统一身份认证

用户指南 (巴黎区域)

文档版本 19

发布日期 2021-07-30

华为技术有限公司

商标声明


和其他华为商标均为华为技术有限公司的商标。
本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

华为技术有限公司

地址： 深圳市龙岗区坂田华为总部办公楼 邮编：518129

网址： https://www.huawei.com

客户服务邮箱： support@huawei.com

客户服务电话： 4008302118

安全声明

漏洞处理流程

华为公司对产品漏洞管理的规定以“漏洞处理流程”为准，该流程的详细内容请参见如下网址：
https://www.huawei.com/cn/psirt/vul-response-process
如企业客户须获取漏洞信息，请参见如下网址：
https://securitybulletin.huawei.com/enterprise/cn/security-advisory

目 录

1 产品简介

1.1 统一身份认证服务

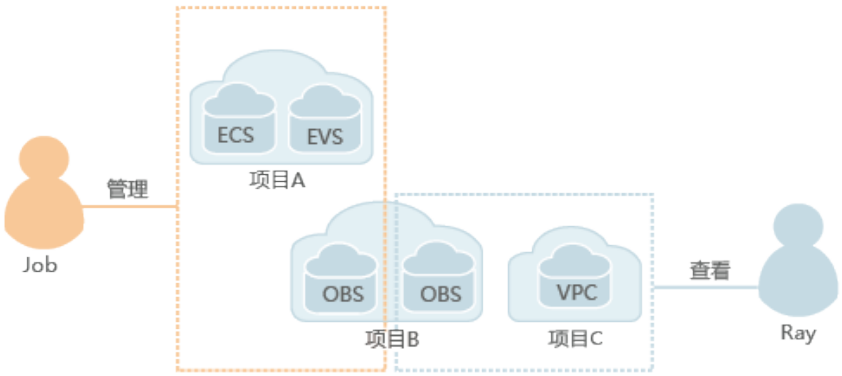
统一身份认证（Identity and Access Management，简称IAM），是提供用户身份认证、权限分配、访问控制等功能的身份管理服务。通过IAM您可以创建用户（用户可以是个人用户、系统或应用程序等），并授予用户管理您账号下资源的权限，避免共享您的API密码/访问密钥，帮助您高效的管理资源。您还可以设置账号安全策略来确保账号的安全，从而降低您的企业信息安全风险。

1.2 功能介绍

IAM为您提供身份认证及权限管理等基本功能，主要功能如下：

- 精细的权限管理
  您可以通过IAM控制不同用户访问不同的项目，还能控制不同的用户在相同项目下具备不同的权限。例如：控制某些用户管理对象存储，而让另外一些用户只能从对象存储中读取数据。

图 1-1 权限管理模型



- 便捷的用户授权

  使用IAM完成用户授权仅需要两步：

  a. 按照用户职责规划用户组，并将对应职责的权限授予用户组。

  b. 将用户加入用户组。
- 联邦身份认证

  您可以通过联邦身份认证，用户在企业管理系统完成身份认证后，实现单点登录，不需要重新创建用户。
- 委托第三方账号或者云服务管理资源

  通过委托信任机制，用户可以将自己的操作权限委托给更专业、高效的第三方账号或者云服务，第三方账号或者云服务可以代维管理用户的资源。
- 为其他服务提供认证和授权功能

  使用IAM认证后的用户可以根据权限使用系统中的其他服务，如：关系型数据库、云审计、对象存储等。
- 集中管理安全策略

  通过设置多因素认证、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。

1.3 身份管理

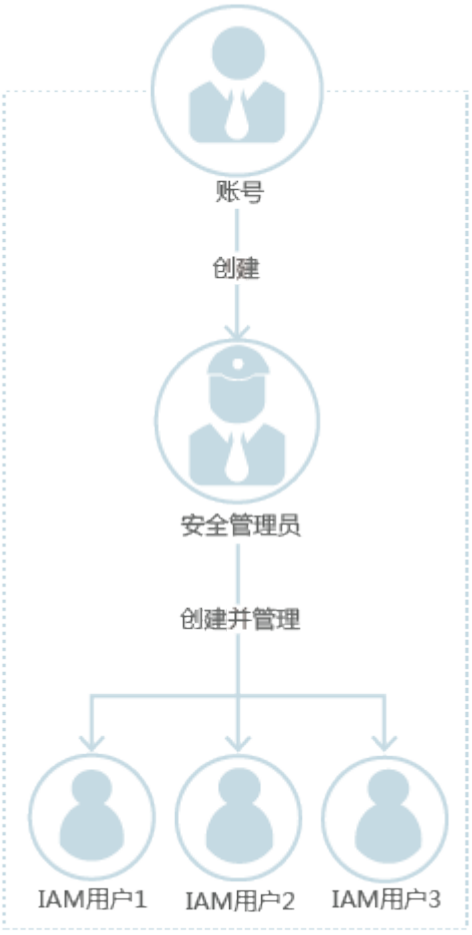
您可以通过IAM管理您账号中的用户及其安全凭证，也可以通过IAM的联邦身份认证让其他系统的用户直接访问系统，实现单点登录，让用户管理更简单。

账号

用户注册后自动创建，该账号对其所拥有的资源具有完全的访问权限。

为了确保账号的安全性，建议您为自己的账号创建安全管理员（具有Security Administrator权限），使用安全管理员管理账号中的用户及其权限。

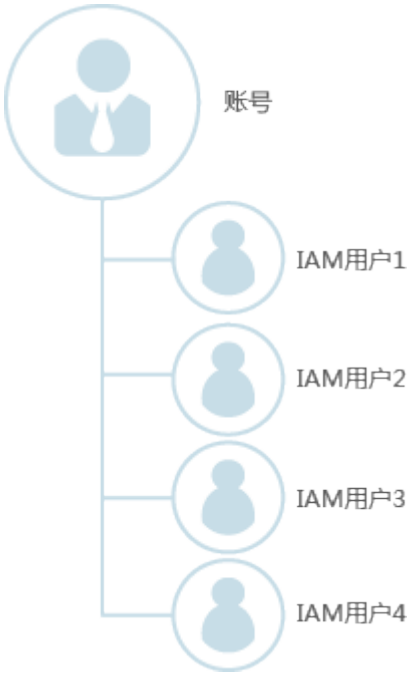
图 1-2 账号管理模型



IAM 用户

由管理员在IAM中创建的用户，是云服务的使用人员，对应员工、系统或应用程序，具有身份凭证（密码和访问密钥），可以登录管理控制台或者访问API。

图 1-3 账号与 IAM 用户的关系



联邦用户

通过联邦身份认证方式登录的用户称为联邦用户。

联邦身份认证是指用户通过身份提供商认证后，不需要通过服务提供商再次认证即可访问服务提供商的资源。

- 身份提供商（Identity Provider，简称IdP ）是为用户提供身份认证的系统。在IAM联邦身份认证中身份提供商指企业自身的身份认证系统（如：企业管理系统）。
- 服务提供商（Service Provider，简称SP）是指为用户提供服务的系统。

IdP的用户通过联邦身份认证访问时，仅需要使用IdP提供的安全凭证（无需IAM为其生成新的安全凭证）即可访问系统，即实现单点登录。

1.4 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 1-1 IAM 系统权限

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

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

说明

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

表 1-2 常用操作与系统权限的关系

操作	Security Administrator	Agent Operator	FullAccess	IAM ReadOnlyAccess
创建IAM用户	√	×	√	×
查询IAM用户详情	√	×	√	√
修改IAM用户信息	√	×	√	×
查询IAM用户安全设置	√	×	√	√
修改IAM用户安全设置	√	×	√	×
删除IAM用户	√	×	√	×
创建用户组	√	×	√	×
查询用户组详情	√	×	√	√
修改用户组信息	√	×	√	×
添加用户到用户组	√	×	√	×
从用户组移除用户	√	×	√	×
删除用户组	√	×	√	×
为用户组授权	√	×	√	×
移除用户组权限	√	×	√	×
创建自定义策略	√	×	√	×
修改自定义策略	√	×	√	×

操作	Security Administrator	Agent Operator	FullAccess	IAM ReadOnlyAccess
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	√	×	√	×
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	√	×	√	×

操作	Security Administrator	Agent Operator	FullAccess	IAM ReadOnlyAccess
删除协议	√	×	√	×
删除映射	√	×	√	×
查询配额	√	×	√	×

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

表 1-3 访问密钥操作与系统权限的关系

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

FullAccess 策略内容

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

IAM ReadOnlyAccess 策略内容

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

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

Security Administrator 角色内容

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

Agent Operator 角色内容

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

Tenant Guest 角色内容

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



```
            }
        },
        "Action": [
            "*:*:get*",
            "*:*:list*",
            "*:*:head*"
        ],
        "Effect": "Allow"
    }
  ]
}
```

Tenant Administrator 角色内容

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

1.5 个人数据保护机制

为了确保用户的个人数据（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，保证用户个人数据的安全。

收集范围

IAM收集及产生的个人数据如表1-4所示：

表 1-4 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

类型	收集方式	是否可以修改	是否必须
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 用户可以选择使用密码或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，可以通过删除后新建的方式修改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。

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，可以重新创建AK/SK，无法通过界面或者接口重新获取该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。

2 快速入门

2.1 快速使用 IAM

账号具有所有资源的完全访问权限，为了确保账号安全，建议您不要使用账号进行日常管理工作，而是创建安全管理员并使用安全管理员进行日常管理工作。

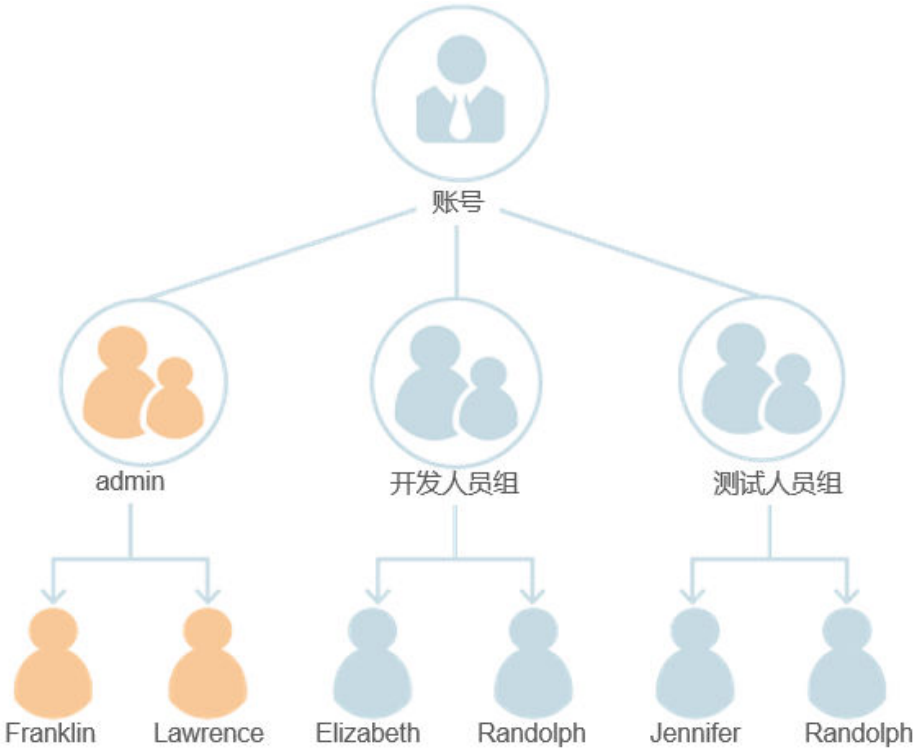
如果其他用户需要访问您账号中的资源，您可以使用安全管理员创建单独的IAM用户和最小权限的用户组，再将用户加入用户组中，使用户具有用户组中的权限，这些用户可以使用您新创建的IAM用户，使用自己单独的安全凭证（用户名/密码）根据权限访问系统，避免和其他用户共享您的账号密码，降低安全风险。

示例

通过如下示例帮助您快速了解如何使用IAM。

账号中有3种职责的用户，一个职责对应一个用户组：安全管理员组（名称为admin）、开发人员用户组和测试人员用户组。每个用户组可以有多个用户，同一个用户也可以属于多个用户组。

图 2-1 用户管理模型



1. 使用您的账号创建一个安全管理员（Franklin），并将Franklin加入到缺省用户组“admin”中。
2. 您的安全管理员（Franklin）使用自己的账号登录，创建其他安全管理员（Lawrence），并将Lawrence加入到缺省用户组“admin”中。
3. 由安全管理员（Franklin或Lawrence）创建用户组“开发人员组”和“测试人员组”并分别为两个用户组授予职责所需的最小权限。
4. 由安全管理员（Franklin或Lawrence）创建开发人员用户（Elizabeth、Randolph），并将Elizabeth和Randolph加入到“开发人员组”用户组中；创建测试人员用户（Jennifer、Randolph），并将Jennifer和Randolph加入到“测试人员组”用户组中。
5. 用户（Elizabeth、Jennifer和Randolph）使用自己的用户登录系统。

说明

安全管理员和用户都是IAM用户，根据加入的用户组不同，具有不同的权限。它们都具有单独的安全凭证（用户名/密码），可以登录系统。

2.2 创建安全管理员

为了确保安全性，建议您为自己创建安全管理员来代替使用账号管理用户。

说明

仅有管理员权限的云联盟用户可以在IAM中创建和管理用户，其他用户必须使用**the Cloud Customer Space**创建用户。在Customer Space的“Right”页面中，单击“添加用户”按钮，详情可参考**如何添加用户**。有关the Cloud Customer Space的更多帮助，请访问**Flexible Engine Assistance Page**。

操作步骤

步骤1 选择“管理与部署 > 统一身份认证服务”。

步骤2 在左侧导航窗格中，单击“用户”。

步骤3 在“用户”界面，单击“创建用户”。

步骤4 在“创建用户”界面，输入“用户名”。

步骤5 选择“凭证类型”为“API密码”。

说明

- API密码用于登录管理控制台，也可以用于API、CLI、SDK等开发工具进行认证，认证成功后可以访问资源。安全管理员用于管理用户，因此建议您选择“凭证类型”为。
- 访问密钥用于API、CLI、SDK等开发工具认证，完成认证后可以访问资源。

步骤6 在“所属用户组”的下拉复合框中，选择“admin”内置用户组。

步骤7 单击“下一步”。

步骤8 选择“密码生成方式”为“自定义”。

说明

安全管理员用于登录管理控制台管理用户。如果您为自己创建安全管理员，建议使用自定义方式设置密码。如果您为他人创建安全管理员，建议使用“首次登录时设置”的方式，由用户自己设置密码。

步骤9 “是否重置密码”：安全管理员需要创建一个新密码登录系统。该功能默认勾选，为了管理员账号安全，建议保持默认勾选状态，保证该管理员账号的密码为管理员本人所设置，防止密码泄露。

步骤10 输入邮箱、手机、API密码和确认密码。

说明

- 建议您为管理员设置邮箱或手机号码，作为安全管理员的凭证。
- 密码必须满足如下复杂度要求：
  - 不能少于6个字符且不超过32个字符。
  - 必须满足**密码设置策略**要求。
  - 包括大写字母（A~Z），小写字母（a~z），数字（0~9）和特殊字符（~`!?,.:;-_'"(){}[]/<>@#$%^&*+|\=和空格）至少2种的组合。
  - 不能是用户名或者用户名的倒序（不区分大小写），例如：用户名为A12345，则密码不能为A12345、a12345、54321A和54321a。

步骤11 单击“确定”。

----结束

2.3 创建用户组并授权

您可以根据用户职责规划用户组。使用安全管理员访问IAM并创建用户组，再根据职责赋予用户组对应的权限。

操作步骤

步骤1 选择“管理与部署 > 统一身份认证服务”。

步骤2 在左侧导航窗格中，单击“用户组”。

步骤3 在“用户组”界面中，单击“创建用户组”。

步骤4 输入“用户组名称”。

步骤5 （可选）输入“描述”。

说明

建议给用户组添加描述，比如给用户组授予Security Administrator权限，可以在描述中添加“Security Administrator：创建、删除、修改用户并为用户授权”或者自定义内容，方便用户直观的查看自己所具备的权限及权限作用。具体权限描述信息请参见：权限集。

步骤6 单击“确定”。

返回用户组列表，用户组列表中显示新创建的用户组。

步骤7 单击新建用户组右侧的“修改”。

步骤8 在“用户组权限”中，单击需要授权项目右侧的“修改”。

说明

授予的权限仅对当前项目生效。如果需要为用户组授予多个项目的权限，请分别单击所需要授权的项目右侧的“修改”进行授权。

步骤9 给新建用户组选择策略。

说明

您也可以通过输入关键字快速找到相关策略。

步骤10 单击“确定”。

----结束

2.4 创建用户并加入用户组

您可以使用安全管理员创建用户并将用户加入到对应的用户组中，使其继承用户组中的权限。

说明

仅有管理员权限的云联盟用户可以在IAM中创建和管理用户，其他用户必须使用**the Cloud Customer Space**创建用户。在Customer Space的“Right”页面中，单击“添加用户”按钮，详情可参考**如何添加用户**。有关the Cloud Customer Space的更多帮助，请访问**Flexible Engine Assistance Page**。

操作步骤

步骤1 选择“管理与部署 > 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”>“创建用户”。

步骤3 在“创建用户”界面，输入“用户名”。

步骤4 选择“凭证类型”。

凭证类型	适用场景
API密码	• 登录管理控制台。 • 使用支持密码认证的API、CLI、SDK等开发工具来访问云服务。
访问密钥	使用支持密钥认证的API、CLI、SDK等开发工具来访问云服务。

步骤5 在“所属用户组”的下拉框中，选择需要加入的用户组。

说明

- 您也可以通过输入关键字快速找到相关用户组。
- 一个用户可以同时加入多个用户组。

根据步骤4中选择的凭证类型，进行后续操作。

凭证类型	后续操作
API密码	请执行6。
访问密钥	单击“确认”。下载生成的密钥，创建用户操作完成。 **说明** 访问密钥是在IAM中认证的凭证，如果不下载生成的密钥则无法获取对应的访问密钥。如果该用户需要使用访问密钥在IAM中认证，需要重新生成。

步骤6 单击“下一步”。选择“密码生成方式”。

密码生成方式	说明	后续操作
首次登录时设置	系统会通过邮件发送一次性登录链接给用户。用户使用该链接登录管理控制台时设置密码。	1. 输入“邮箱”。用于接收登录链接。 2. （可选）输入“手机”。
自动生成	由系统随机生成10位密码。适用于使用支持密码认证的API、CLI、SDK等开发工具来访问云服务。	1. （可选）输入“邮箱”。 2. （可选）输入“手机”。

密码生成方式	说明	后续操作
自定义	自定义用户的登录密码。	1. （可选）输入“邮箱”。 2. （可选）输入“手机”。 3. 输入“密码”和“确认密码”。 **说明** 密码必须满足如下复杂度要求： • 不能少于6个字符且不超过32个字符。 • 必须满足**密码设置策略**要求。 • 包括大写字母（A~Z），小写字母（a~z），数字（0~9）和特殊字符（~`!?,.:;-_'"(){}[]/<>@#$%^&*+|\=和空格）至少2种的组合。 • 不能是用户名或者用户名的倒序（不区分大小写），例如：用户名为A12345，则密码不能为A12345、a12345、54321A和54321a。

步骤7 “是否重置密码”：用户需要创建一个新密码登录系统。该功能默认勾选，为了用户账号安全，建议保持默认勾选状态，保证该账号的密码为用户本人所设置，防止密码泄露。

步骤8 单击“确定”。

创建用户完成。

----结束

2.5 使用新创建的用户登录控制台

您可以使用在IAM中新创建的用户登录系统，并根据权限访问云服务。

背景信息

当开启以下任一功能时，您登录成功后，将进入“登录验证”页面，请单击“确定”进入管理控制台。

- “安全设置”的“登录验证策略”中开启“最近登录提示”功能。
- “安全设置”的“登录验证策略”中设置“登录验证提示”信息。

操作步骤

步骤1 在Orange Cloud for Business登录界面，单击右上角的“API登录”。

步骤2 输入“账户名”、“用户名/邮箱/电话号码”和“API密码”，并单击“登录”。

说明

- 账户名是您在Orange Cloud for Business注册时的名称，用户名是在IAM创建用户时的名称。
- 您首次登录时，需在“首次登录”页面修改初始密码，定期修改密码可以提高账号的安全性。
- 如果开启了登录验证功能，您在“登录验证”页面还需输入验证码进行验证。

登录成功后，进入管理控制台。

----结束

3 用户指南

3.1 IAM 用户

3.1.1 创建用户

当您需要与新用户共享您账号中的资源时，您可以在控制台或通过调用API接口创建IAM用户。创建用户时可以设置安全凭证和权限。已创建的用户可以通过管理控制台或调用API访问系统。

说明

仅有管理员权限的云联盟用户可以在IAM中创建和管理用户，其他用户必须使用**the Cloud Customer Space**创建用户。在Customer Space的“Right”页面中，单击“添加用户”按钮，详情可参考**如何添加用户**。有关the Cloud Customer Space的更多帮助，请访问**Flexible Engine Assistance Page**。

操作步骤

步骤1 在统一身份认证服务的左侧导航窗格中，单击“用户”。

步骤2 在“用户”界面，单击“创建用户”。

步骤3 在“创建用户”界面，输入“用户名”。

步骤4 选择“凭证类型”。

凭证类型	适用场景
API密码	• 登录管理控制台。 • 使用支持密码认证的API、CLI、SDK等开发工具来访问云服务。
访问密钥	使用支持密钥认证的API、CLI、SDK等开发工具来访问云服务。

步骤5 在“所属用户组”的下拉框中，选择需要加入的用户组。

说明

- 您也可以通过输入关键字快速找到相关用户组。
- 一个用户可以同时加入多个用户组。

根据步骤4中选择的凭证类型，进行后续操作。

凭证类型	后续操作
API密码	请执行6。
访问密钥	单击“确认”。下载生成的密钥，创建用户操作完成。 **说明** 访问密钥是在IAM中认证的凭证，如果不下载生成的密钥则无法获取对应的访问密钥。如果该用户需要使用访问密钥在IAM中认证，需要重新生成。

步骤6 单击“下一步”。选择“密码生成方式”。

密码生成方式	说明	后续操作
首次登录时设置	系统会通过邮件发送一次性登录链接给用户。用户使用该链接登录管理控制台时设置密码。 该链接的有效期为7天，请提醒用户及时登录并设置密码。	1. 输入“邮箱”。用于接收登录链接。 2. （可选）输入“手机”。 3. 单击“确定”。
自动生成	由系统随机生成密码。适用于使用支持密码认证的API、CLI、SDK等开发工具来访问云服务。	1. （可选）输入“邮箱”。 2. （可选）输入“手机”。 3. 单击“确定”。 4. 下载密码文件。

密码生成方式	说明	后续操作
自定义	自定义用户的登录密码。	1. （可选）输入“邮箱”。 2. （可选）输入“手机”。 3. 输入“密码”和“确认密码”。 **说明** 密码必须满足如下策略： – 不能少于6个字符且不超过32个字符。 – 包括大写字母（A~Z），小写字母（a~z），数字（0~9）和特殊字符（~`!?,.:;-_'"(){}[]/<>@#$%^&*+|\=和空格）至少2种的组合。 – 不能是用户名或者用户名的倒序（不区分大小写），例如：用户名为A12345，则密码不能为A12345、a12345、54321A和54321a。 – 不能包含手机号或邮箱。 4. 单击“确定”。

说明

- 用户可以使用此处设置的用户名、邮箱或手机号码任意一种方式登录系统。
- 当用户忘记密码时，可以通过此处绑定的邮箱或手机号码来重置密码。

步骤7 “是否重置密码”：用户下次登录时需要创建一个新密码，保证该用户的密码是由使用者本人所设置，防止密码泄露。该功能默认勾选，为了账号安全，建议保持默认勾选状态。

步骤8 单击“确定”。

创建用户完成。

----结束

相关任务

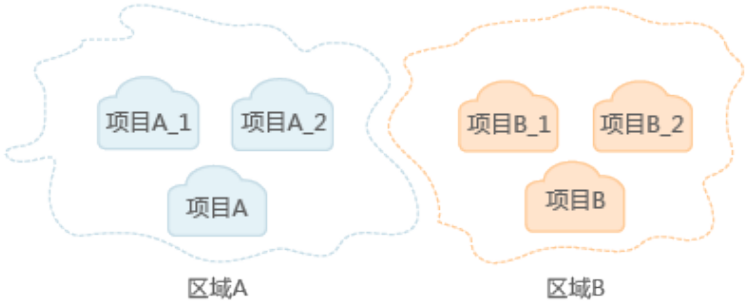
- 查看用户信息和修改用户信息（包括用户状态、绑定的邮箱、手机号码、所属用户组、用户日志等）。
- 删除用户：在用户列表中，单击“删除”。

3.1.2 管理用户及其权限

您可以通过为用户组授权并将用户加入到用户组的方式，使用户具有用户组中的权限，用户可以根据权限访问系统。

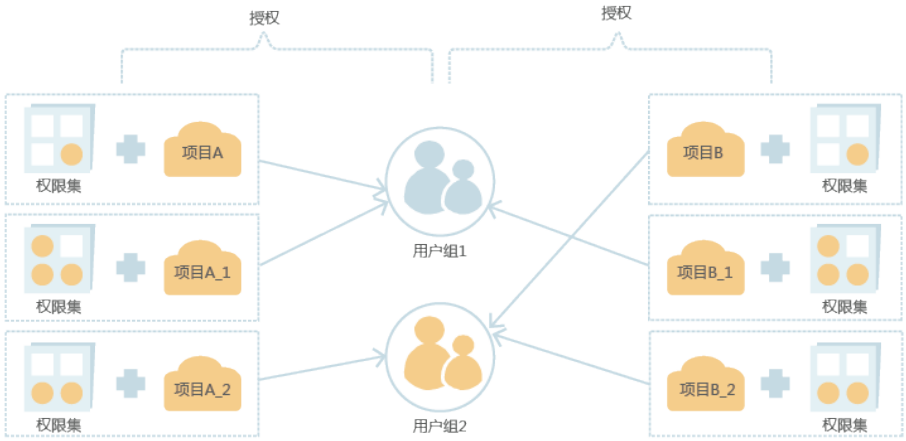
步骤1 安全管理员在区域下创建项目，使得各项目之间相互隔离。

图 3-1 项目隔离模型



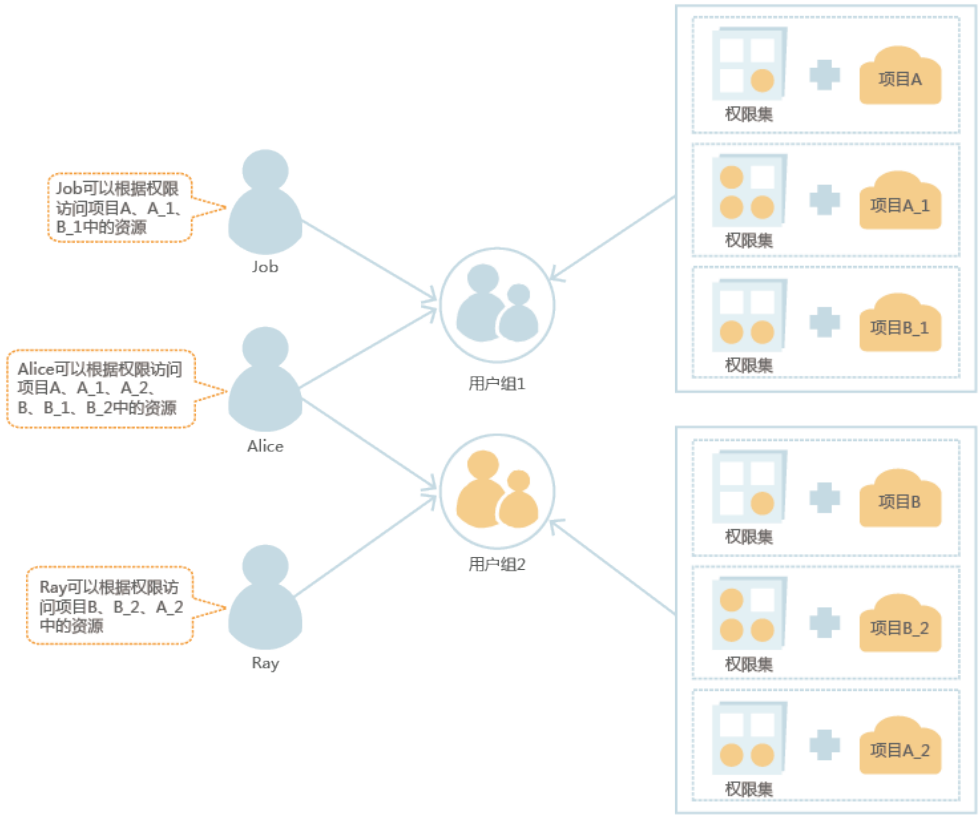
步骤2 安全管理员按照用户职责规划用户组并为用户组授权。

图 3-2 用户组授权模型



步骤3 安全管理员创建用户并根据用户职责将用户加入到对应的用户组中。

图 3-3 用户授权模型



步骤4 用户根据权限访问系统。

----结束

3.1.3 查看或修改用户信息

查看用户信息

在用户列表中，可以单击对应用户左侧的下拉框，查看用户的详细信息。包括基本信息、所属用户组以及用户日志。

修改用户信息

在用户列表中，单击对应用户右侧的“修改”，进入“修改用户”界面。

- 修改用户状态：用户默认为“启用”状态，如果需要停止使用该用户，可以将用户的“状态”为设置为“停用”。
- 修改登录验证方式
  - 虚拟MFA：只有用户绑定了MFA应用程序，才能将用户的登录验证方式修改为虚拟MFA。修改后，用户登录系统时需要在“登录验证”页面输入虚拟MFA验证码。
  - 手机：只有用户绑定了手机，才能将用户的登录验证方式修改为手机。修改后，用户登录系统时需要在“登录验证”页面输入手机验证码。
  - 邮箱：只有用户绑定了邮箱，才能将用户的登录验证方式修改为邮箱。修改后，用户登录系统时需要在“登录验证”页面输入邮箱验证码。

- 修改手机、邮箱、描述。
- 绑定虚拟MFA：给用户绑定或者解绑虚拟MFA设备。
- 修改所属用户组：在“所属用户组”区域的下拉框中选择要加入的用户组，或者单击目标用户组右侧的“删除”，退出选中的用户组。

说明

您也可以通过输入关键字快速找到相关用户组。

设置用户凭证

在用户列表中，单击右侧“设置凭证”，可修改用户的API密码或管理用户的访问密钥。

凭证类型	生成方式	说明	适用场景
API密码	通过邮箱设置	系统会通过邮件发送一次性登录链接给用户，用户使用该链接登录管理控制台时设置密码。	已绑定邮箱的用户重置API密码。该用户需要使用密码登录管理控制台。
	自动生成	由系统随机生成10位API密码。 **说明** 自动生成的密码可以在单击“确认”后下载。	使用支持密码认证的API、CLI、SDK等开发工具通来访问系统的用户重置密码。
	自定义	自定义用户的API密码。	任何用户。
访问密钥	用户自己创建或通过安全管理员创建	在“管理访问密钥”区域，可新增或删除访问密钥。 **说明** 每个用户最多可创建2个访问密钥，有效期为360天。为了账号安全性，建议您妥善保管访问密钥。	通过访问密钥认证访问系统的用户。

- “是否重置密码”：用户下次登录时需要创建一个新密码，保证该用户的密码是由使用者本人所设置，防止密码泄露。该功能默认勾选，为了账号安全，建议保持默认勾选状态。
- 登录失败次数清零

  在用户列表中，单击右侧“失败清零”，可清零该用户登录失败的次数，解锁被锁定的用户。

说明

当管理员账号（该账号不能被修改）被锁定时，请联系工程师处理。

3.1.4 修改用户权限

修改用户权限的方法有以下两种：

- 通过修改用户功能，修改用户所属用户组。该方法适用于调整单个用户权限变化。方法请参考**查看或修改用户信息**。
- 通过修改用户组功能，修改用户组权限或修改用户组中包含的用户。该方法适用于将多个用户加入到同一用户组中，或将多个用户从同一用户组中删除。方法请参考：**查看或修改用户组**。

3.1.5 切换项目或区域

不同项目或区域中的资源互相隔离，您仅能访问被授权项目或区域下的资源。如果您不具备当前项目或区域下的权限，请先切换到被授权的项目或区域下。

操作步骤

步骤1 在系统首页，单击“控制台”。

步骤2 在控制台页面左上角的下拉框中，选择需要访问的项目或区域。

切换至目标项目或区域即可访问对应的资源。

----结束

3.2 用户组及授权

3.2.1 创建用户组并授权

您可以根据用户职责规划用户组，并赋予用户组对应职责的权限，使得用户组中的用户拥有对应职责的权限。通过用户组来管理用户权限可以使权限管理更有条理。

操作步骤

步骤1 在统一身份认证服务的左侧导航窗格中，单击“用户组”。

步骤2 在“用户组”界面中，单击“创建用户组”。

步骤3 输入“用户组名称”。

步骤4 （可选）输入“描述”。

说明

建议给用户组添加描述，比如给用户组授予Security Administrator权限，可以在描述中添加“Security Administrator：创建、删除、修改用户并为用户授权”或者自定义内容，方便用户直观的查看自己所具备的权限及权限作用。具体权限描述信息请参见：权限集。

步骤5 单击“确定”。

返回用户组列表，用户组列表中显示新创建的用户组。

步骤6 单击新建用户组右侧的“修改”。

步骤7 在“用户组权限”中，单击需要授权项目右侧的“修改”。

说明

授予的权限仅对当前项目生效。如果需要为用户组授予多个项目的权限，请分别单击所需要授权的项目右侧的“修改”进行授权。

步骤8 给新建用户组选择策略。

说明

您也可以通过输入关键字快速找到相关策略。

步骤9 单击“确定”。

----结束

3.2.2 查看或修改用户组

安全管理员可以查看和修改用户组的基本信息、权限及用户组中包含的用户。当用户权限发生变化时可以通过修改用户组的方式快速完成用户权限修改。

操作步骤

步骤1 在统一身份认证服务的左侧导航窗格中，单击“用户组”。

步骤2 在“用户组”列表中，可以查看或修改用户组信息。

- 查看用户组信息

  在用户组列表中，单击对应用户组左侧的 ，可以查看用户组的详细信息。包括基本信息、用户组权限以及用户组中包含的用户。

- 修改用户组信息

  在用户组列表中，单击对应用户组右侧的“修改”，进入“修改用户组”界面。

  说明

  - 系统缺省用户组，只能修改其中包含的用户，不能修改基本信息与权限。
  - 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。

修改信息	修改方法
用户组权限	1. 单击需要授权项目“操作”列的“修改”。 2. 在“可选择策略”区域中选择策略。 3. 单击“确定”。
用户组中包含的用户	– 增加用户 在“包含用户”区域的下拉列表中选择需要加入的用户。 **说明** 您也可以通过输入关键字快速找到相关用户。 – 删除用户 在“包含用户”区域的删除对应用户。

----结束

3.2.3 依赖角色的授权方法

由于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。

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 单击勾选权限下方的 ，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5 单击“确定”，完成依赖角色的授权。

----结束

3.3 权限管理

3.3.1 细粒度策略

细粒度授权策略是描述一组权限集的语言，它可以精确地描述对授权云服务可以执行的操作。通过策略，用户可以自由搭配需要授予的权限集。通过给用户组授予策略，用户组中的用户就能获得策略中定义的权限。IAM通过策略定义的权限内容实现精细的权限管理。

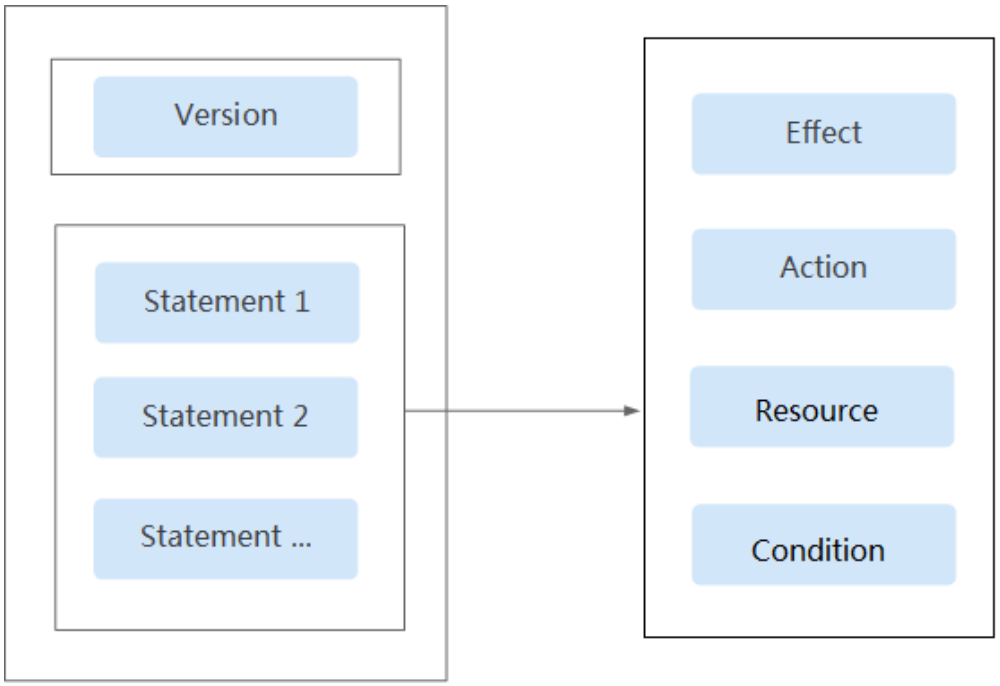
IAM支持以下两种形式的策略：

- 系统策略：系统预置的常用权限集，主要针对不同云服务的只读权限或管理员权限，比如对ECS的只读权限、对ECS的管理员权限等；系统策略只能用于授权，不能编辑和修改。
- 自定义策略：由用户自己创建和管理的权限集，是对系统策略的扩展和补充。

3.3.2 策略语言说明

策略内容

细粒度授权策略内容包括策略版本号（Version）及策略授权语句（Statement）列表。



- 策略版本号：Version，标识策略的版本号，主要用于区分Role-Based Access Control策略和细粒度策略。
  - 1.0：Role-Based Access Control（RBAC）)策略。RBAC策略是将服务作为一个整体进行授权，授权后，用户可以拥有这个服务的所有权限，RBAC策略只能由系统预置。
  - 1.1：细粒度策略。相比RBAC策略，细粒度策略基于服务的API接口进行权限拆分，授权更加精细。授权后，用户可以对这个服务执行特定的操作。细粒度策略包括系统预置和用户自定义两种：
    - 系统预置策略：系统预置服务常用的权限集，包括服务的只读权限或管理员权限。
    - 用户自定义策略：由用户自己创建和管理的权限集，是对系统策略的扩展和补充。例如：针对ECS服务，控制用户仅能变更云服务器规格。
- 策略授权语句：Statement，描述的是策略的详细信息，包含作用（Effect）、授权项（Action）、资源类型（Resource）、条件（Condition）。
  - 作用（Effect）

    作用包含两种：允许（Allow）和拒绝（Deny），一个自定义策略中可以同时包含允许和拒绝的授权语句，当策略中既有允许又有拒绝的授权语句时，遵循Deny优先的原则。
  - 授权项（Action）

    对资源的具体操作权限，支持单个或多个操作权限。

    格式为：服务名:资源类型:操作，例如：vpc:ports:create。
  - 资源类型（Resource）

    策略所作用的资源。

    格式为：服务名:region:domainId:资源类型:资源路径, 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（Condition）

使策略生效的特定条件，包括条件键和运算符。条件键表示策略语句的Condition 元素中的键值，分为**全局级条件键**和服务级条件键（由云服务定义，请参见云服务帮助中心）。全局级条件键（前缀为g:）适用于所有操作，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。运算符与条件键一起使用，构成完整的条件判断语句。

格式为：条件运算符: {条件名：[条件值1, 条件值2]}。

示例:

- "StringEndWithIfExists":{"g:UserName":["specialCharactor"]}：表示当用户输入的用户名以"specialCharactor"结尾时该条statement生效。

表 3-1 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: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

说明

- 服务名：产品名称，例如ecs、evs和vpc等，服务名仅支持小写。
- 资源类型和操作没有大小写要求，支持通配符号*，用户不需要罗列全部授权项，通过配置通配符号*可以方便快捷地实现授权。

策略样例

- 支持单个操作权限，例如：查询弹性云服务器详情权限

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ecs:servers:list",
```



```
                "ecs:servers:get",
                "ecs:serverVolumes:use",
                "ecs:diskConfigs:use",
                "ecs:securityGroups:use",
                "ecs:serverKeypairs:get",
                "vpc:securityGroups:list",
                "vpc:securityGroups:get",
                "vpc:securityGroupRules:get",
                "vpc:networks:get",
                "vpc:subnets:get",
                "vpc:ports:get",
                "vpc:routers:get"
            ]
        }
    ]
}
```

- 支持多个操作权限，例如：锁定云服务器和创建云硬盘权限。

```
{
   "Version": "1.1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ecs:servers:lock",
                "evs:volumes:create"
            ]
        }
    ]
}
```

- 通配符号*用法示例：对IMS服务资源的所有权限。

```
{
      "Version": "1.1",
      "Statement": [
            {
                  "Action": [
                        "ims:*:*",
                        "ecs:*:list",
                        "ecs:*:get",
                        "evs:*:get"
                  ],
                  "Effect": "Allow"
            }
      ]
}
```

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



```
    ]
}
```

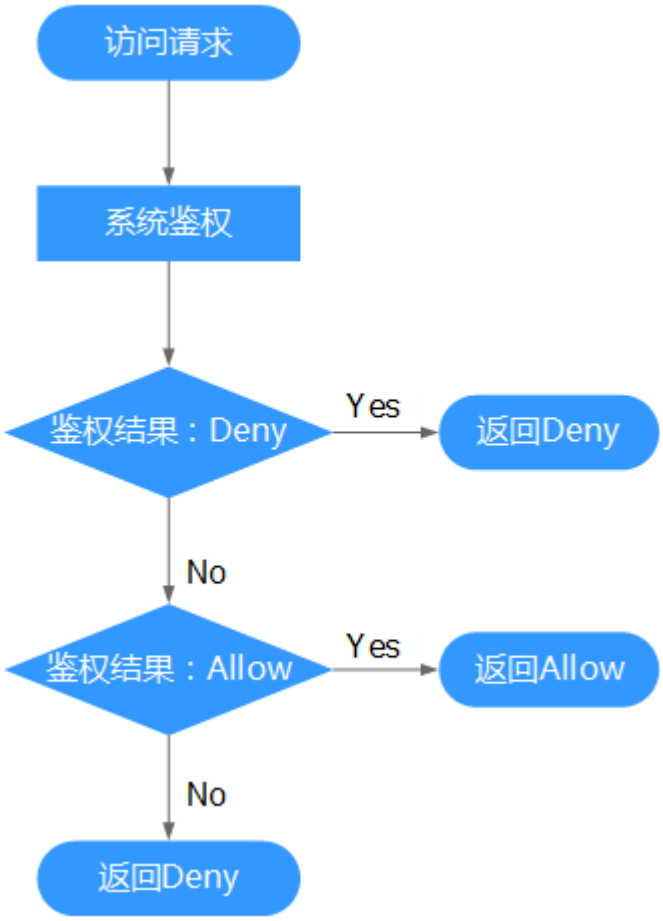
说明

当前仅部分服务支持资源级授权，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。

检查规则

系统根据用户被授予的策略，对用户进行鉴权。系统鉴权逻辑如下：

图 3-4 系统鉴权逻辑图



说明

每条策略做评估时， Action之间是或(or)的关系。

1. 用户访问系统，发起操作请求。
2. 系统评估用户被授予的访问策略，鉴权开始。
3. 在用户被授予的访问策略中，系统将优先寻找显式拒绝指令。如找到一个适用的显式拒绝，系统将返回Deny决定。
4. 如果没有找到显式拒绝指令，系统将寻找适用于请求的任何Allow指令。如果找到一个显式允许指令，系统将返回Allow决定。
5. 如果找不到显式允许，最终决定为Deny，鉴权结束。

3.3.3 创建自定义策略

系统预置的权限不能满足要求时，您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。

可视化视图配置自定义策略

步骤1 在统一身份认证服务的左侧导航窗格中，单击“策略”>“创建自定义策略”。

步骤2 输入“策略名称”。

步骤3 “策略配置方式”选择“可视化视图”。

步骤4 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。
3. 选择“操作”，根据需求勾选产品权限。
4. 选择资源类型，如选择“特定类型”可以单击“通过资源路径指定”来指定需要授权的资源。
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 3-2 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，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。
运算符	与条件键一起使用，构成完整的条件判断语句。
值	与条件键和运算符一起使用，当运算符需要某个关键字时，需要输入关键字的值，构成完成的条件判断语句。

步骤5 （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6 （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7 输入“策略描述”（可选）。

步骤8 单击“确定”，自定义策略创建完成。

步骤9 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。

----结束

JSON 视图配置自定义策略

步骤1 在统一身份认证服务的左侧导航窗格中，单击“策略”>“创建自定义策略”。

步骤2 输入“策略名称”。

步骤3 “策略配置方式”选择“JSON视图”。

步骤4 （可选）在“策略内容”区域，单击“从已有策略复制”，例如选择“VPC Admin”作为模板。

步骤5 单击“确定”。

步骤6 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授权项列表中“授权项”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7 （可选）输入“策略描述”。

步骤8 单击“确定”，自定义策略创建完成，策略列表中显示新创建的策略。

步骤9 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。

----结束

3.3.4 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:*:*"：表示对费用中心的所有操作。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“ECS FullAccess”，但不希望用户拥有ECS FullAccess中的删除云服务器权限（ecs:cloudServers:delete），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ECS 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ECS执行除了删除云服务器外的所有操作。

  以下策略样例表示：拒绝IAM用户删除云服务器。

```
{
   "Version": "1.1",
   "Statement": [
      {
         "Effect": "Deny",
         "Action": [
               "ecs:cloudServers:delete"
         ]
      }
   ]
}
```

- 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、AOM、ELB

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

- 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、AOM、ELB外的其他所有服务。

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



```
                "Effect": "Deny"
            }
        ]
}
```

3.4 设置账号安全策略

拥有安全管理员权限（Security Administrator权限）的用户可以设置登录验证策略、API密码策略、访问控制列表来提高用户信息和系统的安全性。

操作步骤

步骤1 设置登录验证策略。

1. 在左侧导航窗格中，选择“>登录验证策略”
2. 在“账号锁定策略”区域输入“限定时间长度”、“限定时间内登录失败次数”、“账号锁定时长”。

   如果在限定时间长度内达到登录失败次数后，账号会被锁定一段时间。如：在10分钟内连续3次登录失败，用户会被锁定15分钟。15分钟后可以尝试再次登录。
3. 在“账号停用策略”区域，选中“如果账号在有效期内未使用过，则将被停用”，设置“账号有效期限”。如果在设置的有效期限内，用户没有通过管理控制台或者API接口访问系统，账号将会被停用。

   “账号停用策略”为账号安全保护策略，账号被停用后，不影响账号内的资源使用，用户可以联系管理员重新启用账号。
4. 在“会话超时策略”区域，设置“会话超时时长”，会话超时时长默认为15分钟，用户可以在15分钟至24小时的范围内进行设置，若用户超过设置的时长未操作界面，需要重新登录。
5. 在“最近登录提示”区域中，选中“登录成功时，将看到上次登录的时间等信息”。

   用户将在登录时的“登录验证”页面中看到上次登录的时间等登录提示信息。
6. 在“最近验证提示”区域，自定义登录时的验证信息。

   用户将在“登录验证”页面中看到自定义的验证提示信息。
7. 单击“确定”。

步骤2 设置密码策略。

1. 在左侧导航窗格中，选择“>密码策略” 。
2. 在“密码设置策略”区域中，进行如下设置：
   - 设置“密码最小长度”。

     说明

     系统默认值为6个字符。
   - 选择“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，可以在1~32之间设置。
   - 选择“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，可以在1~10之间设置。
3. 在“密码有效期策略”区域中，选择“密码过期后，系统强制要求修改密码。（距离密码到期15天时开始提示用户修改密码。）”，设置“密码有效期”。

   密码过期后，用户必须根据系统提示修改密码，否则无法登录系统。

说明

密码必须满足如下策略：

- 不能少于6个字符且不超过32个字符。
- 包括大写字母（A~Z），小写字母（a~z），数字（0~9）和特殊字符（~`!?,.:;-_'"(){}[]/<>@#$%^&*+|\=和空格）至少2种的组合。
- 不能是用户名或者用户名的倒序（不区分大小写），例如：用户名为A12345，则密码不能为A12345、a12345、54321A和54321a。
- 不能包含手机号或邮箱。

4. 在“密码最短使用时间策略”区域中，选择“密码初次生成和每次修改之后，密码的使用时间必须超过设置的最短使用时间，才能进行修改”，设置“密码最短使用时间”。

   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。

5. 单击“应用”。

步骤3 设置访问控制列表。

1. 在左侧导航窗格中，选择“>访问控制列表”。
2. 在“访问控制列表”界面中，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地址登录系统。
   - “允许访问的IP地址或网段”：限制用户只能从设定的IP地址或网段登录系统。例如：10.10.10.10/32。

   说明

   - 设置访问控制列表仅对账号下的IAM用户生效，对账号本身不生效。
   - 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，默认值0.0.0.0~255.255.255.255，同时将“允许访问的IP地址或网段”清空。
   - “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。
3. 单击“应用”。

----结束

3.5 项目

项目用于将OpenStack的资源（计算资源、存储资源和网络资源）进行分组和隔离。您账号中的资源必须挂载在项目下，项目可以是一个部门或者项目组。您可以使用安全管理员访问IAM，并在区域下创建项目，来实现资源的隔离管理。

操作步骤

步骤1 在统一身份认证服务的左侧导航窗格中，单击“项目”。

步骤2 在“项目”界面，单击“创建项目”。

步骤3 在“所属区域”下拉列表中选择待创建项目所属的区域。

步骤4 输入“项目名称”。

说明

- 项目名称的格式为：*区域名称_项目名称*，区域名称不允许修改。
- 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5 （可选）输入“描述”。

步骤6 单击“确定”。

返回项目列表，新创建的项目“状态”显示为“正常”。

----结束

后续处理

给项目授权

在“用户组详情”界面，“用户组权限”区域中，单击目标项目右侧的“修改”，给对应项目选择需要的权限集。详情请参见**创建用户组并授权**。

相关任务

- 查看项目的详细信息
  a. 在项目列表查看对应区域下面的项目。
  b. 在“操作”列单击对应项目的“查看”。
     查看项目的详细信息以及绑定在该项目上面的用户。

     说明

     通过为用户组授予对应项目的权限，再将用户加入到用户组中，使用户继承用户组的权限，并实现用户与项目之间的绑定。用户通过切换项目来访问对应的资源。
  c. 单击用户权限列表“权限”列的“查看”。
     查看绑定在项目上面的用户对应的权限。
- 修改项目
  a. 在项目列表单击待修改项目所属区域前的加号图标。
  b. 在“操作”列单击对应项目的“修改”，在“修改项目”页面修改项目名称和描述信息。

     说明

     项目名称的格式为：*区域名称_项目名称*，区域名称不允许修改。
- 删除项目
  a. 单击待删除项目右侧的“删除”。

     说明

     只有区域下创建的项目可以删除，区域对应的项目不能删除。
  b. 输入“登录密码”和对应验证码。
  c. 单击“确定”。
     返回项目列表，待删除项目的状态显示为“删除中”。

> **说明**
>
> 系统删除项目中的资源后，将会彻底删除该项目。

- 切换项目，方法请参考**切换项目或区域**。

3.6 委托

3.6.1 委托其他管理资源

3.6.1.1 基本流程

通过委托信任功能，您可以将自己中的资源操作权限委托给更专业、高效的其他，被委托的可以根据权限代替您进行资源运维工作。

> **说明**
>
> 只能对进行委托，不能对IAM用户进行委托。

步骤1 （可选）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。

步骤2 B或者IAM用户管理委托资源。

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

----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，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”。

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：**管理用户及其权限**。
- 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（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

- 已有其他与您创建了委托关系。
- 您已经获取到委托方的名称、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。
5. 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“”。
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中，帮助您管理委托资源。

----结束

后续操作

被委托方或分配了委托权限的IAM用户均可以**切换角色**至委托方中，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中，根据权限管理委托方的资源。

前提条件

- 已有与您创建了委托关系。
- 您已经获取到委托方的名称及所创建的委托名称。

操作步骤

步骤1 使用或者**步骤2**中新建的用户登录。

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，输入委托方的名称。

说明

输入名称后，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中。

3.6.2 委托其他云服务管理资源

由于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**
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。

在 IAM 控制台创建云服务委托

步骤1 登录。

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”。

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“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 身份提供商

3.7.1 身份提供商概述

IAM支持基于SAML、OIDC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 3-3 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。
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。
OIDC	OIDC是OpenID Connect的简称，是一个基于OAuth 2.0协议的身份认证标准协议。IAM支持使用OIDC1.0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OIDC 1.0协议。
OAuth 2.0	OAuth 2.0是Open Authorization 2.0的简称，是一种开放授权协议，授权框架支持第三方应用程序以自己的名义获取访问权限。

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。

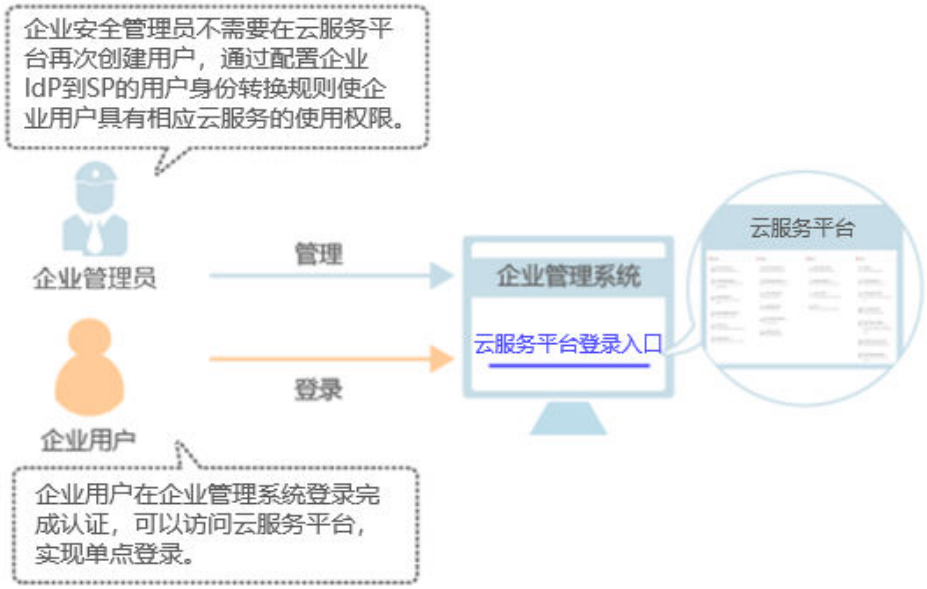
  使用联邦身份认证后，企业管理员只需要在企业管理系统中为用户创建账号，用户即可同时访问两个系统，降低了人员管理成本。

- 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 3-5 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：
  - 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。

3.7.2 虚拟用户 SSO 与 IAM 用户 SSO 的适用场景

目前支持两种身份提供商类型：虚拟用户SSO和IAM用户SSO。本文为您介绍两种身份提供商的适用场景和选择依据，帮助您根据整体业务需求选择合适的身份提供商类型。

虚拟用户 SSO

身份提供商中的用户登录后，系统为其自动创建虚拟用户信息，并按照身份转换规则授权。虚拟用户SSO适用于以下场景：

- 出于管理成本考虑，您不希望在云平台创建和管理IAM用户，从而避免用户同步带来的工作量。
- 您希望根据用户在本地企业IdP中加入的组或者用户的某个特殊属性，来区分云上拥有的权限。当企业Idp用户进行权限调整时，只需要在本地进行分组或属性的更改，即可同步到云平台。
- 您的各个分支机构存在多个企业IdP，都需要访问同一个账号，您需要在一个账号中内配置多个IdP进行联邦认证。

IAM 用户 SSO

身份提供商中的用户登录后，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。IAM用户SSO适用于以下场景：

- 您需要使用的云产品中有部分暂时不支持虚拟用户SSO访问。
- 您没有上述需要使用虚拟用户SSO的业务需求，而又希望尽量简化IdP配置。

两者的区别

虚拟用户SSO和IAM用户SSO的区别有身份转换方式、IAM用户身份、IAM侧权限分配3个方面的区别：

1、身份转换方式：虚拟用户SSO通过**身份转换规则**进行Idp用户和IAM用户的身份转换。IAM用户SSO使用外部身份ID来进行身份转换，Idp用户的IAM_SAML_Attributes_xUserId值与IAM用户的外部身份ID一一对应，一个或多个具有相同IAM_SAML_Attributes_xUserId值的Idp用户均可跳转至对应ID值的SP用户。因此，使用IAM用户SSO登录，请务必在Idp侧断言中设置IAM_SAML_Attributes_xUserId，在SP侧设置IAM用户外部身份ID。

2、IAM侧用户身份：虚拟用户SSO无法在IAM用户列表中找到Idp用户对应的IAM用户，跳转时系统临时为其自动创建虚拟用户信息。IAM用户SSO则在IAM用户列表中存在Idp用户对应的绑定外部身份ID的IAM子用户。

3、IAM侧权限分配：虚拟用户SSO中，Idp用户跳转后的权限取决于身份转换规则，规则中说明跳转后临时生成的虚拟用户拥有哪些用户组权限。IAM用户SSO中，Idp用户跳转后直接集成IAM子用户所在用户组的权限。

3.7.3 基于 SAML 协议的虚拟用户 SSO

3.7.3.1 基于 SAML 协议的虚拟用户 SSO 配置概述

与企业进行联邦认证登录时，是服务提供商（SP），企业自有的身份管理系统是身份提供商（IdP）。本节为您介绍企业IdP与，基于SAML协议进行虚拟用户SSO联邦认证的内部实现流程和配置步骤。

⚠ 注意

请确保您使用的企业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的联邦身份认证关系，配置流程如下。

1. **创建身份提供商并建立互信关系**：与企业IdP建立联邦认证，需要创建一个与企业IdP对应的身份提供商程序。然后，建立联邦认证的双方需首先建立互信关系，双方交换元数据文件，在企业IdP中上传元数据文件，在上传企业IdP的元数据文件。
2. **配置企业IdP参数**，规定在交互过程中，企业IdP向发送哪些信息。
3. **在华为云配置身份转换规则**：通过配置身份转换规则，明确企业IdP用户登录后的身份和权限，例如登录后的用户名、加入的用户组和拥有的访问权限。
4. **登录验证**：发起单点登录，测试是否能成功从企业IdP跳转登录。
5. **（可选）配置企业管理系统登录入口**：将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，如所示。

企业管理系统与联邦身份认证交互流程

为用户在发起单点登录请求后，企业管理系统与间的交互流程。

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，浏览器向发起单点登录请求。
2. 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。
6. 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。

说明

断言中要携带签名，否则会导致登录失败。

3.7.3.2 步骤 1：创建身份提供商

配置联邦身份认证，需要在企业IdP上传的元数据文件（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，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、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 对的信任关系

在企业IdP中配置的元数据文件，以建立企业IdP对的信任。

步骤1 将上述文件上传到企业IdP服务器上。上传方法请参见企业IdP的帮助文档。

步骤2 获取企业IdP的元数据文件。获取方法请参见企业IdP的帮助文档。

----结束

在上创建身份提供商

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中建立对企业IdP的信任关系，使得企业用户可以直接访问。

步骤1 进入，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 3-4 身份提供商基本参数

参数	含义
名称	身份提供商的名称。身份提供商名称在全局范围内不能重复，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协议的虚拟用户SSO**。
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。本章介绍虚拟用户SSO，此处选择虚拟用户SSO。 虚拟用户SSO：该身份提供商中的用户登录后，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。
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

在上配置元数据文件

配置元数据文件，即把企业IdP的Metadata文件配置到。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。

说明

企业IdP的Metadata文件获取方法请参考企业IdP提供商的帮助文档。

- **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。
  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”，保存设置信息。
- **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。 **不需要手动选择，系统自动生成。**
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。 **支持配置多个，默认使用第一个。**
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。 **支持配置多个，默认使用第一个。**

参数	是否必选	含义
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。 **支持配置多个，默认使用第一个。**
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。 **支持配置多个，默认使用第一个。**

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 3-6 某企业 IdP 的元数据文件

c. 单击“确定”，保存设置信息。

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

- **配置企业IdP：**在企业IdP系统中配置单点登录相关参数，决定向提供哪些用户信息。

- **配置身份转换规则：**在“身份转换规则”区域，配置身份转换规则，建立企业管理系统用户与IAM用户组间的映射关系，使得企业管理系统用户登录后，获得对应的操作权限。身份转换规则详情请参见：**步骤3：配置身份转换规则**。
- **登录验证：**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，方法请参考：**步骤4：登录验证**。

3.7.3.3 步骤 2：配置企业 Idp

您可以在企业IdP中配置单点登录相关参数，决定向提供哪些用户信息。企业IdP与交互过程中，需要将企业IdP用户的相关信息发送给，会结合接收到的信息和身份转换规则，确定联邦用户的身份和权限。

常用的企业 IdP 配置参数

表 3-5 常用的企业 IdP 配置参数

参数名	描述	适用场景
IAM_SAML_Attributes_redirect_url	指定联邦登录重定向的目标网址	用户在SSO登录过程中，希望跳转到控制台的指定页面。
IAM_SAML_Attributes_domain_id	与企业IdP建立联邦认证的ID值	从企业IdP侧发起联邦认证登录，必须在企业IdP侧配置该参数。
IAM_SAML_Attributes_idp_id	与企业IdP建立联邦认证的中，创建的身份提供商名称	从企业IdP侧发起联邦认证登录，必须在企业IdP侧配置该参数。

3.7.3.4 步骤 3：配置身份转换规则

企业IdP用户登录后，会根据身份转换规则，决定联邦用户的身份和拥有的权限。身份转换规则需要用户根据自身场景自定义，若不对身份转换规则进行配置，则联邦用户在中的用户名默认为“FederationUser”，权限默认仅能访问，没有其他任何权限。

您可对联邦用户的以下特征进行配置：

- 用户名：企业IdP用户在中显示不同的用户名。
- 用户权限：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，使用的资源。配置时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

- 企业管理员在注册了可用的账号，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**。
- 已在本系统创建身份提供商，如何创建身份提供商请参见：**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：**联邦用户身份转换规则说明**。

- **创建规则**
  a. 管理员在的左侧导航窗格中，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 3-6 参数说明

参数名	描述	说明
用户名	联邦用户在中显示的用户名，以下简称“联邦用户名”。	为了区分的用户与联邦用户，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	联邦用户在中所属的用户组。	联邦用户拥有所属用户组的权限。可以选择已创建的用户组。

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。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。

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的用户在中映射的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，进入，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：**联邦用户身份转换规则说明**。

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。

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**。

3.7.3.5 步骤 4：登录验证

登录验证

按照登录请求发起方可将联邦用户登录方式分为两类：

- Idp侧登录：用户从IdP侧（企业自己的身份提供商侧）发起登录请求，例如从Microsoft Active Directory（AD FS）、Shibboleth侧发起登录云服务平台控制台的请求。
- SP侧登录：用户从SP侧（服务提供商侧）发起登录请求，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，SP侧登录链接可在IAM控制台身份提供商详情页面获取。

不同的企业IdP发起Idp侧登录的方式差异较大，云服务平台帮助文档不做详述，具体操作请参考企业IdP的帮助文档。本节重点介绍SP侧发起登录的方法：

步骤1 联邦用户登录。

在控制台的“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“ ”，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。

----结束

跳转到指定区域或服务

如需指定联邦用户登录的目标页面，有以下两种配置方式：

- SP侧登录配置方法

  拼接控制台获取的登录链接与指定url，拼接格式为“**登录链接&service=指定url**”。
- IdP侧登录配置方法

  在企业IdP的SAML 断言中配置IAM_SAML_Attributes_redirect_url声明，声明值为指定跳转的目标URL。

3.7.3.6 （可选）步骤 5：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。

前提条件

- 已在本系统创建身份提供商，如何创建身份提供商请参见：**步骤1：创建身份提供商**。
- 企业管理系统界面已创建登录入口。

操作步骤

步骤1 在的左侧导航窗格中，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“ ”。

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>"> </a>
```

步骤5 用户登录企业管理系统后通过单击可以直接访问。

----结束

3.7.4 基于 SAML 协议的 IAM 用户 SSO

3.7.4.1 基于 SAML 协议的 IAM 用户 SSO 配置概述

与企业进行联邦认证登录时，是服务提供商（SP），企业自有的身份管理系统是身份提供商（IdP），通过基于SAML协议的单点登录，企业员工在登录以后，将跳转至，以IAM用户的方式访问。

本节为您介绍企业IdP与，基于SAML协议进行IAM用户SSO联邦认证的内部实现流程和配置步骤。

注意

请确保您使用的企业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的联邦身份认证关系，配置流程如下。

1. **创建身份提供商并建立互信关系**：与企业IdP建立联邦认证，需要创建一个与企业IdP对应的身份提供商程序。然后，建立联邦认证的双方需首先建立互信关系，双方交换元数据文件，在企业IdP中上传元数据文件，在上传企业IdP的元数据文件。
2. **配置企业IdP**：配置企业IdP参数，规定在交互过程中，企业IdP向发送哪些信息。
3. **配置外部身份ID**：配置外部身份ID，建立IAM用户与企业IdP用户的对应关系，当企业IdP用户使用IAM用户SSO时，会以指定外部身份ID的IAM用户身份登录。例如，企业用户"IdP_Test_User"的ID值与IAM用户“Alice”的外部身份ID一致，则IdP_Test_User会以Alice的身份登录IAM。
4. **登录验证**：发起单点登录，测试是否能成功从企业IdP跳转登录。
5. **（可选）配置企业管理系统登录入口**：将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，如所示。

企业管理系统与联邦身份认证交互流程

为用户在发起单点登录请求后，企业管理系统与间的交互流程。

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，浏览器向发起单点登录请求。
2. 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。
6. 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。

说明

断言中要携带签名，否则会导致登录失败。

3.7.4.2 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。

建立企业 IdP 对的信任关系

在企业IdP中配置的元数据文件，以建立企业IdP对的信任。

步骤1 将上述文件上传到企业IdP服务器上。上传方法请参见企业IdP的帮助文档。

步骤2 获取企业IdP的元数据文件。获取方法请参见企业IdP的帮助文档。

----结束

在上创建身份提供商

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中建立对企业IdP的信任关系，使得企业用户可以直接访问。

步骤1 进入，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 3-7 身份提供商基本参数

参数	含义
名称	身份提供商的名称。身份提供商名称在全局范围内不能重复，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协议的虚拟用户SSO**。

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。本章介绍IAM用户SSO，此处选择IAM用户SSO。 IAM用户SSO：该身份提供商中的用户登录后，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

在配置元数据文件

配置元数据文件，即把企业IdP的Metadata文件配置到。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。

说明

企业IdP的Metadata文件获取方法请参考企业IdP提供商的帮助文档。

- **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。
  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”，保存设置信息。
- **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。 **不需要手动选择，系统自动生成。**
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。 **支持配置多个，默认使用第一个。**
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。 **支持配置多个，默认使用第一个。**
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。 **支持配置多个，默认使用第一个。**
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。 **支持配置多个，默认使用第一个。**

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 3-7 某企业 IdP 的元数据文件

c. 单击“确定”，保存设置信息。

3.7.4.3 步骤 2：配置企业 IdP

您可以在企业IdP中配置单点登录相关参数，决定向提供哪些用户信息。企业IdP与交互过程中，需要将企业IdP用户的相关信息发送给，会结合接收到的信息，确定联邦用户的身份和权限。

说明

IAM用户SSO类型的单点登录，企业IdP必须要配置IAM_SAML_Attributes_xUserId断言。

常用的企业 IdP 配置参数

表 3-8 常用的企业 IdP 配置参数

参数名	描述	适用场景
IAM_SAML_Attributes_xUserId	选择IAM用户SSO时，企业IdP用户的ID值。	使用IAM SSO时，必须配置此参数。 企业IdP用户与IAM用户一一对应，企业IdP用户的IAM_SAML_Attributes_xUserId值，与对应IAM用户的外部身份ID相同。
IAM_SAML_Attributes_redirect_url	指定联邦登录重定向的目标网址	用户在SSO登录过程中，希望跳转到控制台的指定页面。
IAM_SAML_Attributes_domain_id	与企业IdP建立联邦认证的ID值	从企业IdP侧发起联邦认证登录，必须在企业IdP侧配置该参数。
IAM_SAML_Attributes_idp_id	与企业IdP建立联邦认证的中，创建的身份提供商名称	从企业IdP侧发起联邦认证登录，必须在企业IdP侧配置该参数。

3.7.4.4 步骤 3：配置外部身份 ID

IAM用户SSO类型的单点登录，必须要为企业IdP用户对应的IAM用户配置外部身份ID。外部身份ID值要与企业IdP的IAM_SAML_Attributes_xUserId值保持一致。您可以在IAM用户创建时配置外部身份ID，或者直接修改现有IAM用户的外部身份ID：

- **创建IAM用户并设置外部身份ID**

- 修改现有IAM用户的外部身份ID

创建 IAM 用户并设置外部身份 ID

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”，单击右上方的“创建用户”。

步骤3 在“创建用户”页面配置IAM“用户信息>外部身份ID”。其他创建IAM用户详情参见创建用户。

----结束

修改现有 IAM 用户的外部身份 ID

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用户外部身份ID。

3.7.4.5 步骤 4：登录验证

登录验证

按照登录请求发起方可将联邦用户登录方式分为两类：

- Idp侧登录：用户从IdP侧（企业自己的身份提供商侧）发起登录请求，例如从Microsoft Active Directory（AD FS）、Shibboleth侧发起登录云服务平台控制台的请求。
- SP侧登录：用户从SP侧（服务提供商侧）发起登录请求，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，SP侧登录链接可在IAM控制台身份提供商详情页面获取。

不同的企业IdP发起Idp侧登录的方式差异较大，云服务平台帮助文档不做详述，具体操作请参考企业IdP的帮助文档。本节重点介绍SP侧发起登录的方法：

步骤1 联邦用户登录。

在控制台的“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“”，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 查看联邦用户是否跳转至实体IAM用户。

----结束

跳转到指定区域或服务

如需指定联邦用户登录的目标页面，有以下两种配置方式：

- SP侧登录配置方法

  拼接控制台获取的登录链接与指定url，拼接格式为“**登录链接&service=指定url**”。
- IdP侧登录配置方法

在企业IdP的SAML 断言中配置IAM_SAML_Attributes_redirect_url声明，声明值为指定跳转的目标URL。

3.7.4.6 （可选）步骤 5：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。

前提条件

- 已在创建身份提供商，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登录入口。

操作步骤

步骤1 在的左侧导航窗格中，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“ ”。

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>">  </a>
```

步骤5 用户登录企业管理系统后通过单击可以直接访问。

----结束

3.7.5 基于 OIDC 协议的虚拟用户 SSO

3.7.5.1 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，在创建身份提供商并配置授权信息，从而建立企业管理系统和的信任关系。
2. **配置身份转换规则**：通过在配置身份转换规则，将IdP中的用户、用户组及其访问权限映射到。
3. **配置企业管理系统登录入口**：将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。

企业管理系统与联邦身份认证交互流程

为用户在发起单点登录请求后，企业管理系统与间的交互流程。

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，浏览器向发起单点登录请求。

2. 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。
6. 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。

3.7.5.2 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，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OIDC身份提供商。设置授权定向URI为：https:///authui/oidc/redirect和https:///authui/oidc/post。

步骤2 获取企业IdP的OAuth 2.0凭据。

----结束

在上创建身份提供商

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。

步骤1 进入，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

在上配置授权信息

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 3-9 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。 • 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。 **如果您需要使用SSO方式访问，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。

步骤3 在修改身份提供商页面，填写“配置信息”。

表 3-10 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。**

配置信息	说明
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。**
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。

- 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管理系统。
- 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，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，方法请参考：**（可选）步骤3：配置企业管理系统登录入口**。

3.7.5.3 步骤 2：配置身份转换规则

在IAM上创建身份提供商后，联邦用户在中的用户名默认为“FederationUser”，且联邦用户仅能访问，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：**联邦用户身份转换规则说明**。

- **创建规则**
  a. 管理员在的左侧导航窗格中，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 3-11 参数说明

参数名	描述	说明
用户名	联邦用户在中显示的用户名，以下简称“联邦用户名”。	为了区分的用户与联邦用户，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	联邦用户在中所属的用户组。	联邦用户拥有所属用户组的权限。可以选择已创建的用户组。
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。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。

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的用户在中映射的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，进入，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：**联邦用户身份转换规则说明**。

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“ ”，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**。

3.7.5.4 （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。

前提条件

- 已在本系统创建身份提供商，如何创建身份提供商请参见：**步骤1：创建身份提供商**。
- 企业管理系统界面已创建登录入口。

操作步骤

步骤1 在的左侧导航窗格中，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“ ”。

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>"> </a>
```

步骤5 用户登录企业管理系统后通过单击可以直接访问。

----结束

3.7.6 联邦用户身份转换规则说明

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

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

- 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：表示联邦用户映射到系统中的身份转换规则。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。
- local：表示联邦用户在系统中的用户信息。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。

规则条件示例

通过示例来加深您对身份转换规则条件（empty、any_one_of、not_any_of）的理解。

- empty：该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}”，如下所示。

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



```
        }
      ]
    }
  ]
```

表示联邦用户在系统中的用户名称为“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。

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

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

如果联邦用户需要在系统中属于多个用户组，身份转换规则如下所示。

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

表示联邦用户在系统中的用户名称为“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*。

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：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。

```
[
    {
        "local": [
            {
                "user": {
                    "name": "{0}"
                }
            },
            {
                "group": {
                    "name": "admin"
                }
```



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

表示联邦用户在系统中的用户名为“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。

如果联邦用户需要在系统中属于多个用户组，身份转换规则如下所示。

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

表示联邦用户在系统中的用户名为“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。

- 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系统。

  ```
  {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访问系统。

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

- 含有正则表达式的条件：你可以在条件里指定一个“"regex": true”用来表示系统将以正则匹配的方式来计算结果。

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



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

表示该规则对以任意值开头，“@mail.com”结尾的用户生效，在系统中的用户名为*UserName*，所属用户组为“admin”。

- 条件组合：多个条件间，以“逻辑与”的方式组合。

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

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：在系统中的用户名为*UserName*，所属用户组为“admin”。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"
            ]
        }
    ]
  }
]
```

- 多规则

  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，否则系统不允许此用户登录；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。

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

  表示针对IdP中属于“idp_admin”用户组的用户生效，在系统中的用户名为*UserName*，所属用户组为“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。在系统中的用户名为John Smith，所属用户组为“admin”。

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

3.8 多因素认证和虚拟 MFA

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。

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。

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，遵循基于时间的一次性密码（Timbe-based One-Time Password，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。

多因素认证应用的场景

多因素认证主要应用于登录验证。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。

3.9 审计

3.9.1 云审计服务支持的 IAM 操作列表

云审计服务记录统一身份认证服务相关的操作事件，如表3-12所示。

表 3-12 云审计服务支持的 IAM 操作列表

操作名称	资源类型	事件名称
获取Token	token	createTokenByPwd
获取Token	token	createTokenByHwAccessKey
获取Token	token	createTokenByToken

操作名称	资源类型	事件名称
获取Token	token	createTokenByAssumeRole
用户登录	user	login
用户登录失败	user	loginFailed
用户登出	user	logout
修改用户密码	user	changePassword
创建用户	user	createUser
修改用户信息	user	updateUser
删除用户	user	deleteUser
修改用户密码	user	updateUserPwd
创建AK/SK	user	addCredential
删除AK/SK	user	deleteCredential
修改邮箱	user	modifyUserEmail
修改手机	user	modifyUserMobile
修改密码	user	modifyUserPassword
上传头像	user	modifyUserPicture
管理员设置用户密码	user	setPasswordByAdmin
创建用户组	userGroup	createUserGroup
更新用户组	userGroup	updateUserGroup
删除用户组	userGroup	deleteUserGroup
添加用户到用户组	userGroup	addUserToGroup
从用户组删除用户	userGroup	removeUserFromGroup
创建项目	project	createProject
修改项目	project	updateProject
更新项目状态	project	updateProjectStatus
创建委托	agency	createAgency
修改委托	agency	updateAgency
删除委托	agency	deleteAgency
切换角色	user	switchRole
注册身份提供商	identityProvider	createIdentityProvider

操作名称	资源类型	事件名称
更新身份提供商	identityProvider	updateIdentityProvider
删除身份提供商	identityProvider	deleteIdentityProvider
注册映射	mapping	createMapping
更新映射	mapping	updateMapping
删除映射	mapping	deleteMapping
注册协议	protocol	createProtocol
更新协议	protocol	updateProtocol
删除协议	protocol	deleteProtocol
租户中用户组增加权限	roleGroupDomain	assignRoleToGroupOnDomain
删除某租户中指定用户组权限	roleGroupDomain	unassignRoleToGroupOnDomain
项目对应用户组增加权限	roleGroupProject	assignRoleToGroupOnProject
删除项目对应用户组权限	roleGroupProject	unassignRoleToGroupOnProject
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
解绑虚拟MFA	MFA	UnBindMFA

3.9.2 查看审计日志

开启了云审计服务后，系统开始记录统一身份认证服务相关的操作。云审计服务管理控制台保存最近7天的操作记录。

查看 IAM 的云审计日志

步骤1 登录管理控制台。

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

步骤3 单击左侧导航树的“事件列表”，进入事件列表信息页面。

步骤4 单击事件列表右上方的“筛选”，设置对应的操作事件条件。

当前事件列表支持四个维度的组合查询，详细信息如下：

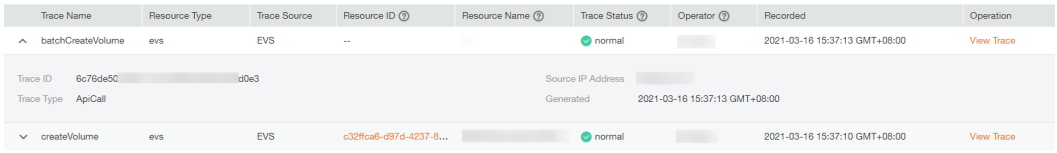
- “事件来源”、“资源类型”和“筛选类型”。

  - 在下拉框中选择查询条件。其中，“事件来源”选择“IAM”。
  - 筛选类型选择事件名称时，还需选择某个具体的事件名称。
  - 选择资源ID时，还需选择或者手动输入某个具体的资源ID。
  - 选择资源名称时，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”、，只可选择其中一项。
- “起始时间”、“结束时间”：可通过选择时间段查询操作事件。

步骤5 单击“查询”，查看对应的操作事件。

步骤6 展开记录的详细信息，展开记录如图3-8所示。

图 3-8 展开记录



步骤7 在需要查看的记录右侧，单击“查看事件”，弹出一个窗口，如图3-9所示，显示了该操作事件结构的详细信息。

图 3-9 查看事件

查看事件


```
{
    "service_type": "IAM",
    "user": {
        "name": "[redacted]",
        "id": "5bfe084fc075457ca6e737ede73fb22c",
        "domain": {
            "name": "[redacted]",
            "id": "0c264ba0cefb48c0a9674fee0c6e144f"
        }
    },
    "time": "2018/05/04 17:47:41 GMT+08:00",
    "code": 302,
    "resource_type": "user",
    "resource_name": "[redacted]",
    "resource_id": "5bfe084fc075457ca6e737ede73fb22c",
    "source_ip": "[redacted]",
    "trace_name": "login",
    "trace_type": "ConsoleAction",
    "record_time": "2018/05/04 17:47:41 GMT+08:00",
    "trace_id": "2fbc06e0-4f80-11e8-b6f4-286ed488cbe3",
    "trace_status": "normal"
}
```


----结束

4 常见问题

4.1 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，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。

前提条件

用户需要绑定了手机/邮箱，才可以开启短信/邮箱验证；用户需要**绑定虚拟MFA**应用程序后，才可以开启虚拟MFA验证。

操作步骤

- 在统一身份认证服务，修改用户功能中开启登录验证功能

步骤1 在统一身份认证服务左侧导航窗格中，单击“用户”。

步骤2 在用户列表中，单击对应用户栏目的“修改”。

步骤3 在“修改用户”界面，登录验证栏目，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

- 在我的凭证中开启登录验证功能。

步骤1 单击右上方登录的用户，在下拉列表中选择“我的凭证”。

步骤2 在我的凭证页面，单击“登录验证”栏目的“修改”。

步骤3 在“修改登录保护”页面中，选择需要使用的验证方式，输入相应的验证码。

步骤4 单击“确认”。

----结束

4.2 如何绑定虚拟 MFA 设备

Multi-Factor Authentication (MFA) 是一种非常简单的最佳安全实践方法，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。

如需了解更多相关内容，请参考：**多因素认证和虚拟MFA**。

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。

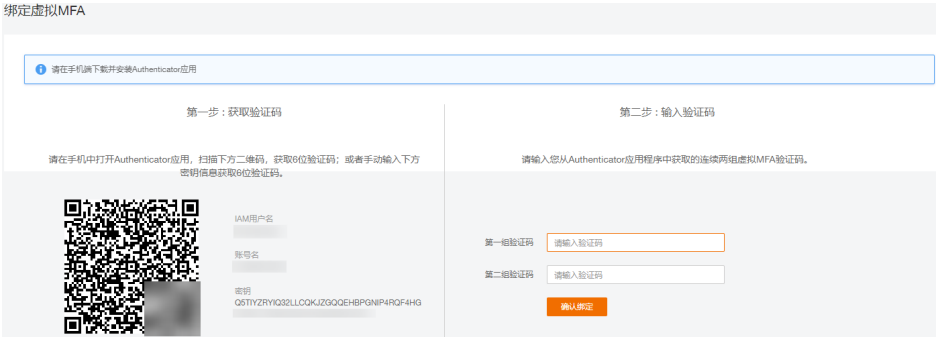
操作步骤

步骤1 在控制台页面，单击右上方登录的用户，在下拉列表中选择“我的凭证”。

步骤2 在我的凭证页面，单击虚拟MFA栏目的“绑定”。

步骤3 进入“绑定虚拟MFA”页面。

图 4-1 绑定虚拟 MFA



说明

密钥是获取MFA验证码的凭证，使用一次后失效，为了保证您的账户安全，请勿向任何人提供此密钥。

步骤4 在您的MFA应用程序中添加用户。

- 扫描二维码

  打开手机上已安装好的MFA应用程序，单击应用程序上右下角的“+”，选择“扫描条形码”，扫描“登录验证策略”页面上的二维码。扫描成功后，系统会自动添加用户，应用程序上会显示您的账号和密钥。

- 手动输入

  打开手机上已安装好的MFA应用程序，单击应用程序上右下角的“+”，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5 添加用户完成，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6 在“登录验证策略”页面输入连续的两组口令，然后单击“确认绑定”，完成绑定虚拟MFA设备的操作。

----结束

4.3 如何获取 MFA 验证码

在开启使用MFA进行登录验证后，用户登录管理控制台时，输入用户名和密码后，还需输入MFA应用程序的动态验证码。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。

4.4 如何解绑 MFA

只要手机不丢失或者没有删除虚拟MFA应用程序，用户可以在界面自助完成解绑MFA的操作。

1. 在系统首页，单击“控制台”。
2. 单击右上方登录的用户，在下拉列表中选择“我的凭证”。

3. 单击虚拟MFA设备右侧的“解绑”。
4. 在页面中，在页面中输入从虚拟MFA设备获取的动态验证码。
5. 单击“确定”，验证成功后，完成解绑MFA操作。

4.5 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：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。
  b. 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。
  c. 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”**
  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。

4.6 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“账号安全设置”，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

4.7 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。

IAM 和企业管理的区别

- 开通方式
  - IAM是的身份管理服务，注册系统后，无需付费即可使用。
  - 企业管理是的资源管理服务，注册系统后，。
- 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>管理项目。
  - 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。

IAM 与企业管理的关系

- IAM和企业管理的创建用户以及用户组功能，两边是相互同步关系。
- 申请开通企业管理服务后，使用企业管理的用户组授权功能时，该功能依赖IAM的策略授权。如果企业管理中系统预置的策略不能满足您的使用要求，需要在IAM中创建自定义策略，自定义策略会同步到企业管理中，可以在IAM或者企业管理中给用户组授权自定义策略。
- 如果在IAM和企业管理中同时给用户组授权，用户同时拥有基于IAM项目的策略和基于企业项目的策略，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。
  - 如果策略中包含相同的Action，以在IAM中设置的生效，例如：用户请求创建云服务器，鉴权结果为IAM中定义的Deny，不能创建云服务器。

```
IAM项目策略中包含以下action：
{
  "Action": [
    "ecs:cloudServers:create"
  ],
  "Effect": "Deny"
}
```



```
企业项目策略中包含以下action：
{
  "Action": [
    "ecs:cloudServers:create"
  ],
  "Effect": "Allow"
}
```

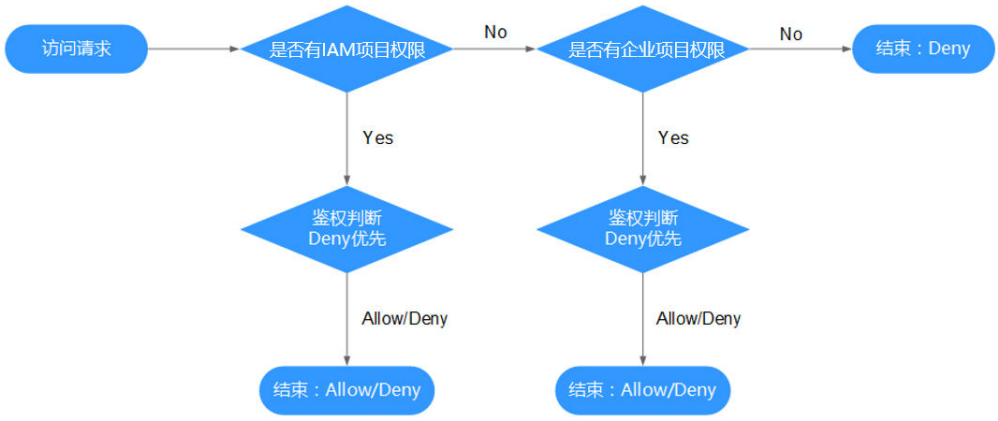
- 如果策略中包含不同的Action，则IAM和企业管理中设置的都生效。以下示例表示用户可以创建云服务器以及删除云服务器。

```
IAM项目策略中包含以下action：
{
  "Action": [
    "ecs:cloudServers:create"
  ],
  "Effect": "Allow"
}
企业项目策略中包含以下action：
{
  "Action": [
    "ecs:cloudServers:delete"
  ],
  "Effect": "Allow"
}
```

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 4-2 请求鉴权逻辑图



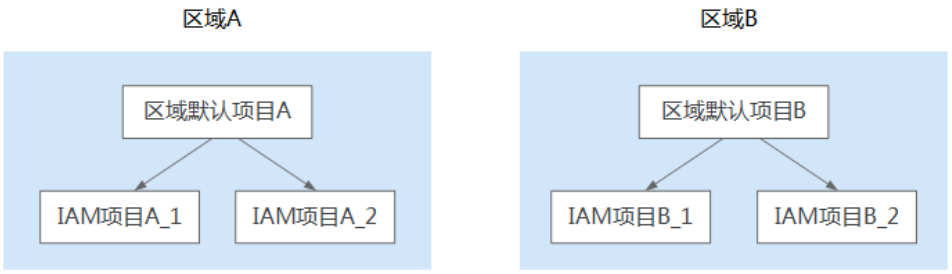
1. 用户发起访问请求。
2. 系统在用户被授予的访问权限中，优先寻找基于IAM项目授权的权限，在权限中寻找请求对应的action。
3. 如果找到匹配的Allow或者Deny的action，系统将返回对请求的鉴权决定，Allow或者Deny，鉴权结束。
4. 如果在基于IAM项目的权限中没有找到请求对应的action，系统将继续寻找基于企业项目授权的权限，在权限中寻找请求对应的action。
5. 如果找到匹配的Allow或者Deny的action，系统将返回对请求的鉴权决定，Allow或者Deny，鉴权结束。
6. 如果用户不具备任何权限，系统将返回鉴权决定Deny，鉴权结束。

4.8 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。

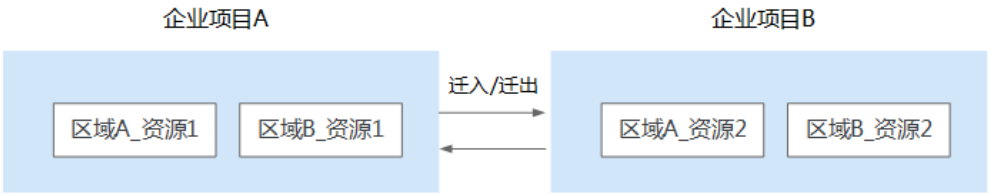
使用IAM项目，请参考：用户指南>管理项目。



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。

使用企业项目，请参考：《企业管理用户指南》。



4.9 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：

- ：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，方法请参见：用户指南>创建委托（委托方操作）。
- 请管理员授予使用IAM服务的权限。

4.10 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、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。

- 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。

4.11 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，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，下次登录时，登录界面的密码输入框会自动联想填充字符，为了确保及密码安全，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”。

----结束

后续处理

清除已保存的登录信息的方法：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。

4.12 如何为 IAM 用户授予“欧洲-巴黎”区域云服务权限

问题描述

管理员已开通“欧洲-巴黎”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。

由于华为云“欧洲-巴黎”区域用户属于联邦认证授权访问“欧洲-巴黎”云服务系统的虚拟用户，不是“欧洲-巴黎”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“欧洲-巴黎”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“欧洲-巴黎”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“欧洲-巴黎”区域。

步骤2 在“欧洲-巴黎”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“欧洲-巴黎”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“欧洲-巴黎”区域，可以按照权限使用云服务资源。

4.13 如何获取“欧洲-巴黎”区域的访问密钥 AK/SK

问题描述

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

由于华为云“欧洲-巴黎””区域用户属于联邦认证授权访问“欧洲-巴黎”云服务系统的虚拟用户，不是“欧洲-巴黎”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“欧洲-巴黎”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“欧洲-巴黎”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“欧洲-巴黎”区域。
2. 在“欧洲-巴黎”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“欧洲-巴黎”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“欧洲-巴黎”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

A 文档修订记录

表 A-1 修订记录

日期	修订记录
2022-11-30	第二十次正式发布 本次变更说明如下： • 新增**IAM用户登录失败怎么办**章节。 • 新增**如何控制IAM用户访问控制台**章节。 • 新增**IAM和企业管理的区别**章节。 • 新增**IAM项目和企业项目的区别**章节。 • 新增**创建委托时提示权限不足怎么办**章节。 • 新增**Internet Explorer浏览器下输入框提示信息无法自动消失怎么办**章节。 • 新增**如何在Google Chrome浏览器禁用密码联想与保存**章节。
2022-07-25	第十九次正式发布 本次变更说明如下： 修改**创建安全管理员**，**创建用户并加入用户组**，**创建用户**，**（可选）分配委托权限（被委托方操作）**章节创建用户描述。
2021-07-30	第十八次正式发布 本次变更说明如下： • 新增**权限管理**章节。 • 新增**自定义策略使用样例**章节。
2020-08-30	第十七次正式发布 本次变更说明如下： • 修改**身份提供商**章节结构。 • 新增**基于OIDC协议的虚拟用户SSO**章节。

日期	修订记录
2020-03-31	第十六次正式发布 本次变更说明如下： **策略语言说明**中策略授权语句（Statement）新增资源类型（Resource）和条件（Condition）。
2020-01-03	第十五次正式发布 本次变更说明如下： **创建委托（委托方操作）**中删除以下说明：“委托类型”为“云服务”的委托不支持。
2018-08-30	第十四次正式发布。 本次变更说明如下： **设置账号安全策略**中新增设置“会话超时策略”。
2018-08-10	第十三次正式发布。 本次变更说明如下： • 新增**个人数据保护机制**章节。 • 新增**审计**章节。
2018-06-29	第十二次正式发布。 本次变更说明如下： **查看或修改用户信息**中新增“是否重置密码”步骤。
2018-04-30	第十一次正式发布。 本次变更说明如下： • **查看或修改用户信息**中新增“失败清零”的操作。 • **设置账号安全策略**中新增配置“会话超时时长”的操作。 • 新增**如何绑定虚拟MFA设备**章节。 • 新增**如何获取MFA验证码**章节。 • 新增**如何解绑MFA**章节。 • 新增**权限管理**章节。
2018-02-09	第十次正式发布。 本次变更说明如下： **创建委托（委托方操作）**中新增委托类型的表格。
2017-10-27	第九次正式发布。 调整文档大纲。增加**产品简介**、**快速入门**等内容。
2017-10-15	第八次正式发布。 本次变更说明如下： 删除权限说明章节，权限说明详情请参考权限说明。

日期	修订记录
2017-07-27	第七次正式发布。 本次变更说明如下： ● 新增“CTS Administrator”权限描述。 ● **创建身份提供商**中新增系统自动提取和手动编辑元数据内容。
2017-05-26	第六次正式发布。 本次变更说明如下： 新增**建立的信任关系**
2017-04-27	第五次正式发布。 本次变更说明如下： ● 新增**创建委托（委托方操作）**章节。 ● 新增**（可选）分配委托权限（被委托方操作）**章节。
2017-03-30	第四次正式发布。 本次变更说明如下： ● 新增“Agent Operator”权限描述。 ● 新增“RTS Administrator”权限描述。 ● **查看或修改用户信息**增加设置用户凭证的说明。
2017-02-10	第三次正式发布。 本次变更说明如下： 增加“Guest”权限描述。
2017-01-20	第二次正式发布。 本次变更说明如下： 新增“MRS Administrator”权限描述。
2016-12-30	第一次正式发布。