"
            ],
            "Resource": [
                "obs:*:*:object:my-bucket/my-object/*"
            ],
            "Condition": {
                "StringStartWith": {
                    "g:UserName": [
                        "TestUser"
                ]
            }
        }
    ]
}
```

- 以下策略样例表示：允许IAM用户使用除了ECS、EVS、VPC、ELB、AOM、APM外的其他所有服务。

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "*:*:*"
            ]
        },
        {
            "Action": [
                "ecs:*:*",
        "evs:*:*",
        "vpc:*:*",
        "elb:*:*",
        "aom:*:*",
        "apm:*:*"
            ],
            "Effect": "Deny"
        }
    ]
}
```

3.4.5.4 支持 IAM 资源粒度授权的云服务

如果您需要授予IAM用户特定资源的相应权限，可以**创建自定义策略**并选择特定资源，该IAM用户将仅拥有对应资源的使用权限。例如创建自定义策略时，选择资源类型并添加资源路径：OBS:*:*:bucket:TestBucket*，即可授予IAM用户以TestBucket命名开头的桶相应权限。

下表为当前支持资源级别授权的云服务及对应资源类型。

表 3-13 支持资源粒度授权的云服务及其资源类型

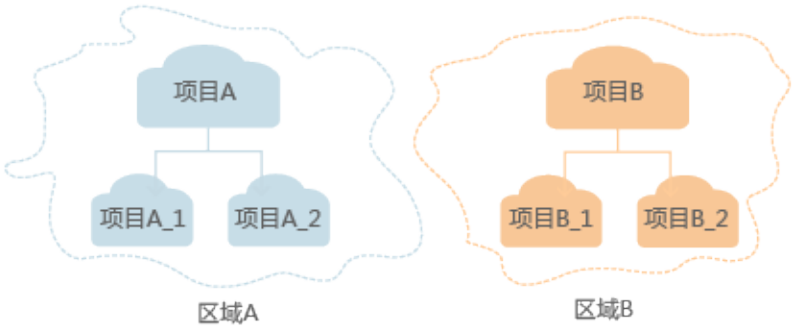
服务	资源类型	资源名称
弹性云服务器（ECS）	instance	弹性云服务器
云硬盘（EVS）	volume	云硬盘
对象存储服务（OBS）	bucket	桶
	object	对象
容器镜像服务（SWR）	chart	chart
	repository	仓库
	instance	实例
数据湖探索（DLI）	queue	队列
	database	数据库
	table	表
	column	列
	datasourceauth	安全认证信息
	jobs	作业
图引擎服务（GES）	graphName	图名称
	backupName	备份名称
函数工作流服务（FunctionGraph）	function	函数
	trigger	触发器
分布式消息服务（DMS）	rabbitmq	RabbitMQ实例
	kafka	Kafka实例
密钥管理服务（KMS）	KeyId	密钥ID

3.5 项目

每个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），以区域默认单位为项目进行授权，IAM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，并在子项目中创建资源，然后以子项目为单位进行授权，使得IAM用户仅能访问特定子项目中的资源，使得资源的权限控制更加精确。

图 3-20 项目隔离模型



说明

IAM项目中的资源不能转移。

创建项目

步骤1 在IAM控制台的左侧导航窗格中，选择“项目”页签，单击“创建项目”。

步骤2 在“所属区域”下拉列表中选择需要创建子项目的区域。

步骤3 输入“项目名称”。

说明

- 项目名称的格式为：区域默认项目名称_子项目名称，区域默认项目名称不允许修改。
- 项目名称可以由字母、数字、下划线（_）、中划线（-）组成。“区域名称_项目名称”的总长度不能大于64个字符。

步骤4 （可选）输入“描述”。

步骤5 单击“确定”，项目列表中显示新创建的项目。

----结束

基于项目给用户组授权

以子项目为单位进行授权，使得IAM用户仅能访问特定子项目中的资源，使得资源的权限控制更加精确。

步骤1 在用户组列表中，单击用户组右侧的“授权”，进入授权页面。

步骤2 在授权页面中，勾选需要授予用户组的区域级项目权限，并单击“下一步”。

步骤3 选择作用范围。此处选择区域项目，则还需要选择待授权的项目。

步骤4 单击“确定”，完成授权。

说明

更多有关用户组授权的内容，请参见**创建用户组并授权**。

----结束

切换项目或区域

登录后需要先切换区域或项目，才能访问并使用授权的云服务，否则系统将提示没有权限。全局区域服务无需切换。

步骤1 登录控制台。

步骤2 进入具体的云服务页面，若云服务为项目级服务，则单击页面左上角下拉框，选择区域。

----结束

3.6 委托

3.6.1 委托其他账号管理资源

3.6.1.1 基本流程

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。

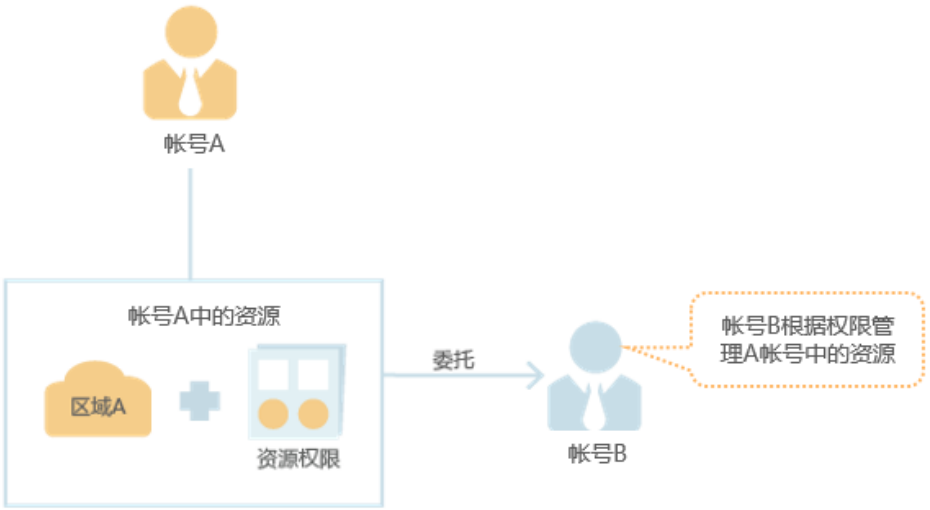
说明

只能对账号进行委托，不能对IAM用户进行委托。

如下以A账号委托B账号管理资源为例，讲述委托的原理及方法。A账号为委托方，B账号为被委托方。

步骤1 账号A创建委托。

图 3-21 账号 A 创建委托



步骤2 （可选）账号B分配委托权限。

1. 创建用户组并授予用户组管理委托的权限。

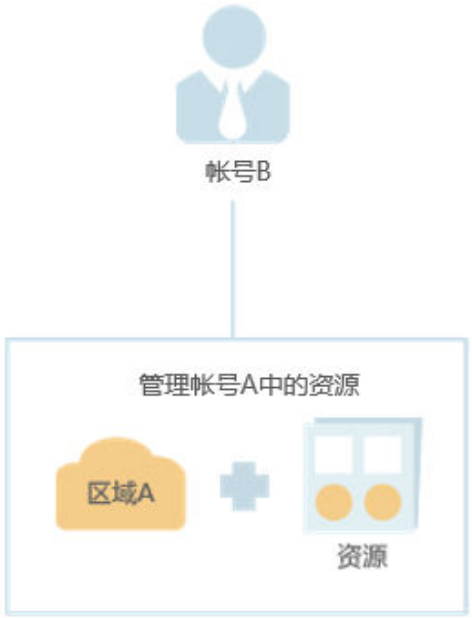
2. 创建用户并将用户加入到用户组中。

图 3-22 账号 B 分配委托权限

步骤3 账号B或者IAM用户管理委托资源。

1. 被委托方登录自己的账号，切换角色到账号A。
2. 切换到被授权的区域A，管理账号A的资源。

图 3-23 账号 B 切换角色



----结束

3.6.1.2 创建委托（委托方操作）

通过创建委托，可以将资源共享给其他账号，或委托更专业的人或团队来代为管理资源。被委托方使用自己的账号登录后，切换到委托方账号，即可管理委托方委托的资源，避免委托方共享自己的安全凭证（密码/密钥）给他人，确保账号安全。

前提条件

在创建委托前，建议管理员提前了解并规划以下内容：

- 了解权限的**基本概念及分类**。
- 规划委托需要的权限集，并确认权限是否有依赖，如果有，需要同时**设置依赖的权限**。

操作步骤

步骤1 登录IAM控制台。

步骤2 在统一身份认证服务的左侧导航窗格中，选择“委托”页签，单击右上方的“创建委托”。

步骤3 在创建委托页面，设置“委托名称”。

图 3-24 委托名称

步骤4 “委托类型”选择“普通账号”，在“委托的账号”中输入需要建立委托关系的其他账号的账号名。

说明

- 普通账号：将资源共享给其他账号或委托更专业的人或团队来代为管理账号中的资源。委托的账号只能是账号，不能是联邦用户、IAM用户。
- 云服务：授权指定云服务使用其他云服务。详情请参见：**委托其他云服务管理资源**。

步骤5 选择“持续时间”，填写“描述”信息。

步骤6 单击“下一步”，进入给委托授权页面。

步骤7 勾选需要授予委托的权限，单击“下一步”，选择权限的作用范围。

说明

- 给委托授权即给其他账号授权，给用户组授权即给账号中的IAM用户授权，两者操作方法相同，仅可选择的权限个数不同，授权操作请参见：**给用户组授权**。
- 为了保障您的账号安全，委托将不能添加Security Administrator权限，建议您按照业务场景为委托授予最小权限。

步骤8 单击“确定”，委托创建完成。

说明

委托方操作完成，将自己的账号名称、创建的委托名称、委托ID以及委托的资源权限告知被委托方后，被委托方可以通过切换角色至委托方号中管理委托资源。

----结束

3.6.1.3 （可选）分配委托权限（被委托方操作）

当其他账号与您创建了委托关系，即您是被委托方，默认情况下只有较大权限的用户（账号本身以及admin用户组中的成员）可以管理委托资源，如果您需要普通IAM用户帮助您管理委托，可以将管理委托的权限分配给IAM用户。

如果您有多个委托关系，可以授予IAM用户较大的委托权限，即管理所有的委托，也可以授予IAM用户精细的权限，仅管理指定的委托，即IAM用户进行角色切换时，仅能切换到被授权的委托中，不能切换其他委托，您可以创建细粒度的委托权限，授权IAM用户管理指定的委托。

前提条件

- 已有其他账号与您创建了委托关系。
- 您已经获取到委托方的账号名称、所创建的委托名称以及委托ID。

操作步骤

步骤1 创建用户组并授权。

1. 在用户组界面，单击“创建用户组”。
2. 输入“用户组名称”。
3. 单击“确定”，用户组创建完成。
4. 单击新建用户组右侧的“授权”。
5. 创建自定义策略。

说明

如果需要授予IAM用户精细的委托权限，仅管理指定的委托，请执行以下步骤创建细粒度的委托权限。如果不需要进行精细的委托授权，授予IAM用户管理所有的委托权限，请跳过该步骤，直接执行**f**。

a. 在选择策略页面，单击权限列表右上角“新建策略”。
b. 输入“策略名称”。
c. “策略配置方式”选择“JSON视图”。
d. 在“策略内容”区域，填入以下内容：

```
{
    "Version": "1.1",
    "Statement": [
        {
```

```
                "Action": [
                    "iam:agencies:assume"
                ],
                "Resource": {
                    "uri": [
                        "/iam/agencies/b36b1258b5dc41a4aa8255508xxx..."
                    ]
                },
                "Effect": "Allow"
            }
        ]
}
```

说明

- "b36b1258b5dc41a4aa8255508xxx..."需要替换为待授权委托的ID，需要提前向委托方获取，其他内容不需修改，直接拷贝即可。
- 本文简要讲述快速完成委托细粒度授权的必要操作，更多权限内容，详情请参考**权限管理**。

e. 单击“下一步”，继续完成授权。

6. 选择上一步创建的自定义策略或者“Agent Operator”权限，单击“下一步”。
   - 自定义策略：用户仅能管理指定ID的委托，不能管理其他委托。
   - “Agent Operator”权限：用户可以管理所有委托。
7. 选择授权范围方案。
8. 单击“确定”，用户组授权完成。

步骤2 创建IAM用户并加入用户组。

1. 在用户界面，单击“创建用户”。
2. 在创建用户界面，输入用户信息。
3. “访问方式”选择“管理控制台访问”中的“首次登录时设置”。
4. “登录保护”选择“开启”，并选择身份验证方式，单击“下一步”。
5. 在“可选用户组”中，选择**步骤1**中新创建的用户组，单击“创建用户”。
6. 完成IAM用户创建。

说明

分配委托权限操作完成，新创建的IAM用户可以通过切换角色至委托方账号中，帮助您管理委托资源。

----结束

后续操作

被委托方账号或分配了委托权限的IAM用户均可以**切换角色**至委托方账号中，查看并根据权限使用委托资源。

3.6.1.4 切换角色（被委托方操作）

当其他账号与您创建了委托关系，即您是被委托方，您已经分配了委托权限的用户，可以切换角色至委托方账号中，根据权限管理委托方的资源。

前提条件

- 已有账号与您创建了委托关系。
- 您已经获取到委托方的账号名称及所创建的委托名称。

操作步骤

步骤1 使用账号或者**步骤2**中新建的用户登录云服务平台。

说明

步骤2中新建的用户具有管理委托的权限，可以切换角色。

步骤2 鼠标移动至右上方的用户名，选择“切换角色”。

步骤3 在“切换角色”页面中，输入委托方的账号名称。

说明

输入账号名称后，系统将会按照顺序自动匹配委托名称，如果自动匹配的是没有授权的委托，系统将提示您没有权限访问，您可以删除委托名称，在下拉框中选择已授权的委托名称。

步骤4 单击“确定”，切换至委托方账号中。

----结束

后续步骤

鼠标移动至右上角的用户名，选择“切换角色”，可以返回到您自己的账号中。

3.6.2 委托其他云服务管理资源

由于云服务平台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。

当前IAM提供两种创建委托方式：

1. **在IAM控制台创建云服务委托**

   以对象存储服务OBS为例：将操作权限委托给OBS，允许OBS以您的身份使用其他服务，例如访问AOM读取监控数据。

2. 在云服务控制台使用某项资源时，系统提示您自动创建委托，以完成云服务间的协同工作。

   以创建弹性文件服务SFS委托为例：

   a. 在SFS控制台创建文件系统。
   b. 在创建文件系统页面，开启“静态数据加密”。
   c. 弹窗提示需要创建SFS委托，单击“确定”，系统自动为您在当前项目创建SFS委托，并授予KMS CMKFullAccess权限，授权成功后，SFS可以获取KMS密钥用来加解密文件系统。
   d. 您可以在IAM控制台的委托列表中查看已创建的委托。

在 IAM 控制台创建云服务委托

步骤1 登录IAM控制台。

步骤2 在统一身份认证服务的左侧导航窗格中，选择“委托”页签，单击“创建委托”。

步骤3 在创建委托页面，设置“委托名称”。

图 3-25 云服务委托名称

步骤4 “委托类型”选择“云服务”，在“云服务”中选择需要授权的云服务。

步骤5 选择“持续时间”。

步骤6 （可选）填写“委托描述”。建议填写描述信息。

步骤7 单击“下一步”，进入给委托授权页面。

步骤8 勾选需要授予委托的权限，单击“下一步”，选择权限的作用范围，给委托授权。

步骤9 单击“确定”，委托创建完成。

----结束

3.6.3 删除或修改委托

修改委托

如果需要修改委托的权限、持续时间、描述等，可以在委托列表中，单击委托右侧的“修改”，修改委托。

说明

- 云服务委托支持修改云服务、持续时间、描述、权限，委托名称、类型不支持修改。
- 修改云服务委托权限后可能会影响该云服务部分功能的使用，请谨慎操作。

删除委托

如果不再需要使用委托，可以在委托列表中，单击委托右侧的“删除”，删除委托。

3.7 安全设置

3.7.1 安全设置概述

当您需要对账号的安全信息进行设置时，可以通过“安全设置”进行操作。“安全设置”包括“**账号设置**”、“**敏感操作**”、“**登录验证策略**”、“**密码策略**”、“**访问控制**”。本章为您介绍“安全设置”的使用对象和如何进入“安全设置”。

使用对象

表 使用对象为安全设置中不同页签下对应的不同使用对象。

表 3-14 使用对象

功能	使用对象
账号设置	所有IAM用户可以修改。
敏感操作	**管理员**可以修改，普通IAM用户不可查看。
登录验证策略	**管理员**可以修改，普通IAM用户仅可查看。
密码策略	**管理员**可以修改，普通IAM用户仅可查看。
访问控制	**管理员**可以修改，普通IAM用户不可查看。

如何进入安全设置

步骤1 **管理员**登录统一身份认证服务控制台。

步骤2 在左侧导航栏中，选择“安全设置”页签。

----结束

3.7.2 账号设置

本页面的所有操作允许账号和IAM用户修改。

说明

- 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。
- 一个用户（IAM用户或账号）仅能绑定一个手机、邮件地址、虚拟MFA设备，即为敏感操作进行二次验证的设备。

登录密码、关联手机号、绑定邮件地址

修改登录密码、关联手机号、绑定邮件地址类似，以修改密码为例。

步骤1 进入安全设置。

步骤2 在“安全设置”页面中，选择“账号设置”页签，单击“登录密码”右侧的“立即修改”，进入“修改密码”页面。

步骤3 （可选）选择身份验证方式，获取并输入验证码。

说明

如果邮件地址和手机都未绑定，则无需验证。

步骤4 输入原密码、新密码并确认密码。

说明

- 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。
- 密码的强弱程度，例如密码的最小长度等，可以由管理员在密码策略中进行设置。

步骤5 单击“确定”，完成密码修改。

----结束

3.7.3 敏感操作

只有管理员可以设置敏感操作，普通IAM用户只有查看权限，不能对其进行设置，如需修改，请联系管理员为您操作或添加权限。

说明

联邦用户在执行敏感操作时，不需要进行身份验证。

虚拟 MFA

虚拟Multi-Factor Authentication (MFA) 是能产生6位数字认证码的设备，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，目前仅支持基于软件的虚拟MFA，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，非常方便，虚拟MFA是多因素认证方式中的一种。

本节介绍如何绑定虚拟MFA，如果您已安装其他MFA应用程序，请根据应用程序指引添加用户。如需了解有关解绑虚拟MFA、重置虚拟MFA的操作，请参见：虚拟MFA。

说明

您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。

步骤1 进入安全设置。

步骤2 在“安全设置>敏感操作”页面，单击“虚拟MFA”右侧的“前往绑定”。

步骤3 根据右侧弹出的绑定虚拟MFA页面，在您的MFA应用程序中添加用户。

您可以通过扫描二维码、手动输入两种方式绑定MFA设备：

- 扫描二维码

  打开手机上已安装好的MFA应用程序，选择“扫描条形码”，扫描“绑定虚拟MFA”弹窗中的二维码。扫描成功后，应用程序会自动添加用户。

- 手动输入

  打开手机上已安装好的MFA应用程序，选择“输入提供的密钥”，手动添加用户。

  说明

  手动输入添加用户方式只支持基于时间模式，建议在移动设备中开启自动设置时间功能。

步骤4 添加用户完成，在返回MFA应用程序首页，查看虚拟MFA的动态口令页面。动态口令每30秒自动更新一次。

步骤5 在“绑定虚拟MFA”页面输入连续的两组口令，然后单击“确定”，完成绑定虚拟MFA设备的操作。

----结束

登录保护

开启登录保护后，您或账号中的IAM用户在登录云服务平台时，除了在登录页面输入用户名和密码外（第一次身份验证），还需要在登录验证页面输入验证码（第二次身份验证），该功能是一种安全实践，**建议开启登录保护**，多次身份认证可以提高账号安全性。

账号只能自己开启登录保护，账号或管理员都可以为IAM用户开启登录保护。

- **管理员为IAM用户开启登录保护**

  管理员在IAM用户列表中，单击操作列的“安全设置”，单击“登录保护>验证方式”右侧的“ ”，选择验证方式为手机、邮件地址或虚拟MFA，为IAM用户开启登录保护。

- **账号开启登录保护**

  进入安全设置后，账号可以在“安全设置 > 敏感操作 > 登录保护 > ”中单击“立即设置”，选择“开启”，并设置验证方式，开启登录保护。

操作保护

- **开启操作保护**

  开启后，账号以及账号中的IAM用户进行敏感操作时，例如删除弹性云服务器资源，需要输入验证码进行验证，避免误操作带来的风险和损失。“操作保护”默认为开启状态，为了您的资源安全，建议保持开启状态。

  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。

步骤1 管理员进入安全设置。

步骤2 在“敏感操作 > 操作保护 > ”中，单击“立即启用”。

图 3-26 开启操作保护

步骤3 在右侧弹窗中选择“开启”，勾选“操作员验证”或“指定人员验证”。

如选择“指定人员验证”，开启操作保护时，需要进行初次身份核验，确保指定人员验证方式可用。

图 3-27 操作保护设置

- 操作员验证：触发敏感操作的账号或IAM用户进行二次验证。
- 指定人员验证：账号及IAM用户触发的敏感操作均由指定人员进行验证。支持手机号、邮件地址，不支持虚拟MFA验证。

步骤4 单击“确定”开启操作保护。

----结束

- **关闭操作保护**

关闭后，账号以及账号中的IAM用户进行敏感操作时，不需要输入验证码进行验证。

步骤1 管理员**进入安全设置**。

步骤2 管理员在“敏感操作>操作保护 > ”中，单击“立即修改”。

图 3-28 单击立即修改

步骤3 在右侧弹窗中选择“关闭”，并单击“确定”。

图 3-29 关闭操作保护

步骤4 在“身份验证”弹窗中输入验证码。

- 操作员验证：关闭操作保护管理员本人进行二次验证。支持手机号、邮件地址、虚拟MFA。
- 指定人员验证：由指定人员进行验证。支持手机号、邮件地址，不支持虚拟MFA验证。

步骤5 单击“确定”，关闭操作保护。

----结束

说明

- 敏感操作由各个云服务单独定义。
- 用户如果进行敏感操作，将进入“操作保护”页面，选择认证方式，包括邮件地址、手机和虚拟MFA三种认证方式。
  - 如果用户只绑定了手机号，则认证方式只能选择手机。
  - 如果用户只绑定了邮件地址，则认证方式只能选择邮件地址。
  - 如果用户未绑定邮件地址、手机和虚拟MFA，进行敏感操作时，将提示用户绑定邮件地址、手机或虚拟MFA。
- 使用邮件地址、手机进行认证可能出现收不到验证码故障，建议您使用MFA验证方式。
- 开启操作保护后，执行敏感操作时，需要输入验证码进行验证，此验证码将会发送至进行操作的IAM用户所绑定的手机号或邮件地址，而不是该IAM用户所属的账号。

访问密钥保护

- **开启访问密钥保护**

  开启后，仅管理员才可以创建、启用/停用或删除IAM用户的访问密钥。由于“访问密钥保护”默认为关闭状态，为了保障资源安全，建议开启访问密钥保护功能。

管理员进入安全设置后，在“敏感操作>访问密钥保护 > ”中，单击“ ”，开启访问密钥保护。

- **关闭访问密钥保护**

  关闭后，所有IAM用户可以创建、启用/停用或删除自己的访问密钥。

  管理员进入安全设置后，在“敏感操作>访问密钥保护 ”中，单击“ ”，关闭访问密钥保护。

自主管理用户属性

- **开启自主管理用户属性**

  开启后，所有IAM用户可以管理自己的基本信息，可以根据场景选择IAM用户可以修改的属性信息，可以选择登录密码、手机号、邮件地址。默认开启，且支持IAM用户修改所有属性。

  管理员进入安全设置后，在“安全设置 > 敏感操作>自主管理用户属性 > ”中，单击“立即启用”。在“自主管理用户属性设置”弹窗中，选择“开启”并勾选支持IAM用户自主修改的属性，单击“确定”，开启IAM用户自主管理用户属性。

- **关闭自主管理用户属性**

  关闭后，仅管理员可以管理自己的基本信息。IAM用户如需修改登录密码、手机号、邮件地址，请联系管理员参考查看或修改IAM用户信息进行操作。

  管理员进入安全设置后，在“安全设置 > 敏感操作>自主管理用户属性 > ”中，单击“立即修改”。在“自主管理用户属性设置”弹窗中，选择“关闭”，单击“确定”，关闭IAM用户自主管理用户属性。

3.7.4 登录验证策略

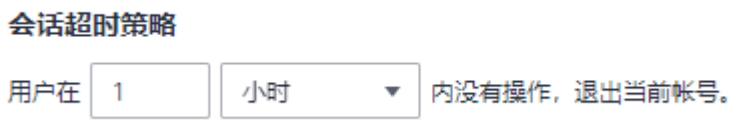
进入安全设置后，选择“登录验证策略”页签，可以对会话超时策略、账号锁定策略、账号停用策略、最近登录提示、登录验证提示进行修改，登录验证策略对账号和账号中的IAM用户生效。

只有管理员可以设置登录验证策略，普通IAM用户只有查看权限，不能对其进行设置，如需修改，请联系管理员为您操作或添加权限。

会话超时策略

如果用户超过设置的时长未操作界面，会话将会失效，需要重新登录。

图 3-30 会话超时策略



管理员可以设置会话超时的时长，会话超时时长默认为1个小时，可以在15分钟~24小时之间进行设置。

账号锁定策略

如果在限定时间长度内达到登录失败次数后，用户会被锁定一段时间。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。

图 3-31 账号锁定策略

管理员可以设置限定时间长度、限定时间内登录失败次数、账号锁定时长。

- 限定时间长度（分钟）：默认为15分钟，可以在15~60分钟之间进行设置。
- 限定时间内登录失败次数：默认为5次，可以在3~10次之间进行设置。
- 账号锁定时长（分钟）：默认为15分钟，可以在15~30分钟之间进行设置。

账号停用策略

如果IAM用户在设置的有效期内没有通过界面控制台或者API访问云服务平台，再次登录时将会被停用。

账号停用策略默认关闭，管理员可以选择开启，并在1~240天之间进行设置。

该策略仅对账号下的IAM用户生效，对账号本身不生效。IAM用户被停用后，可以联系管理员重新启用。

最近登录提示

如果开启最近登录提示，用户登录成功后，将在“登录验证”页面中看到上次登录成功时间，最近登录提示可以帮助用户查看是否存在异常登录信息，如果存在不是本人的登录信息，建议立即修改密码。

最近登录提示默认关闭，管理员可以选择开启。

登录验证提示

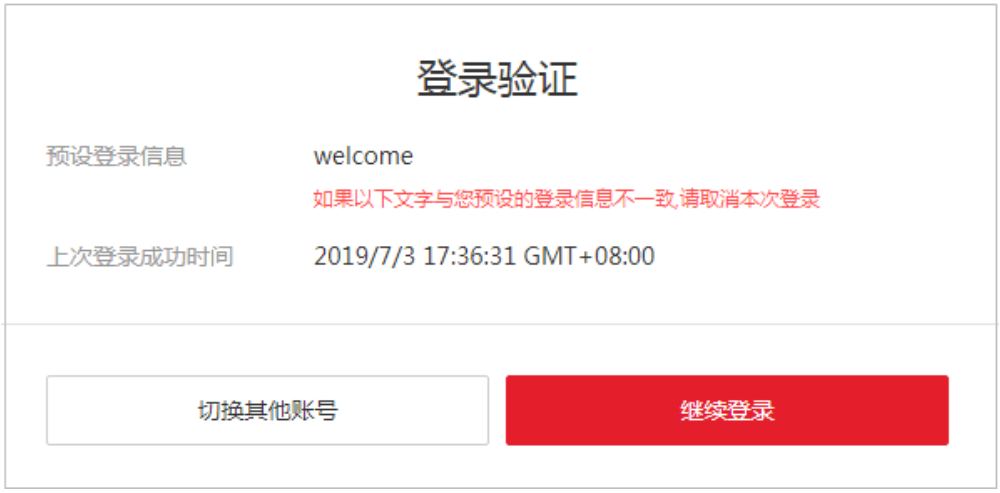
管理员可以在最近登录提示中进行公告，例如欢迎语，或者提示用户谨慎删除资源等。

登录验证提示默认关闭，管理员可以选择开启。

图 3-32 登录验证提示

开启后，用户将在“登录验证”页面中看到公告信息。

图 3-33 登录验证



3.7.5 密码策略

进入安全设置后，选择“密码策略”页签，可以对**密码设置策略**、**密码有效期策略**、**密码最短使用时间策略**进行修改。

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。

建议IAM管理员设置密码策略，例如密码最小长度、密码中同一字符连续出现的最大次数、密码不能与历史密码相同，保证用户在修改密码时，新密码都是满足密码策略的复杂程度高的强密码。

密码设置策略

- 密码至少包含字符种类（大写字母、小写字母、数字、特殊字符）默认为2种，可以在2~4种之间设置。
- 密码最小长度默认为6个字符，可以在6~32个字符之间设置。
- （可选）开启“设置密码时同一字符不能连续出现”，设置密码中允许同一字符连续出现的最大次数。例如设置为1，表示密码中不允许出现相同字符。
- （可选）开启“新密码不能与最近的历史密码相同”，设置新密码不能与最近几次的历史密码相同。例如设置为3，表示不能使用最近三次的历史密码，用户在设置新密码时，如果新密码与历史密码相同，系统将会提示用户不能使用最近三次的历史密码，需要重新设置密码。

修改密码设置策略，将对后续新增IAM用户和后续修改密码的账号以及账号下的IAM用户生效。

密码有效期策略

用户在设置的时间内必须修改密码，否则密码将会失效，无法登录云服务平台，IAM会在密码到期前15天开始提示用户修改密码。密码有效期策略可以强制用户修改密码，提高账号安全性。

密码有效期策略默认关闭，管理员可以选择开启，在1~180天之间进行设置。

修改密码有效期策略，将对账号以及账号下的IAM用户立即生效。

说明

密码过期后，请通过邮箱链接设置新密码，新密码不允许与旧密码相同。

密码最短使用时间策略

当用户密码修改后，再次修改密码时需要满足该策略设置的时间后才能修改。密码最短使用时间策略可以防止用户频繁修改密码，导致忘记密码。

密码最短使用时间策略默认关闭，管理员可以选择开启，在0~1440分钟之间进行设置。

修改密码最短使用时间策略，将对账号以及账号下的IAM用户立即生效。

3.7.6 访问控制

进入安全设置后，选择“访问控制”页签，可以对**允许访问的IP地址区间**、**允许访问的IP地址或网段**、**允许访问的VPC Endpoint**进行修改。

管理员可以设置访问控制策略，限制用户只能从特定IP地址区间、网段及VPC Endpoint访问云服务平台。普通IAM用户没有权限查看此页面，如需使用，请联系管理员为您操作或添加权限。

访问控制生效条件：

- 控制台访问（推荐）：仅对账号下的IAM用户登录控制台生效，对账号本身不生效。
- API访问：仅对账号下的IAM用户通过API网关访问API接口生效，修改后2小时生效。

说明

- 访问控制策略最多可设置200条。

允许访问的 IP 地址区间

图 3-34 允许访问的 IP 地址区间

限制用户只能从设定范围内的IP地址访问云服务平台，可以在0.0.0.0~255.255.255.255之间设置。默认值为0.0.0.0~255.255.255.255。如不设置或设置为默认值意味着您的IAM用户可以从任意地方访问云服务平台。

允许访问的 IP 地址或网段

限制用户只能从设定的IP地址或网段访问云服务平台，例如：10.10.10.10/32。

允许访问的 VPC Endpoint

仅在“API访问”页签中可进行配置。限制用户只能从具有设定ID的VPC Endpoint访问云服务平台API，例如：0ccad098-b8f4-495a-9b10-613e2a5exxxx。若未进行访问控制配置，则默认用户从所有VPC Endpoint都能访问API。

说明

- “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。
- 单击“恢复默认值”，可以将“允许访问的IP地址区间”恢复为默认值，即0.0.0.0~255.255.255.255，同时将“允许访问的IP地址区间或网段”、“允许访问的VPC Endpoint ”清空。

3.8 身份提供商

3.8.1 身份提供商概述

IAM支持基于SAML协议的单点登录，如果您已经有自己的企业管理系统，同时您的用户需要使用您账号内的云服务资源，您可以使用IAM的身份提供商功能，实现用户使用企业管理系统账号单点登录云服务平台，这一过程称之为联邦身份认证。

目前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云服务平台。
- 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调用方式访问云服务平台。

基本概念

表 3-15 基本概念

概念	说明
身份提供商（Identity Provider，简称IdP）	负责收集、存储用户身份信息，如用户名、密码等，在用户登录时负责认证用户的服务。在企业与云服务平台联邦身份认证的过程中，身份提供商指企业自身的身份提供商，目前常用的第三方IdP有Microsoft Active Directory（AD FS）、Shibboleth。
服务提供商（Service Provider，简称SP）	服务提供商通过与身份提供商IdP建立信任关系，使用IdP提供的用户信息，为用户提供具体的服务。在企业与云服务平台联邦身份认证的过程中，服务提供商指云服务平台。
联邦身份认证	身份提供商IdP与服务提供商SP建立信任关系并完成交互流程，实现用户单点登录的过程，称之为联邦身份认证。

概念	说明
单点登录（Single Sign-On，简称SSO）	用户在身份提供商IdP系统登录后，就可以通过跳转链接访问已建立互信关系的服务提供商SP系统，这一过程称之为单点登录。如：企业管理系统与云服务平台建立互信关系后，企业管理系统中的用户通过云服务平台提供的登录入口，使用已有的账号密码在企业管理系统中登录后，即可跳转访问云服务平台。
SAML 2.0	安全断言标记语言（Secturity Assertion Markup Language 2.0，缩写为SAML 2.0）是一个由一组协议组成，用来传输安全声明的XML框架。SAML2.0是由标准化组织OASIS提出的用于安全操作的标准，是很多身份提供商（IdP）使用的一种开放标准，关于SAML2.0的详细描述请参见：**SAML 2.0技术概述**。IAM支持使用SAML2.0协议进行联邦身份认证，因此与云服务平台建立联邦身份认证的企业IdP必须支持SAML2.0协议。

使用联邦身份认证的优势

- 管理用户简单

  使用联邦身份认证前，管理员需要在企业管理系统和云服务平台上分别为用户创建账号。

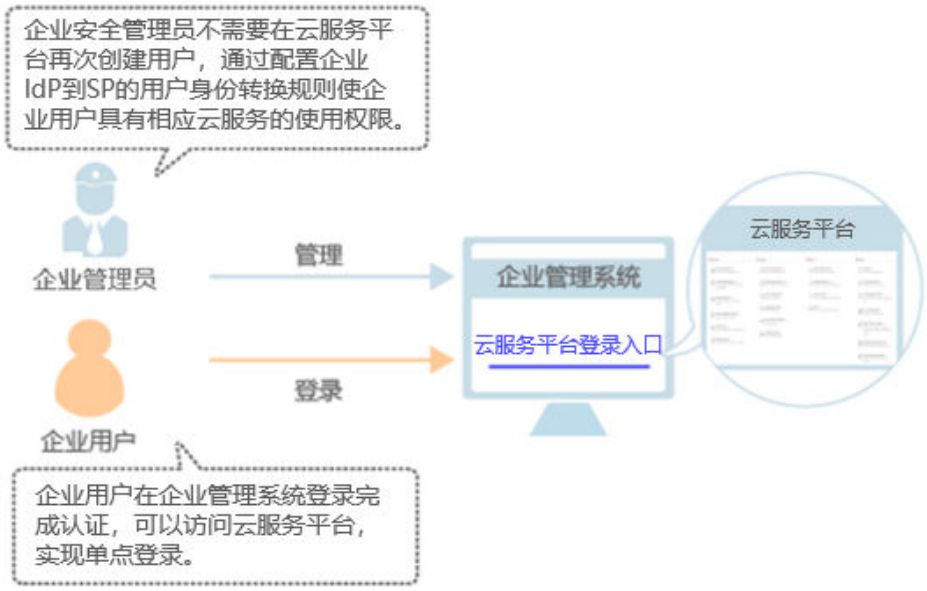
  使用联邦身份认证后，企业管理员只需要在企业管理系统中为用户创建账号，用户即可同时访问两个系统，降低了人员管理成本。

- 用户操作方便

  使用联邦身份认证前，用户访问企业管理系统和云服务平台时需要使用两个系统的账号登录。

  使用联邦身份认证后，用户在本企业管理系统中登录即可访问两个系统。

图 3-35 使用联邦身份认证的优势



注意事项

- 企业IdP服务器的时间需要和云服务平台的时间、时区一致，即都使用GMT时间（Greenwich Mean Time），否则会导致联邦身份认证失败。
- 由于联邦用户的身份信息（如邮件地址、手机号码）保存在企业IdP中，是企业IdP映射到云服务平台的虚拟用户，因此，联邦用户通过身份提供商功能访问云服务平台时有以下约束：
  - 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。
  - 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）。

    如需使用永久AK/SK，只能由账号或是实体IAM用户创建密钥，共享给联邦用户。由于密钥表示用户所拥有的权限，因此建议由与联邦用户同在一个用户组的实体IAM用户创建并分享密钥。

3.8.2 基于 SAML 协议的联邦身份认证

3.8.2.1 联邦身份认证配置概述

本章为您介绍基于SAML协议的企业IdP与本系统进行联邦身份认证的内部实现流程和配置步骤。

注意

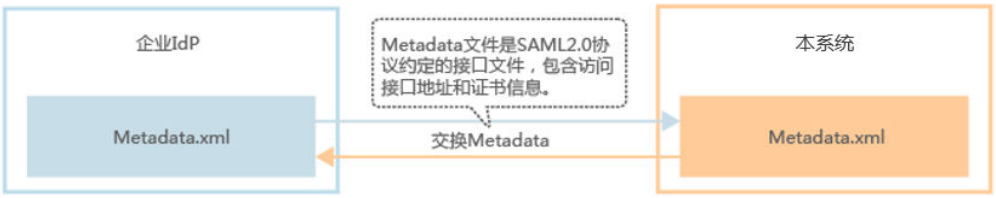
请确保您使用的IdP支持SAML 2.0协议。

联邦身份认证的配置步骤

建立企业管理系统与本系统的联邦身份认证关系，需要完成以下配置步骤。

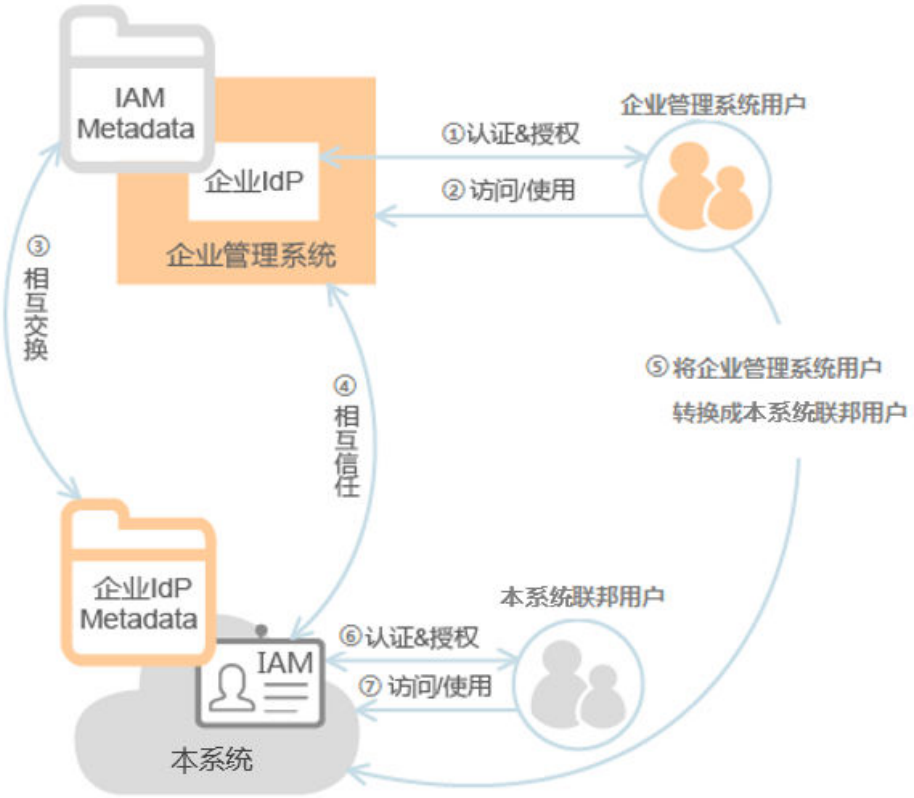
1. **建立互信关系并创建身份提供商**：交换本系统与企业IdP的元数据文件，建立信任关系，并在系统上创建身份提供商。

   图 3-36 交换 Metadata 文件模型

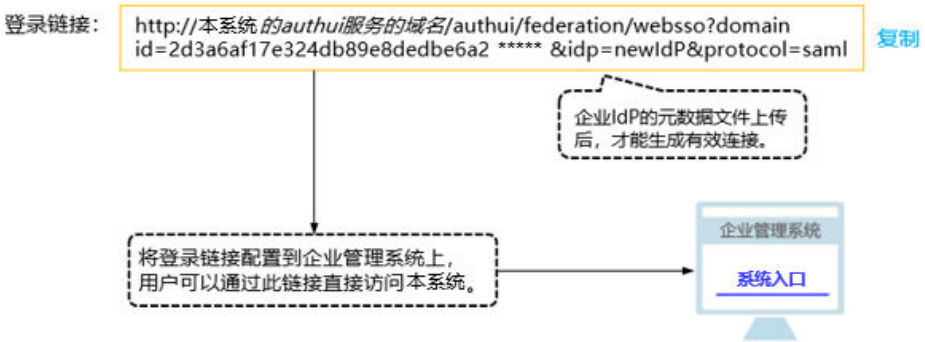
2. **在本系统配置身份转换规则**：通过配置身份转换规则，将IdP中的用户、用户组及其访问权限映射到系统，用户转换模型如**图 用户转换模型**所示。

图 3-37 用户转换模型



3. **配置企业管理系统登录入口**：将系统的访问入口配置到企业管理系统中，用户可通过登录企业管理系统直接访问本系统。

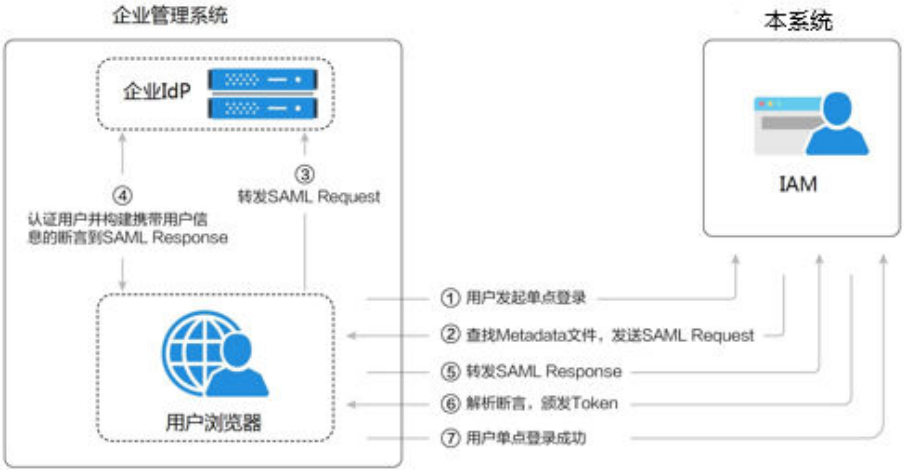
图 3-38 配置单点登录模型



企业身份管理与本系统联邦身份认证交互流程

图 联邦身份认证交互流程为用户在发起单点登录请求后，企业身份管理与本系统间的交互流程。

图 3-39 联邦身份认证交互流程



说明

为方便您查看交互的请求及断言消息，建议您使用Chrome浏览器并安装插件“SAML Message Decoder”。

从上图中可知，联邦身份认证的步骤为：

1. 用户在浏览器中打开创建身份提供商后生成的登录链接，浏览器向系统发起单点登录请求。
2. 系统根据登录链接中携带的信息，查找IAM身份提供商中对应的Metadata文件，构建SAML Request，发送给浏览器。
3. 浏览器收到请求后，转发SAML Request给企业IdP。
4. 用户在企业IdP推送的登录页面中输入用户名和密码，企业IdP对用户提供的身份信息进行验证，并构建携带用户信息的SAML断言，向浏览器发送SAML Response。
5. 浏览器响应后转发SAML Response给系统。
6. 系统从SAML Response中取出断言，并根据已配置的身份转换规则映射到具体的IAM用户组，颁发Token。
7. 用户完成单点登录，访问系统。

说明

断言中要携带签名，否则会导致登录失败。

3.8.2.2 步骤 1：创建身份提供商

配置联邦身份认证，需要在企业IdP上传本系统的元数据文件（Metadata文件），并在IAM控制台上创建身份提供商、上传企业IdP的元数据文件，来建立两个系统之间的互信关系。

前提条件

- 企业管理员在云服务平台上注册了可用的账号，并已在IAM中创建用户组并授权，具体方法请参见：**创建用户组并授权**。在IAM上创建的用户组是用于与企业IdP上的用户建立映射关系，使得IdP中的用户获取IAM中用户组的权限。

- 企业管理员已获取企业IdP的帮助文档或了解企业IdP使用方法。由于不同的企业IdP的配置存在较大差异，云服务平台帮助文档对于企业IdP的配置不做详述，获取企业IdP的元数据文件、云服务平台元数据上传至企业IdP等具体操作请参考企业IdP的帮助文档。

建立企业 IdP 对本系统的信任关系

在IdP中配置系统的元数据文件，以建立IdP对系统的信任。

步骤1 下载系统的元数据文件（metadata文件）。

- WebSSO：访问网址“https://系统的authui服务的域名/authui/saml/metadata.xml”，单击右键，选择“目标另存为”并设置文件名称，例如websso-metadata.xml。
- API接口调用：访问网址“https://*区域的终点节点地址*/v3-ext/auth/OS-FEDERATION/SSO/metadata”，单击右键，选择“目标另存为”并设置文件名称，例如api-metadata-region.xml。

  本系统在不同的区域提供不同的API网关供用户调用API接口，如果用户需要访问多个区域，需要下载多个区域的元数据文件。

步骤2 将上述文件上传到企业IdP服务器上，上传方法请参见IdP提供商的帮助文档。

步骤3 获取企业IdP的元数据文件。获取方法请参见IdP提供商的帮助文档。

----结束

在系统上创建身份提供商

在IAM控制台上创建身份提供商，配置身份提供商的元数据文件后，可以在IAM中建立对IdP的信任关系，使得企业用户可以直接访问本系统。

步骤1 进入IAM控制台，在左侧导航窗格中，选择“身份提供商”页签，单击右上方的“创建身份提供商”。

步骤2 在“创建身份提供商”窗口中设置名称、协议、类型、状态、描述。

表 3-16 身份提供商基本参数

参数	含义
名称	身份提供商的名称。身份提供商名称不能重复，建议以域名唯一标识命名。
协议	身份提供商协议。当前本系统支持基于SAML、OIDC的身份提供商，如需创建基于OIDC协议的联邦身份认证，请参考**基于OIDC协议的联邦身份认证**。

参数	含义
类型	身份提供商类型。一个账号下只能存在一种类型的身份提供商。 • 虚拟用户SSO：该身份提供商中的用户登录G42云后，系统为其自动创建虚拟用户信息。一个账号可以创建多个虚拟用户SSO类型的身份提供商。 • IAM用户SSO：该身份提供商中的用户登录G42云后，系统将自动匹配外部身份ID绑定的对应IAM子用户，从而拥有该子用户所在用户组的权限。一个账号下只能创建一个IAM用户SSO类型的身份提供商。如果选择该类型，请确保您已为用户创建对应的IAM用户并设置外部身份ID，请参考**创建IAM用户**。
状态	身份提供商的状态。默认设置为“启用”。

步骤3 单击“确定”，创建身份提供商成功。

----结束

在系统上配置元数据文件

配置元数据文件，即把**步骤3**获取到的企业IdP的元数据文件配置到系统。IAM支持“上传文件”和“手动编辑”两种配置，选择其中一种即可。如果元数据文件超过500KB，请通过“手动编辑”配置元数据。如果后续元数据有更新，需要用户重新上传或者编辑元数据，否则会影响联邦用户登录本系统。

- **上传元数据**：
  a. 单击身份提供商列表中“操作”列的“修改”。
  b. 单击“上传文件”左侧的“添加文件”，选择获取的企业IdP的元数据文件。

  图 3-40 上传元数据文件

  c. 单击“上传文件”。弹出页面显示系统提取到的元数据，单击“确定”。
     - 提示“系统发现您上传的文件中包含多个身份提供商，请选择您本次需要使用的身份提供商”，请在“Entity ID”下拉框中选择您本次需要使用的身份提供商。
     - 提示元数据文件中Entity ID为空、签名证书过期等内容时，需要您确认元数据文件的正确性后，重新上传或者通过手动编辑提取元数据。
  d. 单击“确定”。
- **手动编辑元数据**
  a. 单击“手动编辑”。
  b. 在“手动编辑元数据”页面中，输入从企业IdP元数据文件中获取的“Entity ID”、“签名证书”和“SingleSignOnService”等参数。

参数	是否必选	含义
Entity ID	是	对应IdP元数据文件中“entityID”的值。 企业身份提供商的唯一标识，元数据文件中可能包含多个身份提供商，需要选择对应的身份提供商。
支持的协议	是	企业IdP与服务提供商之间，通过SAML协议完成联邦身份认证。
支持的NameIdFormat	否	对应IdP元数据文件中“NameIdFormat”的值。 身份提供商支持的用户名称标识格式。名称标识是身份提供商与联邦用户之间实现通信的一种方式。
签名证书	是	对应IdP元数据文件中“<X509Certificate>”的值。 签名证书是一份包含公钥用于验证签名的证书，为了确保安全性，建议使用长度大于等于2048位的公钥。IAM通过元数据文件中的签名证书来确认联邦身份认证过程中断言消息的可信性、完整性。
SingleSignOnService	是	对应IdP元数据文件中“SingleSignOnService” 的值。 单点登录过程中发送SAML请求的方式。元数据文件中的“SingleSignOnService”需要支持HTTP Redirect或HTTP POST方式。
SingleLogoutService	否	对应IdP元数据文件中“SingleLogoutService” 的值。 服务提供商提供会话注销功能，联邦用户在IAM注销会话后返回绑定的地址。“SingleLogoutService” 需要支持HTTP Redirect或HTTP POST方式。

示例：以下为某企业IdP的元数据文件和手动编辑元数据信息时需要填入的内容。

图 3-41 某企业 IdP 的元数据文件

c. 单击“确定”。

- 单击“确定”，保存设置信息。

联邦用户登录验证

步骤1 检查登录链接是否可以跳转到企业的IdP服务器提供的登录界面。

1. 在IAM控制台的“身份提供商”页面，单击“操作”列的“查看”，进入“身份提供商基本信息”页面；单击“登录链接”右侧的“复制”，并在浏览器中打开。
2. 检查浏览器页面是否跳转到IdP登录界面，如果跳转失败，请确认获取的企业元数据文件以及企业IdP服务器配置是否正确。

步骤2 输入企业管理系统的用户名和密码验证是否可以登录到系统。

- 登录成功：表示单点登录验证成功，您可以将该地址以链接的形式配置到企业网站。
- 登录失败：请检查您的用户名和密码。

说明

此时联邦用户只能访问系统，没有任何权限。为联邦用户配置权限需要配置身份转换规则，具体说明请参见：**步骤2：配置身份转换规则**。

----结束

相关操作

- 查看身份提供商信息：在身份提供商列表中，单击“查看”，可查看身份提供商的基本信息、元数据详情、身份转换规则。

  说明

  单击“查看身份提供商”页面下方的“修改身份提供商”，可直接进入“修改身份提供商”界面。
- 修改身份提供商信息：在身份提供商列表中，单击“修改”进入“修改身份提供商”界面。可修改身份提供商的状态（“启用”或“停用”）、描述信息、元数据信息和身份转换规则。
- 删除身份提供商：在身份提供商列表中，单击“删除”，删除对应的身份提供商。

后续任务

- 在“身份转换规则”区域，配置身份转换规则，建立IdP中的用户与IAM中用户组间的映射关系，使得IdP用户获得用户组对应的系统操作权限。身份转换规则详情请参见：**步骤2：配置身份转换规则**。
- 在企业管理系统中配置单点登录，使企业用户可以通过企业管理系统中的系统登录入口直接访问本系统，方法请参考：**步骤3：配置企业管理系统登录入口**。

3.8.2.3 步骤 2：配置身份转换规则

在IAM上创建身份提供商后，联邦用户在系统中的用户名默认为“FederationUser”，且联邦用户仅能访问系统，没有任何权限。您可以在IAM控制台配置身份转换规则，实现：

- 企业管理系统用户在系统中显示不同的用户名。
- 赋予企业管理系统用户使用资源的权限。由于权限的最小授权单位是用户组，因此需要建立联邦用户与IAM用户组的映射关系，从而使得联邦用户获得对应用户组的权限，使用系统中的资源。请确保已创建需要映射的IAM用户组，创建IAM用户组并授权请参见：**创建用户组并授权**。

说明

- 修改身份转换规则后，对已登录的联邦用户不会即时生效，需重新登录后新规则才可生效。
- 如果需要修改用户的权限，修改用户所属用户组的权限即可，修改后，需要重启企业IdP系统使设置生效。

前提条件

已在本系统创建身份提供商，并验证身份提供商的登录链接可以正常使用，如何创建并验证身份提供商请参见：**步骤1：创建身份提供商**。

操作步骤

您可以使用“创建规则”，IAM会将您填写的身份转换规则参数转换成JSON语言；也可以单击“编辑规则”直接编写JSON语言，编辑身份转换规则的详细说明和示例请参见：**身份转换规则详细说明**。

- **创建规则**
  a. 管理员在统一身份认证服务的左侧导航窗格中，单击“身份提供商”。
  b. 在身份提供商列表中，选择您创建的身份提供商，单击“修改”。
  c. 在“身份转换规则”区域单击“创建规则”。

表 3-17 参数说明

参数名	描述	说明
用户名	联邦用户在系统中显示的用户名，以下简称“联邦用户名”。	为了区分系统的用户与联邦用户，建议此处配置用户名为“FederationUser-IdP_XXX”。其中“IdP”为身份提供商名称，如ADFS、Shibboleth等，用于区分不同身份提供商下的联邦用户；“XXX”为自定义的具体名称。 **须知** • 同一身份提供商的联邦用户名需要确保其唯一。如果同一身份提供商内出现重复的联邦用户名，则重名的联邦用户在本系统中对应同一个IAM用户。 • 用户名能包含大小写字母、空格、数字或特殊字符（-_.）且不能以数字开头。不能包含”、\"、\\、\n、\r等特殊字符。
用户组	联邦用户在系统中所属的用户组。	联邦用户拥有所属用户组的权限。 **说明** 用户组名能包含大小写字母、空格、数字或特殊字符（-_.）且不能以数字开头。不能包含”、\"、\\、\n、\r等特殊字符。

参数名	描述	说明
本规则生效条件	联邦用户拥有所选用户组权限的生效条件。	当满足该生效条件时，联邦用户具有所属用户组的权限；当不满足生效条件时，该规则不生效，且不满足生效条件的用户无法访问系统。一个身份转换规则最多可以创建10条生效条件。 “属性”、“值”为企业IdP通过SAML断言返回给系统用户信息；“条件”可选择：empty、any_one_of、not_any_of，详细说明请参见：**身份转换规则详细说明**。 **说明** • 一个规则可以创建多条生效条件，所有生效条件均满足，此规则才可以生效。 • 一个身份提供商可以创建多条规则，规则共同作用。如果所有规则对某个联邦用户都不生效，那么该联邦用户禁止访问本系统。

示例：为企业管理系统管理员设定规则。

- 用户名：FederationUser-IdP_admin
- 用户组：“admin”
- 生效条件：“属性”：“_NAMEID_”；“条件”：“any_one_of”；“值”：“000000001”。

  表示仅用户ID为000000001的用户在云服务平台上映射的IAM用户名为FederationUser-IdP_admin、具有“admin”用户组的权限。

d. 在“创建规则”页面，单击“确定”。

e. 在“修改身份提供商”页面，单击“确定”，使配置生效。

- **编辑规则**

a. 管理员登录云服务平台，进入IAM控制台，并在左侧导航窗格中，单击“身份提供商”。

b. 在身份提供商列表中，选择您创建的身份提供商，单击“修改”。

c. 在“身份转换规则”区域单击“编辑规则”。

d. 在编辑框内输入JSON格式的身份转换规则，具体说明请参见：**身份转换规则详细说明**。

e. 单击“校验规则”，对已编辑的规则进行语法校验。

f. 界面提示“规则正确”：在“编辑规则”页面，单击“确定”；在“修改身份提供商”页面，单击“确定”，使配置生效。

界面提示“JSON文件格式不完整”：请修改JSON语句，或单击“取消”，取消本次修改内容。

验证联邦用户权限

配置身份转换规则后，查看联邦用户是否已有相应权限。

步骤1 联邦用户登录。

在IAM控制台的“身份提供商”页面，单击“操作”列的“查看”，进入“身份提供商基本信息”页面；单击“登录链接”右侧的“复制”，在浏览器中打开，输入企业管理系统用户名和密码，登录成功。

步骤2 查看联邦用户是否具有所属用户组的权限。

例如，配置身份转换规则时，使联邦用户“ID1”对应IAM用户组“admin”，拥有所有云服务的权限。进入控制台，选择任一云服务，查看是否可以访问此服务。

----结束

相关操作

查看规则：在“身份转换规则”区域单击“查看规则”。新创建的身份转换规则在JSON文件中显示。JSON文件内容说明请参考：**身份转换规则详细说明**。

3.8.2.4 （可选）步骤 3：配置企业管理系统登录入口

将身份提供商的登录链接配置到企业管理系统上，企业用户通过该链接访问系统。

前提条件

- 已创建身份提供商，并验证身份提供商的登录链接可以正常使用，如何创建并验证身份提供商请参见：**步骤1：创建身份提供商**。
- 企业管理系统界面已创建本系统登录入口。

操作步骤

步骤1 在IAM控制台的左侧导航窗格中，单击“身份提供商”。

步骤2 单击目标身份提供商列表右侧的“查看”。

步骤3 单击“登录链接”右侧的“复制”。

步骤4 将以下语句添加在企业管理系统页面文件中。

```
<a href="<登录链接>"> 系统入口 </a>
```

步骤5 用户登录企业管理系统后通过单击“系统入口”可以直接访问本系统。

----结束

3.8.3 基于 OIDC 协议的联邦身份认证

3.8.3.1 联邦身份认证配置概述

本章为您介绍基于OIDC协议的企业IdP与本系统进行联邦身份认证的内部实现流程和配置步骤。

联邦身份认证的配置步骤

建立企业管理系统与本系统的联邦身份认证关系，需要完成以下配置步骤。

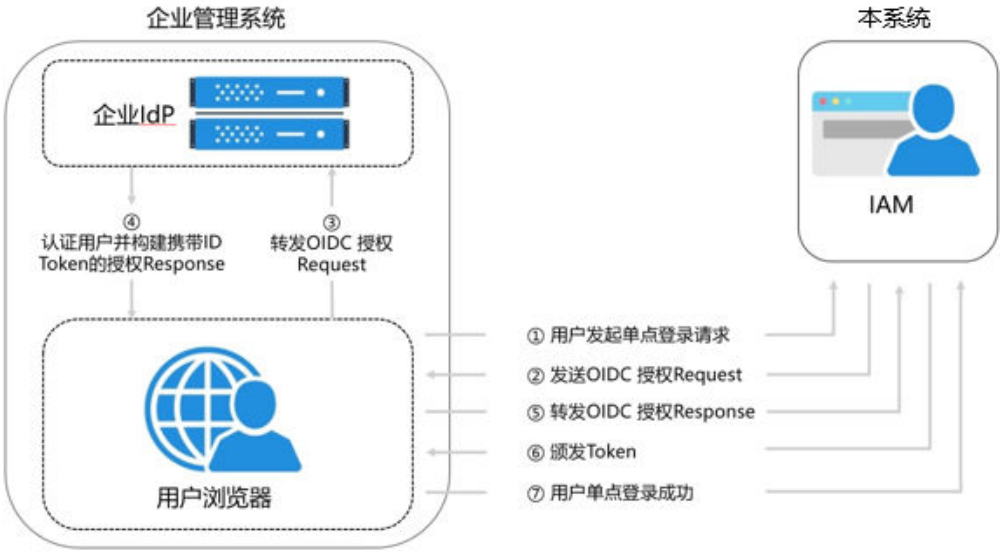
1. **创建身份提供商并创建互信关系**：在企业IdP中创建OAuth 2.0凭据，在本系统上创建身份提供商并配置授权信息，从而建立企业IdP和本系统的信任关系。

2. **配置身份转换规则**：通过在本系统配置身份转换规则，将IdP中的用户、用户组及其访问权限映射到本系统。
3. **配置企业管理系统登录入口**：将本系统的访问入口配置到企业管理系统中，用户可通过登录企业管理系统直接访问本系统。

企业管理系统与本系统联邦身份认证交互流程

图 联邦身份认证交互流程为用户在发起单点登录请求后，企业管理系统与本系统间的交互流程。

图 3-42 联邦身份认证交互流程



从上图中可知，联邦身份认证的步骤为：

1. 用户在浏览器中打开从IAM上获取到的登录链接，浏览器向本系统发起单点登录请求。
2. 本系统根据登录链接中携带的信息，查找IAM身份提供商中对应的配置信息，构建OIDC 授权Request，发送给浏览器。
3. 浏览器收到请求后，转发OIDC授权Request给企业IdP。
4. 用户在企业IdP推送的登录页面中输入用户名和密码，企业IdP对用户提供的身份信息进行验证，并构建携带用户信息的ID Token，向浏览器发送OIDC授权Response。
5. 浏览器响应后转发OIDC授权Response给本系统。
6. 本系统从OIDC授权Response中取出ID Token，并根据已配置的身份转换规则映射到具体的IAM用户组，颁发Token。
7. 用户完成单点登录，访问本系统。

3.8.3.2 步骤 1：创建身份提供商

配置联邦身份认证，需要在企业IdP通过浏览器将用户重定向到OIDC身份提供商并创建OAuth 2.0凭据，在IAM控制台上创建身份提供商、配置授权信息，来建立两个系统之间的互信关系。

前提条件

- 企业管理员在云服务平台上注册了可用的账号，并已在IAM中创建用户组并授权，具体方法请参见：**创建用户组并授权**。在IAM上创建的用户组是用于与企业IdP上的用户建立映射关系，使得IdP中的用户获取IAM中用户组的权限。
- 企业管理员已获取企业IdP的帮助文档或了解企业IdP使用方法。由于不同的企业IdP的配置存在较大差异，云服务平台帮助文档对于企业IdP的配置不做详述，获取企业IdP的OAuth 2.0凭据等具体操作请参考企业IdP的帮助文档。

在企业 IdP 中创建 OAuth 2.0 凭据

步骤1 企业IdP通过浏览器将用户重定向到本系统OIDC身份提供商。

步骤2 获取企业IdP的OAuth 2.0凭据。

说明

由于不同的企业IdP的配置存在较大差异，本章中对于企业IdP的配置不做详述，具体操作请参考IdP提供商的帮助文档。

----结束

在本系统中创建身份提供商

在IAM控制台上创建身份提供商，通过配置授权信息，可以在IAM中建立对IdP的信任关系，使得企业用户可以直接访问本系统。

步骤1 进入IAM控制台，在左侧导航窗格中，选择“身份提供商”页签，单击右上方的“创建身份提供商”。

图 3-43 创建身份提供商

步骤2 在弹出的“创建身份提供商”窗口中填写“名称”，选择“协议”为“OpenID Connect”，选择“状态”为“启用”，单击“确定”，创建身份提供商成功。

说明

身份提供商名称不能重复，建议以域名唯一标识命名。

----结束

在本系统中配置授权信息

步骤1 单击身份提供商列表中“操作”列的“修改”，进入“修改身份提供商”页面。

步骤2 在修改身份提供商页面，选择“访问方式”。

表 3-18 访问方式

访问方式	说明
编程访问和管理控制台访问	• 编程访问：可以使用支持访问密钥认证的API、CLI、SDK等开发工具来访问本系统。 • 管理控制台访问：用户可以使用账号密码登录到管理控制台来访问本系统。 **如果您需要使用SSO方式访问本系统，应该选择此方式。**
编程访问	用户仅可以使用支持访问密钥认证的API、CLI、SDK等开发工具来访问本系统。

步骤3 在修改身份提供商页面，填写“配置信息”。

表 3-19 配置信息

配置信息	说明
身份提供商URL	OpenID Connect身份提供商标识。 对应企业IdP提供的Openid-configuration中"issuer"字段的值。 **说明** Openid-configuration是在OpenID Connect中定义的URL，它提供了有关身份提供程序（IdP）的配置信息。URL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.
客户端ID	在OpenID Connect身份提供商注册的客户端ID。即**在企业IdP中创建的OAuth 2.0凭据**。
授权请求Endpoint	OpenID Connect身份提供商授权地址。对应企业IdP提供的Openid-configuration中"authorization_endpoint"字段的值。 **仅访问方式为“编程访问和管理控制台访问”时需要填写。**
授权请求Scope	授权请求信息范围。默认必选openid。 **仅访问方式为“编程访问和管理控制台访问”时需要填写。** 枚举值： • openid • email • profile
授权请求Response type	授权请求返回参数类型，默认必选id_token。 **仅访问方式为“编程访问和管理控制台访问”时需要填写。**
授权请求Response mode	授权请求返回模式，form_post和fragment两种可选模式，推荐选择form_post模式。 **仅访问方式为“编程访问和管理控制台访问”时需要填写。**

配置信息	说明
签名公钥	验证OpenID Connect身份提供商ID Token签名的公钥。为了您的账号安全，建议您**定期轮换**签名公钥。

步骤4 单击“确定”，完成配置。

----结束

联邦用户登录验证

步骤1 检查登录链接是否可以跳转到企业的IdP服务器提供的登录界面。

1. 在IAM控制台的“身份提供商”页面，单击“操作”列的“修改”，进入“修改身份提供商”页面。
2. 在修改身份提供商页面，单击登录链接右侧的“复制”，并在浏览器中打开。
3. 检查浏览器页面是否跳转到IdP登录界面，如果跳转失败，请确认身份提供商配置信息以及企业IdP服务器配置是否正确。

步骤2 输入企业管理系统的用户名和密码验证是否可以登录到本系统。

- 登录成功：表示单点登录验证成功，您可以将该地址以链接的形式配置到企业网站。
- 登录失败：请检查您的用户名和密码。

说明

此时联邦用户只能访问系统，没有任何权限。为联邦用户配置权限需要配置身份转换规则，具体说明请参见：**步骤2：配置身份转换规则**。

----结束

相关操作

- 查看身份提供商信息：在身份提供商列表中，单击“查看”，可查看身份提供商的基本信息、元数据详情、身份转换规则。

  说明

  单击“查看身份提供商”页面下方的“修改身份提供商”，可直接进入“修改身份提供商”界面。
- 修改身份提供商信息：在身份提供商列表中，单击“修改”进入“修改身份提供商”界面。可修改身份提供商的状态（“启用”或“停用”）、描述信息、元数据信息和身份转换规则。
- 删除身份提供商：在身份提供商列表中，单击“删除”，删除对应的身份提供商。

后续任务

- 配置身份转换规则，建立IdP中的用户与IAM中用户组间的映射关系，使得IdP用户获得用户组对应的操作权限。身份转换规则详情请参见：**步骤2：配置身份转换规则**。
- 在企业管理系统中配置单点登录，使企业用户可以通过企业管理系统中的登录入口直接访问本系统，方法请参考：**步骤3：配置企业管理系统登录入口**。

3.8.3.3 步骤 2：配置身份转换规则

在IAM上创建身份提供商后，联邦用户在系统中的用户名默认为“FederationUser”，且联邦用户仅能访问系统，没有任何权限。您可以在IAM控制台配置身份转换规则，实现：

- 企业管理系统用户在本系统中显示不同的用户名。
- 赋予企业管理系统用户使用云资源的权限。由于权限的最小授权单位是用户组，因此需要建立联邦用户与IAM用户组的映射关系，从而使得联邦用户获得对应用户组的权限，使用系统中的资源。请确保已创建需要映射的IAM用户组，创建IAM用户组并授权请参见：**创建用户组并授权**。

说明

- 修改身份转换规则后，对已登录的联邦用户不会即时生效，需重新登录后新规则才可生效。
- 如果需要修改用户的权限，修改用户所属用户组的权限即可，修改后，需要重启企业IdP使设置生效。

前提条件

已在本系统创建身份提供商，并验证身份提供商的登录链接可以正常使用，如何创建并验证身份提供商请参见：**步骤1：创建身份提供商**。

操作步骤

您可以使用“创建规则”，IAM会将您填写的身份转换规则参数转换成JSON语言；也可以单击“编辑规则”直接编写JSON语言，编辑身份转换规则的详细说明和示例请参见：**身份转换规则详细说明**。

- **创建规则**
  a. 管理员在统一身份认证服务的左侧导航窗格中，单击“身份提供商”。
  b. 在身份提供商列表中，选择您创建的身份提供商，单击“修改”。
  c. 在“身份转换规则”区域单击“创建规则”。

表 3-20 参数说明

参数名	描述	说明
用户名	联邦用户在本系统中显示的用户名，以下简称“联邦用户名”。	为了区分本系统的用户与联邦用户，建议此处配置用户名为“FederationUser-IdP_XXX”。其中“IdP”为身份提供商名称，如ADFS、Shibboleth等，用于区分不同身份提供商下的联邦用户；“XXX”为自定义的具体名称。 **须知** • 同一身份提供商的联邦用户名需要确保其唯一。如果同一身份提供商内出现重复的联邦用户名，则重名的联邦用户在本系统中对应同一个IAM用户。 • 用户名能包含大小写字母、空格、数字或特殊字符（-_.）且不能以数字开头。不能包含”、\"、\\、\n、\r等特殊字符。

参数名	描述	说明
用户组	联邦用户在本系统中所属的用户组。	联邦用户拥有所属用户组的权限。 **说明** 用户组名能包含大小写字母、空格、数字或特殊字符（ -_. ）且不能以数字开头。不能包含”、\"、\\、\n、\r等特殊字符。
本规则生效条件	联邦用户拥有所选用户组权限的生效条件。	当满足该生效条件时，联邦用户具有所属用户组的权限；当不满足生效条件时，该规则不生效，且不满足生效条件的用户无法访问本系统。一个身份转换规则最多可以创建10条生效条件。 **说明** • 一个规则可以创建多条生效条件，所有生效条件均满足，此规则才可以生效。 • 一个身份提供商可以创建多条规则，规则共同作用。如果所有规则对某个联邦用户都不生效，那么该联邦用户禁止访问本系统。

示例：为企业管理系统管理员设定规则。

- 用户名：FederationUser-IdP_admin
- 用户组：“admin”
- 生效条件：“属性”：“_NAMEID_”；“条件”：“any_one_of”；“值”：“000000001”。

  表示仅用户ID为000000001的用户在上映射的IAM用户名为FederationUser-IdP_admin、具有“admin”用户组的权限。

d. 在“创建规则”页面，单击“确定”。

e. 在“修改身份提供商”页面，单击“确定”，使配置生效。

- **编辑规则**

a. 管理员登录本系统，进入IAM控制台，并在左侧导航窗格中，单击“身份提供商”。

b. 在身份提供商列表中，选择您创建的身份提供商，单击“修改”。

c. 在“身份转换规则”区域单击“编辑规则”。

d. 在编辑框内输入JSON格式的身份转换规则，具体说明请参见：**身份转换规则详细说明**。

e. 单击“校验规则”，对已编辑的规则进行语法校验。

f. 界面提示“规则正确”：在“编辑规则”页面，单击“确定”；在“修改身份提供商”页面，单击“确定”，使配置生效。

界面提示“JSON文件格式不完整”：请修改JSON语句，或单击“取消”，取消本次修改内容。

验证联邦用户权限

配置身份转换规则后，查看联邦用户是否已有相应权限。

步骤1 联邦用户登录。

在IAM控制台的“身份提供商”页面，单击“操作”列的“查看”，进入“身份提供商基本信息”页面；单击“登录链接”右侧的“复制”，在浏览器中打开，输入企业管理系统用户名和密码，登录成功。

步骤2 查看联邦用户是否具有所属用户组的权限。

例如，配置身份转换规则时，使联邦用户“ID1”对应IAM用户组“admin”，拥有所有云服务的权限。进入控制台，选择任一云服务，查看是否可以访问此服务。

----结束

相关操作

查看规则：在“身份转换规则”区域单击“查看规则”。新创建的身份转换规则在JSON文件中显示。JSON文件内容说明请参考：**身份转换规则详细说明**。

3.8.3.4 （可选）步骤 3：配置企业管理系统登录入口

将身份提供商的登录链接配置到企业管理系统上，企业用户通过该链接访问本系统。

前提条件

- 已创建身份提供商，并验证身份提供商的登录链接可以正常使用，如何创建并验证身份提供商请参见：**步骤1：创建身份提供商**。
- 企业管理系统界面已创建本系统登录入口。

操作步骤

步骤1 在IAM控制台的左侧导航窗格中，单击“身份提供商”。

步骤2 单击目标身份提供商列表右侧的“查看”。

步骤3 单击“登录链接”右侧的“复制”。

步骤4 将以下语句添加在企业管理系统页面文件中。

```
<a href="<登录链接>"> 系统入口 </a>
```

步骤5 用户登录企业管理系统后通过单击“系统入口”可以直接访问本系统。

----结束

3.8.4 身份转换规则详细说明

联邦身份转换规则采用JSON格式呈现。您可以通过编辑JSON文件来修改规则。JSON格式如下：

```
[
    {
        "local": [
            {
                "<user> or <group> or <groups>"
            }
        ],
        "remote": [
            {
                "<condition>"
            }
        ]
```

```
    }
]
```

参数说明：

- local：表示联邦用户映射到IAM中的身份信息。可以是占位符“{0..n}”，{0}表示remote中用户信息的第一个属性，{1}表示remote中用户信息的第二个属性。
- remote：表示联邦用户在IdP中的用户信息，由断言属性及运算符组成的表达式，取值由断言决定。
  - condition：联邦用户映射到IAM时，身份转换规则的生效条件。当前支持三种条件：
    - empty：无限制，即条件一直生效，返回输入属性的值，值可以用于填充local块中的占位符。
    - any_one_of：输入属性值中只要包含一个指定值即生效，并返回布尔值，返回值不能用于local块中的占位符。
    - not_any_of：输入属性值中不包含任何指定值才生效，并返回布尔值，返回值不能用于local块中的占位符。

须知

映射到IAM中的用户身份信息只能包含：大小写字母、空格、数字或特殊字符（ -_. ）且不能以数字开头。

empty 条件示例

empty条件的特点是能够返回一个具体字串值，该值用于填充local块中的占位符“{0..n}”.

- 以下示例表示联邦用户在IAM中的用户名称为“remote”的第一个属性值+空格+第二个属性值，即*FirstName LastName*。所属用户组为“remote”的第三个属性值，即*Group*，*Group*属性的值只能有一个。

```
[
    {
        "local": [
            {
                "user": {
                    "name": "{0} {1}"
                }
            },
            {
                "group": {
                    "name": "{2}"
                }
            }
        ],
        "remote": [
            {
                "type": "FirstName"
            },
            {
                "type": "LastName"
            },
            {
                "type": "Group"
            }
        ]
```

```
    }
]
```

假设传入以下断言，则联邦用户在IAM中的用户名为John Smith，John Smith在IAM中只属于“admin”用户组。（为了方便理解，简化了断言的结构，之后的示例也将做类似的简化，不再重复提示）

```
{FirstName: John}
{LastName: Smith}
{Group: admin}
```

- 如果联邦用户需要在IAM中属于多个用户组，身份转换规则如下所示。

  以下示例表示联邦用户在IAM中的用户名称为“remote”的第一个属性值+空格+第二个属性值，即*FirstName LastName*。所属用户组为“remote”的第三个属性值，即*Groups*。

```
[
    {
        "local": [
            {
                "user": {
                    "name": "{0} {1}"
                }
            },
            {
                "group":   {
                    "name": "{2}"
                }
            }
        ],
        "remote": [
            {
                "type": "FirstName"
            },
            {
                "type": "LastName"
            },
            {
                "type": "Groups"
            }
        ]
    }
]
```

  假设传入以下断言，则联邦用户在系统中的用户名为John Smith，John Smith属于“admin”和“manager”用户组。

```
{FirstName: John}
{LastName: Smith}
{Groups: [admin, manager]}
```

any one of、not any of 条件示例

any one of、not any of与empty条件不同，这两个条件返回的是一个布尔值，该值不能用于填充local中的占位符。所以以下示例中，仅有一个占位符“{0}”用于被remote块中的第一个Empty条件填充，第二个group为一个固定的值admin。

- 以下示例表示联邦用户在IAM中的用户名为“remote”的第一个属性，即*UserName*。所属用户组为“admin”。该规则仅对在IdP中属于“idp_admin”用户组的用户生效。

```
[
    {
        "local": [
            {
                "user": {
                    "name": "{0}"
                }
```

```
            },
            {
               "group": {
                  "name": "admin"
               }
            }
         ],
         "remote": [
            {
            "type": "UserName"
            },
            {
               "type": "Groups",
               "any_one_of": [
                  "idp_admin"
               ]
            }
         ]
      }
]
```

- 如果联邦用户需要在IAM中属于多个用户组，身份转换规则如下所示。

  以下示例表示联邦用户在IAM中的用户名为“remote”的第一个属性，即UserName。所属用户组为“admin”和“manager”。该规则仅对在IdP中属于“idp_admin”用户组的用户生效。

```
[
      {
         "local": [
            {
               "user": {
                  "name": "{0}"
               }
            },
            {
               "group": {
                     "name":"admin"
               }
            },
            {
               "group": {
                     "name":"manager"
               }
            }
         ],
         "remote": [
            {
            "type": "UserName"
            },
            {
               "type": "Groups",
               "any_one_of": [
                  "idp_admin"
               ]
            }
         ]
      }
]
```

  - 假设传入以下断言，由于John Smith属于“idp_admin”用户组，所以允许该用户访问云服务平台。

```
{UserName: John Smith}
{Groups: [idp_user, idp_admin, idp_agency]}
```

  - 假设传入以下断言，由于John Smith不属于“idp_admin”用户组，所以该规则对John Smith不生效，不允许John Smith访问云服务平台。

```
{UserName: John Smith}
{Groups: [idp_user, idp_agency]}
```

含有正则表达式的条件示例

您可以在条件里指定一个“"regex": true”用来表示云服务平台将以正则匹配的方式来计算结果。

以下示例表示该规则对在IdP中用户组名以任意值开头，“@mail.com”结尾的用户生效，在IAM中的用户名为*UserName*，所属用户组为“admin”。

```
[
    {
        "local": [
            {
                "user": {
                    "name": "{0}"
                }
            },
            {
                "group": {
                    "name": "admin"
                }
            }
        ],
        "remote": [
            {
            "type": "UserName"
            },
            {
                "type": "Groups",
                "any_one_of": [
                    ".*@mail.com$"
                ],
                "regex": true
            }
        ]
    }
]
```

条件组合示例

多个条件间，以“逻辑与”的方式组合。

以下示例表示该规则仅对既不属于IdP的“idp_user”也不属于IdP的“idp_agent”用户组的联邦用户生效。对于生效用户：在IAM中的用户名为*UserName*，所属用户组为“admin”。

```
[
    {
        "local": [
            {
                "user": {
                    "name": "{0}"
                }
            },
            {
                "group": {
                    "name": "admin"
                }
            }
        ],
        "remote": [
            {
            "type": "UserName"
            },
            {
                "type": "Groups",
                "not_any_of": [
                    "idp_user"
                ]
```

```
            },
            {
                "type": "Groups",
                "not_any_of": [
                    "idp_agent"
                ]
            }
        ]
    }
]
```

以上规则等同于：

```
[
    {
        "local": [
            {
                "user": {
                    "name": "{0}"
                }
            },
            {
                "group": {
                    "name": "admin"
                }
            }
        ],
        "remote": [
            {
            "type": "UserName"
            },
            {
                "type": "Groups",
                "not_any_of": [
                    "idp_user",
                    "idp_agent"
                ]
            }
        ]
    }
]
```

多个规则组合示例

多个规则组合，用户名与用户组生成方式不同。

用户名取第一个生效规则的用户名，所有规则中必须至少有一个用户名规则生效，否则云服务平台不允许此用户登录；而用户组则取所有生效规则用户组名称的集合。一种比较实用的多规则配置方式是把用户名配置与用户组配置分离。这样的配置会非常容易阅读。

以下示例表示针对IdP中属于“idp_admin”用户组的用户生效，在IAM中的用户名为*UserName*，所属用户组为“admin”。

```
[
  {
    "local": [
      {
        "user": {
          "name": "{0}"
        }
      }
    ],
    "remote": [
      {
        "type": "UserName"
      }
```

```
    ]
  },
  {
    "local": [
      {
        "group": {
          "name": "admin"
        }
      }
    ],
    "remote": [
      {
        "type": "Groups",
        "any_one_of": [
          "idp_admin"
        ]
      }
    ]
  }
]
```

假设传入以下断言，由于John Smith属于“idp_admin”用户组，因此此规则对John Smith生效。在IAM中的用户名为John Smith，所属用户组为“admin”。

```
{UserName: John Smith}
{Groups: [idp_user, idp_admin, idp_agency]}
```

3.9 多因素认证与虚拟 MFA

3.9.1 多因素认证

什么是多因素认证

多因素认证是一种非常简单的安全实践方法，它能够在用户名称和密码之外再额外增加一层保护。启用多因素认证后，用户进行操作时，除了需要提供用户名和密码外（第一次身份验证），还需要提供验证码（第二次身份验证），多因素身份认证结合起来将为您的账号和资源提供更高的安全保护。

多因素认证主要应用在登录验证和操作保护中，开启了登录验证功能后，用户登录控制台时，除了需要输入用户名和密码外，还需要在登录验证页面输入验证码；开启了操作保护后，用户进行敏感操作时，需要输入验证码确认操作。

多因素认证支持的设备

多因素认证设备支持手机、邮箱和虚拟MFA设备。

多因素认证应用的场景

多因素认证主要应用于登录保护以及操作保护。若开启多因素认证，则管理控制台和REST API均会受到影响。

- **登录保护**：您以及账号中的IAM用户登录时，除了在登录页面输入用户名和密码外，还需要在登录验证页面输入多因素认证设备中的验证码，再次确认登录者身份，进一步提高账号安全性。
- **操作保护**：您以及账号中的IAM用户进行敏感操作时，例如删除弹性云服务器资源，需要输入多因素认证设备中的验证码对操作进行确认，避免误操作带来的风险和损失。

更多有关登录保护和操作保护的介绍，请参见：**敏感操作**。

3.9.2 虚拟 MFA

本章主要为您介绍**如何绑定虚拟MFA**、**如何解绑虚拟MFA**，以及IAM用户手机丢失或删除虚拟MFA应用程序时**管理员如何重置虚拟MFA**。

什么是虚拟 MFA

虚拟Multi-Factor Authentication (MFA) 是能产生6位数字认证码的设备或应用程序，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，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，非常方便，虚拟MFA是多因素认证方式中的一种。

如何绑定虚拟 MFA

您需要在智能设备上安装一个虚拟MFA应用程序后（例如：Google Authenticator或Microsoft Authenticator），才能绑定虚拟MFA设备。

步骤1 **进入安全设置**。

步骤2 在“安全设置>敏感操作”页面，单击“虚拟MFA”右侧的“前往绑定”。

步骤3 根据右侧弹出的绑定虚拟MFA页面，在您的MFA应用程序中添加用户。

您可以通过扫描二维码、手动输入两种方式绑定MFA设备：

- 扫描二维码

  打开手机上已安装好的MFA应用程序，选择“扫描条形码”，扫描“绑定虚拟MFA”弹窗中的二维码。扫描成功后，应用程序会自动添加用户。

- 手动输入

  打开手机上已安装好的MFA应用程序，选择“输入提供的密钥”，手动添加用户。

  说明

  手动输入添加用户方式只支持基于时间模式，建议在移动设备中开启自动设置时间功能。

步骤4 添加用户完成，在返回MFA应用程序首页，查看虚拟MFA的动态口令页面。动态口令每30秒自动更新一次。

步骤5 在“绑定虚拟MFA”页面输入连续的两组口令，然后单击“确定”，完成绑定虚拟MFA设备的操作。

----结束

如何获取虚拟 MFA 验证码

绑定虚拟MFA并开启登录保护或操作保护后，用户在进行登录或进行敏感操作时，需要输入MFA应用程序的动态验证码。

此时，您需要打开智能设备上的虚拟MFA应用程序，查看并输入用户已绑定账号的验证码。

如何解绑虚拟 MFA

解绑虚拟MFA适用于手机未丢失或者没有删除虚拟MFA应用程序的IAM用户或账号，IAM用户或账号可以在界面自助完成解绑虚拟MFA的操作。

步骤1 进入安全设置。

步骤2 在“安全设置>敏感操作”页面，单击“虚拟MFA”右侧的“前往解绑”。

步骤3 在“解绑虚拟MFA”页面中输入从虚拟MFA设备获取的动态验证码。

图 3-44 输入虚拟 MFA 验证码

步骤4 单击“确定”，验证成功后，完成解绑MFA操作。

----结束

重置虚拟 MFA

手机丢失或已删除虚拟MFA应用程序的**IAM用户**，请联系**管理员**重置虚拟MFA，管理员的操作步骤如下所示。

步骤1 登录统一身份认证服务管理控制台。

步骤2 在“统一身份认证服务>用户”页签中的用户列表中，单击用户右侧的“安全设置”。

步骤3 在“安全设置”页面中，单击“虚拟MFA设备”右侧的“重置”。

步骤4 单击“确定”，重置成功。

----结束

3.10 查看 IAM 操作记录

3.10.1 开通云审计服务

云审计服务（Cloud Trace Service，以下简称CTS），是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。

为了方便查看IAM的关键操作事件，例如创建用户、删除用户等，建议管理员开启云审计服务。

操作步骤

步骤1 登录管理控制台。

步骤2 单击“服务列表”，选择“管理与部署 > 云审计服务 CTS”，进入云审计服务信息页面。

步骤3 单击左侧导航树的“追踪器”，进入追踪器信息页面。

步骤4 单击“开通云审计服务”。

步骤5 在开启云审计服务详情页面，单击“开启”，完成开启云审计服务，系统会自动分配一个追踪器。

开启云审计服务成功后，您可以在追踪器信息页面查看系统自动创建的追踪器的详细信息。

----结束

在IAM进行操作，例如创建用户、用户组等，CTS将会记录这些操作。CTS支持记录的IAM相关的操作事件，如下表所示。

表 3-21 CTS 支持的 IAM 操作列表

操作名称	资源类型	事件名称
用户登录	user	login
云联盟用户登录	user	cloudLoginBySaml
登录失败	user	loginFailed
用户登出	user	logout
联邦用户登录	user	tenantLoginBySamlSuccess/ oidcLoginSuccess
IAM用户首次登录、密码过期、密码即将过期提醒等场景修改密码	user	changePassword
创建用户	user	createUser
修改用户信息	user	updateUser
删除用户	user	deleteUser

操作名称	资源类型	事件名称
创建AK/SK	user	createCredential、addCredential
删除AK/SK	user	deleteCredential
停用、启用AK/SK	user	changeCredentialStatus
修改AK/SK	user	updateCredential
修改邮件地址	user	modifyUserEmail
修改手机	user	modifyUserMobile
用户在安全设置自行修改密码	user	modifyUserPassword
管理员设置用户密码	user	setPasswordByAdmin
创建用户组	userGroup	createUserGroup
更新用户组	userGroup	updateGroup、updateUserGroup
删除用户组	userGroup	deleteUserGroup
添加用户到用户组	userGroup	addUserToGroup、updateUser/updateUserGroup
从用户组删除用户	userGroup	removeUserFromGroup、updateUser/updateUserGroup
创建项目	project	createProject
修改项目	project	updateProject
删除项目	project	deleteProject
创建委托	agency	createAgency
修改委托	agency	updateAgency
删除委托	agency	deleteAgency
切换角色	agency	switchRole
	Token	createToken
创建身份提供商	identityProvider	createIdentityProvider
更新身份提供商	identityProvider	updateIdentityProvider
删除身份提供商	identityProvider	deleteIdentityProvider
上传IdP元数据	identityProvider	updateMetaConfigure、uploadMetadataFile

操作名称	资源类型	事件名称
手动编辑IdP元数据	identityProvider	updateMetaConfigure
创建自定义策略	role	createRole
修改自定义策略	role	updateRole
删除自定义策略	role	deleteRole
更新账号登录策略	domain	updateSecurityPolicies
更新密码策略	domain	updatePasswordPolicies
更新访问控制列表	domain	updateACLPolicies

3.10.2 查询审计事件

操作场景

用户进入云审计服务创建管理类追踪器后，系统开始记录云服务资源的操作。在创建数据类追踪器后，系统开始记录用户对OBS桶中数据的操作。云审计服务管理控制台会保存最近7天的操作记录。

本节介绍如何在云审计服务管理控制台查看或导出最近7天的操作记录：

- **在新版事件列表查看审计事件**
- **在旧版事件列表查看审计事件**

在新版事件列表查看审计事件

1. 登录管理控制台。
2. 单击左上角 ☰ ，选择“管理与部署 > 云审计服务 CTS”，进入云审计服务页面。
3. 单击左侧导航树的“事件列表”，进入事件列表信息页面。
4. 事件列表支持通过高级搜索来查询对应的操作事件，您可以在筛选器组合一个或多个筛选条件：
   - 事件名称：输入事件的名称。
   - 事件ID：输入事件ID。
   - 资源名称：输入资源的名称，当该事件所涉及的云资源无资源名称或对应的API接口操作不涉及资源名称参数时，该字段为空。
   - 资源ID：输入资源ID，当该资源类型无资源ID或资源创建失败时，该字段为空。
   - 云服务：在下拉框中选择对应的云服务名称。
   - 资源类型：在下拉框中选择对应的资源类型。
   - 操作用户：在下拉框中选择一个或多个具体的操作用户。
   - 事件级别：可选项为“normal”、“warning”、“incident”，只可选择其中一项。

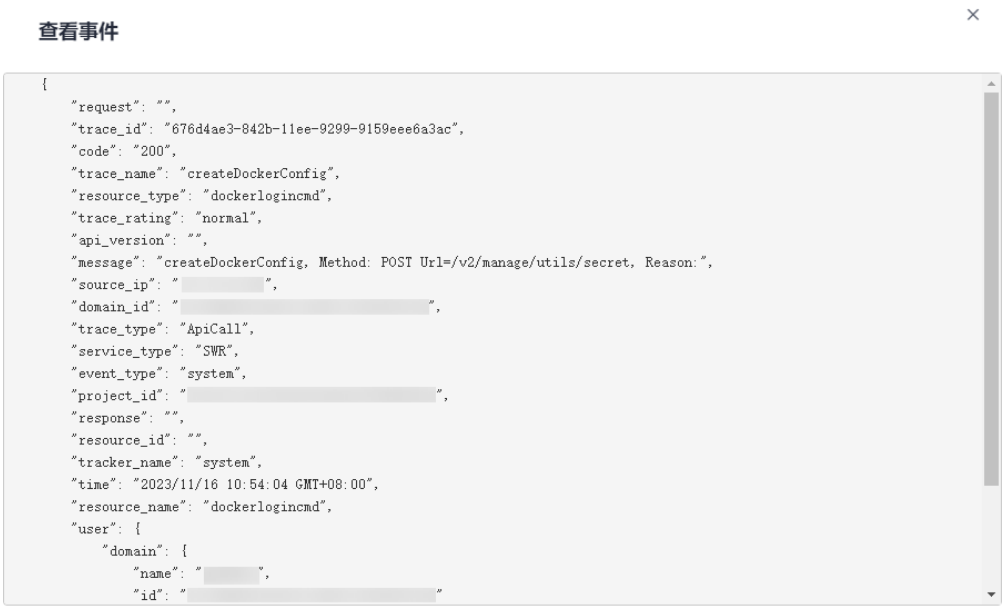
    - normal：表示操作成功。
    - warning：表示操作失败。
    - incident：表示比操作失败更严重的情况，例如引起其他故障等。
  - 时间范围：可选择查询最近1小时、最近1天、最近1周的操作事件，也可以自定义最近1周内任意时间段的操作事件。
5. 在事件列表页面，您还可以导出操作记录文件、刷新列表、设置列表展示信息等。
  - 在搜索框中输入任意关键字，单击 按钮，可以在事件列表搜索符合条件的数据。
  - 单击“导出”按钮，云审计服务会将查询结果以.xlsx格式的表格文件导出，该.xlsx文件包含了本次查询结果的所有事件，且最多导出5000条信息。
  - 单击按钮，可以获取到事件操作记录的最新信息。
  - 单击按钮，可以自定义事件列表的展示信息。启用表格内容折行开关 ，可让表格内容自动折行，禁用此功能将会截断文本，默认停用此开关。
6. 关于事件结构的关键字段详解，请参见“云审计服务事件参考 > 事件结构”章节和“云审计服务事件参考 > 事件样例”章节。
7. （可选）在新版事件列表页面，单击右上方的“返回旧版”按钮，可切换至旧版事件列表页面。

在旧版事件列表查看审计事件

1. 登录管理控制台。
2. 单击左上角 ，选择“管理与部署 > 云审计服务 CTS”，进入云审计服务页面。
3. 单击左侧导航树的“事件列表”，进入事件列表信息页面。
4. 用户每次登录云审计控制台时，控制台默认显示新版事件列表，单击页面右上方的“返回旧版”按钮，切换至旧版事件列表页面。
5. 事件列表支持通过筛选来查询对应的操作事件。当前事件列表支持四个维度的组合查询，详细信息如下：
  - 事件类型、事件来源、资源类型和筛选类型，在下拉框中选择查询条件。
    - 筛选类型按资源ID筛选时，还需手动输入某个具体的资源ID。
    - 筛选类型按事件名称筛选时，还需选择某个具体的事件名称。
    - 筛选类型按资源名称筛选时，还需选择或手动输入某个具体的资源名称。
  - 操作用户：在下拉框中选择某一具体的操作用户，此操作用户指用户级别，而非租户级别。
  - 事件级别：可选项为“所有事件级别”、“Normal”、“Warning”、“Incident”，只可选择其中一项。
  - 时间范围：可选择查询最近7天内任意时间段的操作事件。

- 单击“导出”按钮，云审计服务会将查询结果以CSV格式的表格文件导出，该CSV文件包含了本次查询结果的所有事件，且最多导出5000条信息。

6. 选择完查询条件后，单击“查询”。
7. 在事件列表页面，您还可以导出操作记录文件和刷新列表。
   - 单击“导出”按钮，云审计服务会将查询结果以CSV格式的表格文件导出，该CSV文件包含了本次查询结果的所有事件，且最多导出5000条信息。
   - 单击按钮，可以获取到事件操作记录的最新信息。
8. 在需要查看的事件左侧，单击 展开该记录的详细信息。
9. 在需要查看的记录右侧，单击“查看事件”，会弹出一个窗口显示该操作事件结构的详细信息。



10. 关于事件结构的关键字段详解，请参见《云审计服务用户指南》中的“云审计服务事件参考 > 事件结构”章节和“云审计服务事件参考 > 事件样例”章节。
11. （可选）在旧版事件列表页面，单击右上方的“体验新版”按钮，可切换至新版事件列表页面。

3.11 调整配额

什么是配额?

为防止资源滥用，平台限定了各服务资源的配额，对用户的资源数量和容量做了限制。如您最多可以创建多少个IAM用户、用户组等。

如果当前资源配额限制无法满足使用需要，您可以申请扩大配额。

怎样查看我的配额?

1. 登录管理控制台。
2. 单击管理控制台左上角的 ，选择区域和项目。

3. 单击页面右上角的“My Quota”图标  。
   系统进入“服务配额”页面。
4. 您可以在“服务配额”页面，查看各项资源的总配额及使用情况。
   如果当前配额不能满足业务要求，请参考后续操作，申请扩大配额。

如何申请扩大配额?

1. 登录管理控制台。
2. 在页面右上角，选择“资源 > 我的配额”。
   系统进入“服务配额”页面。
3. 单击“申请扩大配额”。
4. 在“新建工单”页面，根据您的需求，填写相关参数。
   其中，“问题描述”项请填写需要调整的内容和申请原因。
5. 填写完毕后，勾选协议并单击“提交”。

4 常见问题

4.1 用户组及权限管理类

4.1.1 无法找到特定服务的权限怎么办

问题描述

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权限。

可能原因

- 搜索的服务或权限名称不正确。

解决方法

- 请在管理控制台或帮助中心确认服务名称，并在中查看该服务提供的系统权限。

4.1.2 如何为 IAM 用户授予“中东-阿布扎比-OP5”区域云服务权限

问题描述

管理员已开通“中东-阿布扎比-OP5”区域业务，需要为账号中的IAM用户授予该区域云服务使用权限。

由于“中东-阿布扎比-OP5”区域用户属于联邦认证授权访问“中东-阿布扎比-OP5”云服务系统的虚拟用户，不是“中东-阿布扎比-OP5”云服务系统中真实存在的用户。因此需要在华为云默认区域和“中东-阿布扎比-OP5”区域独立授权。

前提条件

- 请确保您已在华为云默认区域创建IAM用户并将其加入用户组。如创建IAM用户“User-001”，并将其加入用户组“UserGroup-001”。请参考**创建IAM用户**、**用户组添加/移除用户**。
- 如果是首次为IAM用户授予“中东-阿布扎比-OP5”区域的云服务权限，需要使用账号进行授权操作，无法使用拥有管理员权限的IAM用户进行授权操作。

操作指导

步骤1 管理员登录华为云，在控制台首页单击“  ”，选择“中东-阿布扎比-OP5”区域。

步骤2 在“中东-阿布扎比-OP5”区域控制台，选择“管理与监管 > 统一身份认证服务”。

步骤3 在统一身份认证服务，左侧导航窗格中，选择“用户组”，单击右上方的“创建用户组”，创建同名用户组，如“UserGroup-001”。

步骤4 在“用户组”页面，单击**3**创建用户组右侧的“修改”。

步骤5 在“修改用户组>用户组权限”页面，单击用户需要授权区域右侧的“修改”，选择所需权限，单击“确定”。

为该同名用户组授权，对应华为云用户组中的IAM用户将拥有该用户组所有权限。

步骤6 单击“确定”，完成IAM用户“中东-阿布扎比-OP5”区域授权。

----结束

授权完成后，IAM用户登录华为云控制台，切换至“中东-阿布扎比-OP5”区域，可以按照权限使用云服务资源。

4.1.3 权限没有生效怎么办

问题描述

管理员在IAM控制台给IAM用户设置权限后，IAM用户登录发现权限没有生效。

问题排查

1. 可能原因：管理员授予IAM用户所在用户组的权限不正确。

   解决方法：管理员确认并修改授予IAM用户所在用户组的权限，方法请参考：用户指南>用户组及授权>查看或修改用户组，权限详情请参考：权限集。

2. 可能原因：管理员授予的权限已拒绝相关操作的授权项。

   解决方法：管理员查看已授予IAM用户的系统权限详情，确认已授予的权限是否有拒绝操作的语句，方法请参考用户指南>权限管理>策略>策略语法。如系统权限无法满足您的场景需要，管理员可以创建自定义策略，允许该操作对应的授权项，方法请参考：用户指南>权限管理>自定义策略。

3. 可能原因：管理员给用户组授予权限后，忘记将IAM用户添加至用户组中。

   解决方法：管理员将IAM用户添加至用户组中，方法请参见：用户指南>用户组及授权>用户组添加/移除用户。

4. 可能原因：对于区域级服务，管理员没有在在对应的区域进行授权。

   解决方法：管理员在对IAM所在用户组授权时，选择对应的区域。如果管理员授予用户默认区域项目的权限，用户只能访问该默认项目中的资源，不拥有该默认项目下IAM子项目的权限，建议您授予IAM用户最小区域权限，方法请参见：用户指南>用户组及授权>创建用户组并授权。

5. 可能原因：对于区域级服务，IAM用户登录控制台后，没有切换到授权区域。

   解决方法：IAM用户访问区域级服务时，请切换至授权区域，方法请参见：用户指南>项目。

6. 可能原因：管理员授予的OBS权限由于系统设计的原因，授权后需等待15-30分钟才可生效。

   解决方法：请IAM用户和管理员等待15-30分钟后重试。

7. 可能原因：浏览器缓存导致权限信息未更新。

   解决方法：请清理浏览器缓存后重试。

8. 可能原因：管理员同时在IAM和企业管理给用户授权，基于企业项目管理权限可能不生效。IAM鉴权优先于企业管理。

   解决方法：请管理员根据情况在IAM控制台修改用户权限。

相关问题

问题描述：如果您仅授予了IAM用户必要的权限，但IAM用户拥有了更多不应有的权限。

可能原因：

1. 管理员授予的权限有依赖角色，系统已自动勾选依赖角色，导致IAM用户拥有了额外的权限。如不勾选依赖角色，权限将不生效。
2. 管理员在企业项目管理中给IAM用户授予了其他权限。如需在IAM中管理项目、用户，建议在企业项目管理中取消相关权限配置。方法请参考：《企业管理用户指南》中的“移除企业项目用户组”章节。

4.2 IAM 用户管理类

4.2.1 IAM 用户登录失败怎么办

问题描述

IAM用户登录系统时提示“用户名或密码错误”、“您的管理员已设置了控制台ACL规则，禁止您所在的终端登录控制台”等，使IAM用户登录失败。

问题排查

- **系统提示“用户名或密码错误”**

  a. 可能原因：IAM用户登录时，未切换IAM登录入口。

     解决方法：单击“IAM用户登录”，切换登录入口。

  b. 可能原因：账号名和IAM用户名输入错误。

     解决方法：输入正确的账号名和IAM用户名。如果您不知道IAM用户名和所属账号，请联系管理员。

c. 可能原因：密码输入错误。

解决方法：输入正确的密码，如确认字母大小写等。如果您忘记密码，请参考以下方法找回：**忘记密码怎么办**。

d. 可能原因：修改过期密码或找回密码后，浏览器缓存信息未刷新。

解决方法：请清理浏览器缓存后，重新登录。

- **系统提示“您的管理员已设置了控制台ACL规则，禁止您所在的终端登录控制台”**

a. 可能原因：管理员在IAM控制台设置了访问控制规则，不允许您所在的IP地址区间、IP地址或网段、VPC Endpoint访问云服务平台。

解决方法：请联系管理员查看控制台ACL规则，从允许访问的设备登录云服务平台或由管理员修改访问控制规则。

4.2.2 如何控制 IAM 用户访问控制台

通过设置访问控制，限制IAM用户只能从特定IP地址区间访问系统，提高用户信息和系统的安全性。

操作步骤

步骤1 登录统一身份认证服务控制台。

步骤2 在左侧导航窗格中，选择“安全设置”，单击“访问控制”页签。

说明

访问控制仅对账号下的IAM用户生效，对账号本身不生效。

步骤3 在“访问控制”界面中，选择控“控制台访问”页签，设置允许访问的IP地址或网段。

- “允许访问的IP地址区间”：限制用户只能从设定范围内的IP地址登录。
- “允许访问的IP地址或网段”：限制用户只能从设定的IP地址或网段登录。

例如：10.10.10.10/32

说明

“允许访问的IP地址区间”和“允许访问的IP地址或网段”同时设置时只要满足其中一种即可允许访问。

步骤4 单击“应用”。

----结束

4.3 安全设置类

4.3.1 如何开启登录验证功能

为了确保您信息的安全，建议您开启登录验证功能。

开启该功能后，账号或IAM用户登录控制台时，需要在“登录验证”页面输入虚拟MFA/短信/邮箱验证码进行验证。

关闭该功能后，账号或IAM用户登录控制台时，仅需要输入账号/用户名、密码进行系统验证。

操作步骤

- 管理员在**统一身份认证服务控制台**开启其他IAM用户的登录验证功能

步骤1 在统一身份认证服务控制台左侧导航窗格中，单击“用户”。

步骤2 在用户列表中，单击对应用户栏目的“安全设置”。

步骤3 在“用户详情>安全设置”界面，“登录保护”下的“验证方式”中，选择需要使用的验证方式，输入相应的验证码。

步骤4 单击“确定”。

----结束

- 账号在**安全设置**中开启自己的登录验证功能

步骤1 登录统一身份认证服务控制台，在左侧导航窗格中，选择“安全设置”。

步骤2 在安全设置页面，“敏感操作”页签中，单击“登录保护”右侧的“立即设置”。

步骤3 在“登录保护设置”页面中，勾选“开启”，并选择需要使用的验证方式，输入相应的验证码。

步骤4 单击“确定”。

----结束

相关操作

开启登录保护后，您可以为其它IAM用户或自己修改登录保护验证方式：

- 管理员在**统一身份认证控制台**的用户列表中，进入对应用户栏目的“安全设置”，单击“登录保护>验证方式”后的“ ”为其它IAM用户修改登录保护验证方式。
- 管理员在**安全设置**的敏感操作页签中，单击“登录保护”右侧的“立即修改”，在弹窗中“验证方式”选择手机/邮件地址/虚拟MFA。

4.3.2 如何关闭登录验证功能

为了确保您信息的安全，建议您开启登录验证功能。

开启该功能后，账号或IAM用户登录控制台时，需要在“登录验证”页面输入虚拟MFA/短信/邮箱验证码进行验证。

关闭该功能后，账号或IAM用户登录控制台时，仅需要输入账号/用户名、密码进行系统验证。

管理员关闭 IAM 用户登录验证

- 管理员在**统一身份认证服务控制台**关闭其他IAM用户的登录验证功能

步骤1 在统一身份认证服务控制台左侧导航窗格中，单击“用户”。

步骤2 在用户列表中，单击对应用户栏目的“安全设置”。

步骤3 在“用户详情>安全设置”界面，“登录保护”下的“验证方式”中，单击“”，选择验证方式为“关闭”。

步骤4 单击“确定”。

----结束

管理员关闭自身登录验证

- 账号在**安全设置**中关闭自己的登录验证功能

步骤1 登录统一身份认证服务控制台，在左侧导航窗格中，选择“安全设置”。

步骤2 在安全设置页面，“敏感操作”页签中，单击“登录保护”右侧的“立即修改”。

步骤3 在“登录保护设置”页面中，勾选“关闭”。

步骤4 单击“确定”。

----结束

4.3.3 如何修改操作保护验证方式

问题描述

管理员开启操作保护后，用户在进行敏感操作时，例如删除资源、生成访问密钥等，需要操作员或指定人员进行验证，避免误操作带来的风险和损失。

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。

- 如当前验证方式为“操作员验证”，修改为“指定人员验证”，请参考：**•当前验证方式为“操作员验证”**。
- 如当前验证方式为“指定人员验证”，修改为“操作员验证”或修改指定人员手机号/邮件地址，请参考：**•当前验证方式为“指定人员验证”**。

操作步骤

- **当前验证方式为“操作员验证”**

步骤1 登录统一身份认证服务控制台，在左侧导航窗格中，选择“安全设置”。

步骤2 在“安全设置”页面中，选择“敏感操作”页签，单击操作保护右侧的“立即修改”。

步骤3 在右侧弹出的“操作保护设置”页面中，选择“指定人员验证”，输入验证手机号/邮件地址、验证码。

步骤4 单击“确定”，修改验证方式为指定人员验证。

----结束

- **当前验证方式为“指定人员验证”**

步骤1 登录统一身份认证服务控制台，在左侧导航窗格中，选择“安全设置”。

步骤2 在“安全设置”页面中，选择“敏感操作”页签，单击操作保护右侧的“立即修改”。

步骤3 在右侧弹出的“操作保护设置”页面中，选择“关闭”，单击“确定”并进行身份验证，关闭操作保护。

步骤4 在“安全设置”页面，“敏感操作”页签中，单击操作保护右侧的“立即启用”。

步骤5 在右侧弹窗中选择“开启”，勾选“操作员验证”或“指定人员验证”。

如选择“指定人员验证”，开启操作保护时，需要进行初次身份核验，确保指定人员验证方式可用。

- 操作员验证：触发敏感操作的账号或IAM用户进行二次验证。
- 指定人员验证：账号及IAM用户触发的敏感操作均由指定人员进行验证。支持手机号、邮件地址，不支持虚拟MFA验证。

步骤6 单击“确定”，修改操作保护验证方式。

----结束

4.3.4 如何关闭操作保护

问题描述

管理员开启操作保护后，用户在进行敏感操作时，例如删除资源、生成访问密钥等，需要操作员或指定人员进行验证，避免误操作带来的风险和损失。如需关闭操作保护，请按照以下步骤操作。

操作步骤

步骤1 登录统一身份认证服务控制台，在左侧导航窗格中，选择“安全设置”。

步骤2 在“安全设置”页面中，选择“敏感操作”页签，单击操作保护右侧的“立即修改”。

步骤3 在右侧弹出的“操作保护设置”页面中，选择“关闭”，单击“确定”并进行身份验证后，操作保护关闭成功。

----结束

4.3.5 如何绑定虚拟 MFA 设备

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户和资源提供更高的安全保护。

MFA设备可以基于硬件也可以基于软件，系统目前仅支持基于软件的虚拟MFA。

虚拟MFA设备是能产生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。此类应用程序可在移动硬件设备（包括智能手机）上运行，非常方便。

前提条件

用户需要先在智能设备上安装一个MFA应用程序（例如：Google Authenticator），才能绑定虚拟MFA设备。

操作步骤

步骤1 登录统一身份认证服务控制台，在左侧导航窗格中，选择“安全设置”。

步骤2 在“敏感操作”页签，单击“虚拟MFA”右侧的“前往绑定”。

步骤3 根据右侧弹出的绑定虚拟MFA页面，在您的MFA应用程序中添加用户。

- 扫描二维码
- 手动输入

步骤4 添加用户完成，查看虚拟MFA的动态口令页面。动态口令每30秒自动更新一次。

步骤5 在“绑定虚拟MFA”页面输入连续的两组口令，然后单击“确定”，完成绑定虚拟MFA设备的操作。

----结束

相关 FAQ

如何获取虚拟MFA验证码

如何解绑、重置虚拟MFA

虚拟MFA验证码校验不通过怎么办

4.3.6 如何获取虚拟 MFA 验证码

绑定虚拟MFA并开启登录保护或操作保护后，用户在进行登录或进行敏感操作时，需要输入MFA应用程序的动态验证码，下图以登录验证为例。

此时，用户需要打开MFA应用程序，在首页查看用户已绑定账号的验证码。

说明

如果虚拟MFA验证码校验不通过，请参考：**虚拟MFA验证码校验不通过怎么办**。

4.3.7 如何解绑、重置虚拟 MFA

- 如果您可以正常使用已与账号绑定的虚拟MFA应用程序，需要解绑MFA，请参考：**解绑虚拟MFA**。
- 如果您无法正常使用已与账号绑定的虚拟MFA应用程序，将无法解绑MFA，只能重置MFA。请参考：**重置虚拟MFA**。

解绑或重置后，如需再次绑定虚拟MFA，请IAM用户在“安全设置”中自行重新绑定，详细操作请参见：**如何绑定虚拟MFA设备**。

解绑虚拟 MFA

1. 登录统一身份认证服务控制台，在左侧导航窗格中，选择“安全设置”。
2. 在“敏感操作”页签，单击“虚拟MFA”右侧的“前往解绑”。
3. 在解绑虚拟MFA页面，输入从虚拟MFA设备获取的动态验证码。
4. 单击“确定”，验证成功后，完成解绑MFA操作。

重置虚拟 MFA

手机丢失或已删除虚拟MFA应用程序的**IAM用户**，请联系管理员重置虚拟MFA，管理员的操作步骤如下所示。

1. 登录统一身份认证服务控制台。
2. 在“统一身份认证服务>用户”页签中的用户列表中，单击用户右侧的“安全设置”。
3. 在“安全设置”页面中，单击“虚拟MFA设备”右侧的“重置”。
4. 单击“确定”，重置成功。

4.3.8 虚拟 MFA 验证码校验不通过怎么办

问题描述

进行二次验证、绑定或解绑虚拟MFA时，MFA验证码校验不通过。

可能原因

- 验证码输入错误。
- 动态验证码未更新。
- 读取了非本账号的虚拟MFA验证码。
- 重新绑定虚拟MFA时，未在虚拟MFA设备中重新添加用户。
- MFA验证码的生成机制和时间相关，如果手机时间和虚拟MFA设备后台服务的系统时间相差30秒以上，生成的MFA验证码将不能通过校验。

解决方法

- 请确保输入正确的验证码。
- 验证码每30秒自动更新一次，请等待更新后再输入连续的两组验证码。
- 请在虚拟MFA设备中确认验证码上方的账号与二次验证、绑定或解绑的账号一致。
- 重新绑定虚拟MFA时，需在虚拟MFA设备中删除原用户信息，重新添加用户并读取该用户对应动态码。
- 请修正手机时间后重新验证。（注意手机时间和时区无关，后台会自动转化为世界协调时间，即UTC时间戳。）

4.3.9 无法接收验证码怎么办

当您绑定或者修改手机号码/邮箱、重置密码等操作时，需要获取验证码进行验证。若您无法接收验证码，请参考以下方法进行操作。

无法接收短信验证码

- 请确认手机号码是否填写正确。
- 请核实手机是否已停机，手机缴费以后一般是24小时内恢复，建议您更换手机号码或者第二天重新获取。
- 网络通讯异常可能会造成短信丢失，请重新获取或稍后再试。您也可以尝试将SIM卡移动到另一部手机，然后重试。

为了不影响您的业务操作，如果以上方法依然未能解决您的问题，建议您将验证方式修改为通过邮箱/虚拟MFA验证。

无法接收邮箱验证码

- 请确认邮箱地址是否填写正确。
- 请核实邮箱是否正常使用，并检查垃圾邮箱夹。
- 网络通讯异常可能会造成邮件丢失，请重新获取或稍后再试。

为了不影响您的业务操作，如果以上方法依然未能解决您的问题，建议您将验证方式修改为通过手机/虚拟MFA验证。

4.3.10 账号被锁定怎么办

问题描述

- 登录系统时，提示“当前用户已被锁定，请15分钟后重试”。
- 调用请求参数包含密码的API时，响应信息如下：

```
{
    "error": {
        "code": 401,
        "message": "The account is locked.",
        "title": "Unauthorized"
    }
}
```

可能原因

账号出现安全异常行为，如多次输入错误密码、账号频繁多地登录等，导致账号被锁定，锁定时间为15分钟。

解决方法

- 如您误操作，导致账号被锁，请等待15分钟后重新登录，且15分钟内请勿再次登录或输入密码。
- 如果您忘记了自己的登录密码，可以找回或重置密码。操作请参考**忘记密码怎么办**。
- 如果您没有进行任何操作，但账号被锁，请尽快修改密码。操作请参考**如何修改密码**。

4.3.11 解绑虚拟 MFA 后，登录时仍需通过虚拟 MFA 进行登录验证

问题描述

您已解绑或重置虚拟MFA，登录云平台时，仍需要通过虚拟MFA进行登录验证。

可能原因

您已开启登录保护，验证方式是“虚拟MFA”，且已解绑或重置虚拟MFA。此时，您的MFA设备和云平台的绑定关系已解除，但是登录保护依然生效，因此需要进行登录验证。

解决方法

- 登录时，重新绑定虚拟MFA，并通过虚拟MFA进行登录验证。

  单击登录验证弹窗中的“绑定虚拟MFA”，操作请参考：**如何绑定虚拟MFA设备**。

- 如果您是IAM用户，还可以请管理员修改登录保护验证方式为手机号或邮件地址，并通过修改后的方式进行登录验证。

  管理员登录IAM控制台，单击用户名称，进入该用户详情页，在“安全设置”页签中修改登录保护验证方式。

4.4 密码凭证类

4.4.1 忘记密码怎么办

如果您忘记了IAM用户或账号的密码，请参考**忘记IAM用户或账号密码**自行重置登录密码。

忘记 IAM 用户或账号密码

如果您是IAM用户，还可以请管理员修改密码，适用于您没有绑定邮箱或者手机，无法自行修改密码，详情请参考：用户指南>IAM用户>修改IAM用户密码。

步骤1 在登录页面，单击“忘记密码”。

步骤2 输入需要重置密码的账号或者IAM用户信息及验证码。

说明

- 账号：注册云服务平台时创建的账号，账号是资源的归属，对其所拥有的资源具有完全控制权限，可以访问所有云服务。使用账号登录后，在IAM的“用户”中可以看到账号对应的用户，在IAM中标识为“企业管理员”。
- IAM用户：由管理员在IAM中创建的用户，IAM用户可以使用账号名、IAM用户名和密码登录云服务平台，并根据权限使用所属账号中的资源。IAM不拥有资源，IAM用户的权限和资源由所属账号统一控制。
- 如果您是IAM用户，且没有绑定邮件地址或手机，将无法通过该方式找回密码，请联系管理员修改您的IAM用户密码。操作请参考：用户指南>IAM 用户>修改IAM用户密码。

步骤3 选择重置密码的方式为账号名/邮件地址或者手机号，并按照界面提示填写验证信息，单击“下一步”。

说明

- 请输入正确的手机号或邮件地址，否则将导致找回密码失败。
- 如果无法接收验证码，请参考**无法获取验证码**进行处理。

步骤4 输入新密码并确认密码，单击“确定”。

步骤5 单击“立即登录”，使用新设置的密码登录云服务平台。

----结束

4.4.2 如何修改密码

- 主动修改密码
  - 如果您是**账号**，需要主动修改密码，请参考**忘记IAM用户或账号密码**自行重置登录密码。
  - 如果您是**IAM用户**，可以在IAM控制台的左侧导航栏中，选择“安全设置”页签，进入“基本信息”页签修改您的用户密码，详情请参考用户指南>IAM用户>修改IAM用户密码。
- 忘记密码
  - 通过登录页面的“忘记密码”功能自行修改密码，详情请参考：**忘记密码怎么办**。

- 如果您是IAM用户，还可以请管理员修改密码，适用于您没有绑定邮箱或者手机，无法自行修改密码，详情请参考：用户指南>IAM 用户>修改IAM用户密码。

4.4.3 丢失访问密钥 AK/SK 怎么办

如果您的访问密钥AK/SK已丢失，建议您先创建新的访问密钥AK/SK，并使用新的访问密钥AK/SK替换正在使用的应用程序等的访问密钥AK/SK之后，确认无其他业务影响，再将丢失的访问密钥AK/SK停用或删除。具体方法请参见：《 我的凭证用户指南 》。

说明

- 每个用户最多可创建**2**个访问密钥，不支持增加配额。
- 如果您是IAM用户，请在“安全设置>敏感操作>访问密钥保护”确认所属账号是否开启**访问密钥保护**。
  - **访问密钥保护**关闭时，所有IAM用户可以管理（包含创建、启用/停用或删除）自己的访问密钥。
  - **访问密钥保护**开启时，仅拥有相应权限的IAM用户才可以管理自己的访问密钥。
- 如果您无法管理您的访问密钥，请联系管理员：
  - 由管理员管理您的访问密钥，方法请参见：用户指南>IAM 用户>管理IAM用户访问密钥。
  - 请管理员为您配置权限或修改访问密钥保护状态。如需配置权限请参见：用户指南>IAM 用户>给IAM用户授权，如需修改访问密钥状态请参见：用户指南>安全设置>敏感操作。

4.4.4 什么是临时安全凭证（临时 AK/SK 和 SecurityToken）

什么是临时安全凭证

临时安全凭证是**具备临时访问权限**的身份凭证，包括临时AK/SK和SecurityToken，临时安全凭证与永久安全凭证的工作方式几乎相同，仅存在小量差异。

临时安全凭证与永久安全凭证的差异

- 临时安全凭证存在有效期，可以在15分钟至24小时之间进行设置；永久安全凭证的有效期为永久，并且不能进行设置。
- 临时安全凭证没有数量限制；每个IAM用户最多可创建2个永久安全凭证。
- 临时安全凭证通过接口获取临时AK/SK获取；永久安全凭证通过我的凭证界面控制台获取。
- 临时安全凭证为动态生成，即时使用，不能嵌入应用程序中，或者进行存储，到期后无法重复使用，只能重新获取。

临时安全凭证的优势

在给外部联邦用户授权时，临时安全凭证的优势尤为明显，您不必给外部联邦用户授予需要定时轮换，主动撤销的永久安全凭证，而是给这些外部联邦用户授予即时使用，定时过期的临时安全凭证，提高账号的安全性，遵循权限最小化的安全实践原则。

临时安全凭证的使用方法

临时安全凭证包括临时AK/SK和SecurityToken，临时AK/SK和SecurityToken必须同时使用，临时安全凭证与永久安全凭证的使用方法几乎相同，使用临时安全凭证进行鉴权时，请求头中需要添加“x-security-token”字段。

4.4.5 如何获取 Security Administrator 权限的 Token

Token是系统颁发给IAM用户的访问令牌，承载用户的身份、权限等信息。调用IAM以及其他云服务的接口时，可以使用本接口获取的IAM用户Token进行鉴权。

Token的权限由用户本身具备的权限决定，即获取Token的用户必须有Security Administrator权限，才能获取具有Security Administrator权限的Token。

获取方法

- 您是账号本身，需要为自己创建一个IAM用户，授予该用户Security Administrator权限后，调用获取用户Token接口即可获取具有Security Administrator权限的Token。
- 您是账号下的IAM用户，需要管理员给您授予Security Administrator权限后，才能获取具有Security Administrator权限Token，否则只能获取您自身已有权限的Token。

Security Administrator 权限说明

表 4-1 Security Administrator 权限说明

权限名称	所属区域	权限描述
Security Administrator	全局	IAM的管理员权限，可以对IAM执行所有操作，包括但不限于： • 创建、修改、删除IAM用户。 • 创建、修改、删除用户组、给用户组授权。 • 创建、修改、删除自定义策略。 • 创建、修改项目。 • 创建、修改、删除委托。 • 创建、修改、删除身份提供商。 • 设置账号安全策略。

4.4.6 如何获取“中东-阿布扎比-OP5”区域的访问密钥 AK/SK

问题描述

管理员已开通“中东-阿布扎比-OP5”区域业务，账号及账号中的IAM用户需要在“中东-阿布扎比-OP5”区域使用访问密钥进行加密签名。

由于“中东-阿布扎比-OP5”区域用户属于联邦认证授权访问“中东-阿布扎比-OP5”云服务系统的虚拟用户，不是中东-阿布扎比-OP5”云服务系统中真实存在的用户。因此需要在华为云默认区域和“中东-阿布扎比-OP5”区域分别获取访问密钥AK/SK。

本文适用于管理员为自己或IAM用户创建永久访问密钥的场景。管理员和IAM用户都可以在“我的凭证”中自行创建临时访问密钥。

操作步骤

步骤1 管理员在“中东-阿布扎比-OP5”区域创建IAM用户。管理员为自己创建访问密钥AK/SK请直接跳转至2。

1. 管理员登录华为云，在控制台首页单击“  ”，选择“中东-阿布扎比-OP5”区域。
2. 在“中东-阿布扎比-OP5”区域控制台，选择“管理与监管 > 统一身份认证服务”。
3. 在统一身份认证服务，左侧导航窗格中，选择“用户”。
4. 单击右上方的“创建用户”。
5. 在“创建用户”界面，填写相关信息，具体说明请参见：**创建IAM用户**。
   为了区分访问密钥AK/SK的使用主体，建议为IAM用户或账号创建同名IAM用户。
6. 单击“确定”，创建IAM用户完成。

步骤2 管理员获取IAM用户的访问密钥AK/SK。

1. 管理员登录“中东-阿布扎比-OP5”区域IAM服务控制台。
2. 在IAM控制台“用户”页面，单击1所创建IAM用户操作列的“设置凭证”。
3. 在IAM用户详情“设置凭证”页面，单击“管理访问密钥”下的“新增访问密钥”。
4. （可选）填写访问密钥描述。
5. 单击“新增访问密钥”弹窗中的“确定”，成功创建访问密钥。
6. 单击“立即下载”，下载访问密钥。

   说明

   - 每个用户最多可创建2个访问密钥，有效期为永久。为了账号安全性，建议妥善保管访问密钥。
   - 管理员及IAM用户仅能在“中东-阿布扎比-OP5”区域使用该访问密钥。
7. （可选）如果为其他IAM用户创建访问密钥AK/SK，需要将访问密钥发送给用户。

----结束

4.5 项目管理类

4.5.1 IAM 和企业管理的区别

企业管理是提供给企业客户的与多层级组织和项目结构相匹配的云资源管理服务。主要包括企业项目管理和人员管理。统一身份认证（Identity and Access Management，简称IAM）是提供用户身份认证、权限分配、访问控制等功能的身份管理服务。

与IAM相同的是，企业管理可以进行人员管理及权限分配，不同的是，企业管理对资源的授权粒度比IAM的更为精细，建议中大型企业使用企业管理服务。更多有关企业管理功能介绍，请参见：《企业管理用户指南》。

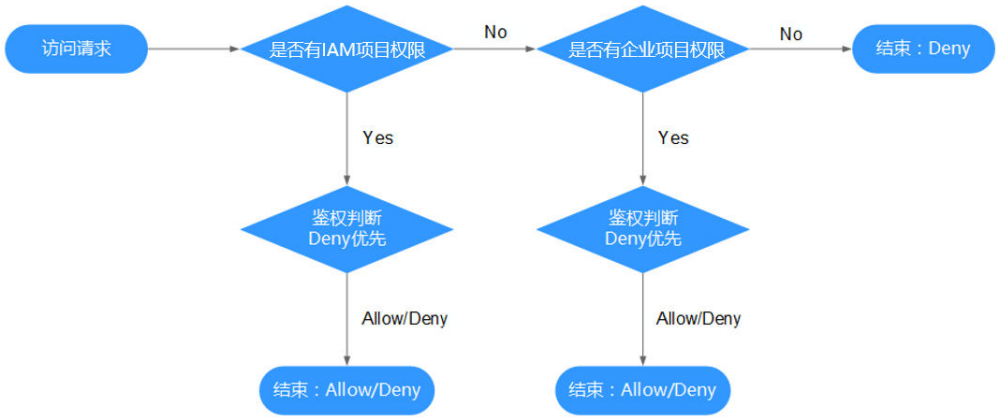
IAM 和企业管理的区别

- 开通方式
  - IAM是云平台的身份管理服务，注册系统后，无需付费即可使用。
  - 企业管理是云平台的资源管理服务，注册系统后，无需付费即可使用。。
- 资源隔离
  - IAM通过在区域中创建子项目，隔离同一个区域中的资源。以子项目为单位进行授权，用户可以访问指定子项目中的所有资源，详情请参见：用户指南>项目。
  - 企业管理通过创建企业项目，隔离企业不同项目之间的资源，企业项目中可以包含多个区域的资源。企业项目还可以实现对特定云资源的授权，例如：将一台特定的ECS添加至企业项目，对企业项目进行授权后，可以控制用户仅能管理这台特定的ECS。

检查规则

用户在发起访问请求时，系统根据用户被授权的访问策略中的action进行鉴权判断。检查规则如下：

图 4-1 请求鉴权逻辑图

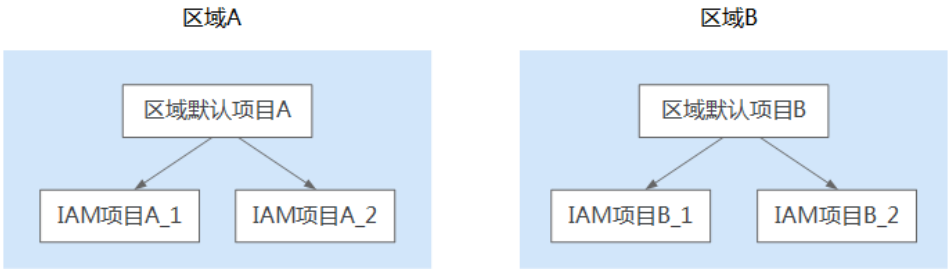


1. 用户发起访问请求。
2. 系统在用户被授予的访问权限中，优先寻找基于IAM项目授权的权限，在权限中寻找请求对应的action。
3. 如果找到匹配的Allow或者Deny的action，系统将返回对请求的鉴权决定，Allow或者Deny，鉴权结束。
4. 如果在基于IAM项目的权限中没有找到请求对应的action，系统将继续寻找基于企业项目授权的权限，在权限中寻找请求对应的action。
5. 如果找到匹配的Allow或者Deny的action，系统将返回对请求的鉴权决定，Allow或者Deny，鉴权结束。
6. 如果用户不具备任何权限，系统将返回鉴权决定Deny，鉴权结束。

4.5.2 IAM 项目和企业项目的区别

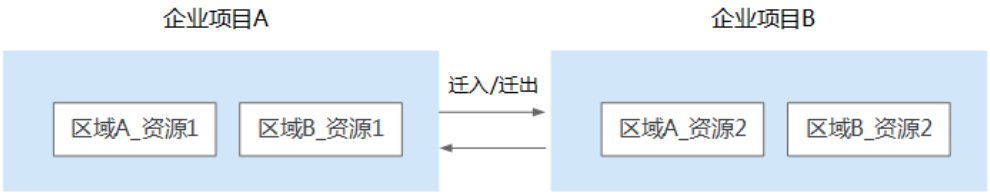
IAM 项目

IAM项目是针对同一个区域内的资源进行分组和隔离，是物理隔离。在IAM项目中的资源不能转移，只能删除后重建。



企业项目

企业项目是IAM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。企业项目可以实现对特定云资源的授权，例如：将一台特定的ECS添加至企业项目，对企业项目进行授权后，可以控制用户仅能管理这台特定的ECS。如果您开通了企业管理，将不能创建IAM项目。



4.6 委托管理类

4.6.1 创建委托时提示权限不足怎么办

问题描述

IAM用户尝试进入IAM控制台创建委托时，系统提示权限不足。

可能原因

该IAM用户不具备使用IAM的权限。

拥有IAM使用权限的对象为：

- 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”或“FullAccess”权限的用户：具备该权限的用户为IAM管理员，可以使用IAM。

解决方法

- 请管理员创建委托。
- 请管理员授予使用IAM服务的权限。

4.7 其他问题

4.7.1 Internet Explorer 浏览器下输入框提示信息无法自动消失怎么办

当用户进行登录、注册、绑定账号、创建用户、找回密码、修改密码等操作时，由于当前输入框不能完全支持Internet Explorer 8及以下版本的浏览器，所以出现输入框提示信息（如“最短不能少于5个字符”等提示信息）无法自动消失的情况，可以参照以下方法进行操作。

图 4-2 提示信息无法消失

- 升级浏览器版本

  将Internet Explorer浏览器升级到IE9及以上版本再进行操作。

- 更换浏览器

  使用Firefox浏览器（38.0及以上版本）或Google Chrome浏览器（43.0及以上版本）进行操作。

4.7.2 如何在 Google Chrome 浏览器禁用密码联想与保存

当用户首次使用Google Chrome浏览器成功登录云服务平台，浏览器会默认弹框提示用户并确认是否保存登录密码，这是由于安装Google Chrome浏览器后，浏览器“设置”页面的“自动填充”区域中，“密码”页面下“提示保存密码”和“自动登录”选项是默认开启的。如果用户根据界面提示确认保存密码后，下次登录云服务平台时，登录界面的密码输入框会自动联想填充字符，为了确保账号及密码安全，用户可关闭该功能。以Google Chrome浏览器的61.0.3163.100正式版本为例，可以参照以下方法进行操作。

操作步骤

步骤1 打开Google Chrome浏览器，单击右上角 ⋮ 并选择“设置”。

步骤2 在“自动填充”区域，选择“密码”。

步骤3 在密码页面，关闭“提示保存密码”和“自动登录”。

图 4-3 关闭“提示保存密码”和“自动登录”

----结束

后续处理

清除已保存的账号登录信息的方法：在密码页面，“已保存的密码”区域下，单击某条登录信息记录右侧的 ，并选择“移除”，即可清除对应网站地址、登录用户名及密码信息。

4.7.3 区域和可用区

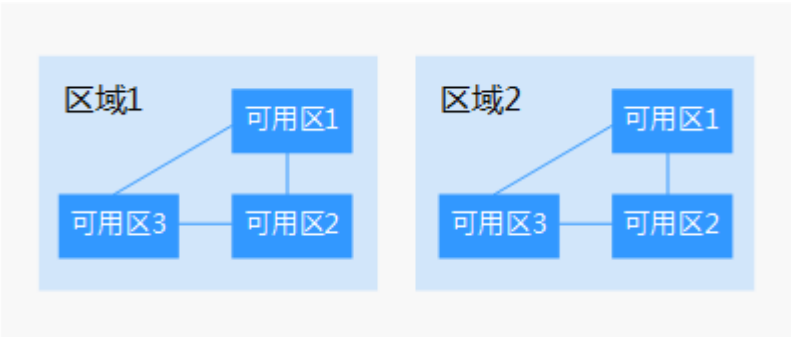
什么是区域、可用区?

区域和可用区用来描述数据中心的位置，您可以在特定的区域、可用区创建资源。

- 区域（Region）指物理的数据中心。每个区域完全独立，这样可以实现最大程度的容错能力和稳定性。资源创建成功后不能更换区域。
- 可用区（AZ，Availability Zone）是同一区域内，电力和网络互相隔离的物理区域，一个可用区不受其他可用区故障的影响。一个区域内可以有多个可用区，不同可用区之间物理隔离，但内网互通，既保障了可用区的独立性，又提供了低价、低时延的网络连接。

图4-4阐明了区域和可用区之间的关系。

图 4-4 区域和可用区



如何选择区域?

建议就近选择靠近您或者您的目标用户的区域，这样可以减少网络时延，提高访问速度。

如何选择可用区?

是否将资源放在同一可用区内，主要取决于您对容灾能力和网络时延的要求。

- 如果您的应用需要较高的容灾能力，建议您将资源部署在同一区域的不同可用区内。
- 如果您的应用要求实例之间的网络延时较低，则建议您将资源创建在同一可用区内。

区域和终端节点

当您通过API使用资源时，您必须指定其区域终端节点。有关云服务的区域和终端节点的更多信息，请参阅**地区和终端节点**。

5 修订记录

表 5-1 修订记录

日期	修订记录
2022-06-23	第五次正式发布。 本次变更有如下改动： 新增**自主管理用户属性**内容。 新增**查看授权记录**内容。 新增**授权记录**内容。 修改**查看或修改用户组**内容。 根据新版界面刷新授权、自定义策略相关章节。
2021-11-30	第三次正式发布。 本次变更根据界面风格、产品功能刷新资料内容。
2021-07-30	第二次正式发布。 本次变更根据产品版本刷新所有章节。
2020-08-17	第一次正式发布。