# IAM 5.0 常见问题

**文档版本** 01

**发布日期** 2025-11-05

**华为云计算技术有限公司**

### 商标声明


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

### 注意

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

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

## 华为云计算技术有限公司

地址： 贵州省贵安新区黔中大道交兴功路华为云数据中心 邮编：550029

网址： https://www.huaweicloud.com/

# 目 录



# 1 权限管理类

## 1.1 在自定义身份策略中无法找到特定服务，或授权时无法找到特定服务的系统身份策略怎么办

### 问题描述

管理员在IAM新版控制台中创建自定义身份策略时无法找到特定服务，或者在IAM新版控制台中为用户、用户组、委托和信任委托授予系统身份策略时，无法找到特定服务的权限。

### 可能原因

- 搜索的服务或身份策略名称不正确。
- 需要设置权限的服务不支持IAM的身份策略。所以创建自定义身份策略时无法找到特定服务，同时也没有该服务的系统身份策略。详情请参见**支持身份策略与信任委托的云服务列表**。

### 解决方法

- 请在管理控制台或帮助中心确认服务名称，并在**身份策略授权参考**查看该服务提供的系统身份策略和自定义身份策略支持的授权项。
- 在IAM旧版控制台中为用户、用户组、委托授予对应服务的系统角色、系统策略、自定义策略来满足权限管理要求。

## 1.2 如何为 IAM 用户授予“欧洲-都柏林”区域云服务权限

### 问题描述

管理员已开通“欧洲-都柏林”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“欧洲-都柏林”区域用户属于联邦认证授权访问“欧洲-都柏林”云服务系统的虚拟用户，不是“欧洲-都柏林”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-都柏林”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**。

## 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-都柏林”区域。

**步骤2** 在“欧洲-都柏林”区域控制台，选择“管理与部署>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“授权”。

**步骤5** 在身份策略列表，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-都柏林”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-都柏林”区域，可以按照权限使用云服务资源。

# 1.3 权限没有生效怎么办

## 问题描述

管理员在IAM新版控制台给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用户的权限不正确。

   解决方法：管理员确认并修改授予IAM用户的权限，方法请参考：**给IAM用户授权**或**创建用户组并授权**，权限详情请参考**身份策略授权参考**。
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**身份策略语法**。
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：**用户组添加用户**。
4. 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。
5. 可能原因：该服务可能提供独立权限控制，如对象存储服务OBS。

   解决方法：请查看对应服务帮助文档，并授予用户对应权限。如**OBS权限控制概述**。

# 1.4 如何授予 IAM 用户不能支付订单、可以提交订单权限

## 问题描述

管理员需授予IAM用户可以提交购买订单，但是不能支付订单的权限。

## 解决方法

目前费用中心在IAM注册的系统权限无法满足管理员的需求，需要自定义身份策略，并将其授权给IAM用户。

## 前提条件

请确保您已创建IAM用户A。详情请参见**创建IAM用户**。

## 操作步骤

**步骤1** 登录华为云控制台。

**步骤2** 在控制台页面，鼠标移动至右上方的用户名，在下拉列表中选择“统一身份认证”。

**步骤3** 在统一身份认证服务，左侧导航窗格中，选择“身份策略”页签，单击右上方的“创建自定义身份策略”。

**图 1-1** 创建自定义身份策略


**步骤4** 输入“策略名称”为“**billing_order**”。

**步骤5** “策略配置方式”选择“可视化视图”。

**步骤6** 在“策略内容”下配置**不能支付订单、可以提交订单**的策略。

- 配置**不能支付订单**的策略
  a. 选择“拒绝”。
  b. 选择“云服务”为“**billing**”。
  c. 在“操作”下打开“**写**”操作，选择“**billing:order:pay**”授权项。

**图 1-2** 配置不能支付订单的策略

d. 选择“**资源类型**”为“所有资源”。

- 配置**可以提交订单**的策略。

a. 选择“允许”。

b. 选择“云服务”为“**billing**”。

c. 在“操作”下打开“**写**”操作，选择“**billing:bill:update**”授权项，并**全选只读**授权项。

**图 1-3** 配置可以提交订单的策略

d. 选择“**资源类型**”为“所有资源”。

**步骤7** 输入“策略描述”为“不能支付订单，可以提交订单的自定义身份策略”。

**步骤8** 单击“确定”，自定义身份策略创建完成。

**步骤9** 将新创建的自定义身份策略附加至IAM用户A。

**说明**

给用户授予自定义身份策略与系统身份策略操作一致，详情请参考：**给IAM用户授权**。

设置成功后，IAM用户A登录到华为云进入“**费用中心>待支付订单**”，将无法单击订单的操作列“**支付**”按钮。

**图 1-4** 设置成功


**图 1-5** 设置失败


**----结束**

# 1.5 仅使用策略进行授权但无法找到错误提示信息中的授权项

## 问题描述

管理员仅使用系统策略或自定义策略给IAM用户授权。如果IAM用户执行了授权范围之外的操作，此时将会被提示没有权限执行该操作，但是管理员在策略中无法找到该提示信息中的授权项。

## 可能原因

该提示信息中的授权项不属于策略的授权项，而属于身份策略的授权项。

## 解决方法

- 可以使用身份策略进行授权，选择提示信息中的身份策略授权项进行授权即可。
- 如果只希望使用策略进行授权，需要找到身份策略授权项对应的策略授权项别名，通过在策略中授予这个身份策略授权项的别名来进行解决。

在使用第二种解决方法之前，需要先了解策略和身份策略生效逻辑，如图1-6所示。

**图 1-6** 策略和身份策略生效逻辑

| 综合鉴权结果 | | 身份策略鉴权结果 | | |
|---|---|---|---|---|
| | | 显式拒绝 | 允许 | 隐式拒绝 |
| 策略鉴权结果 | 显式拒绝 | 显式拒绝 | 显式拒绝 | 显式拒绝 |
| | 允许 | 显式拒绝 | 允许 | 允许 |
| | 隐式拒绝 | 显式拒绝 | 允许 | 隐式拒绝 |

显式拒绝和隐式拒绝的区别见**策略**和**身份策略鉴权规则**。当综合鉴权结果为隐式拒绝时，系统提示没有对应授权项的权限，如下所示：

```
"error_msg": "User: xxx is not authorized to perform action ecs:cloudServers:get on resource ecs:cn-north-5:yyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyy:instance:zzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzz because no identity-based policy allows the ecs:cloudServers:get action."
```

当综合鉴权结果为显式拒绝时，系统提示没有对应授权项的权限，如下所示：

```
"error_msg": "User: xxx is not authorized to perform action ecs:cloudServers:get on resource ecs:cn-north-5:yyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyy:instance:zzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzz with an explicit deny in an identity-based policy."
```

其中，提示信息中说明无权限的授权项以及涉及的资源，但是授权项属于策略还是身份策略并不固定，IAM会根据策略和身份策略的不同拒绝方式来进行综合判断，相关逻辑如**图1-7**所示。

**图 1-7** 鉴权逻辑

| 错误提示信息中授权项来源 | | 身份策略鉴权结果 | | |
|---|---|---|---|---|
| | | 显式拒绝 | 允许 | 隐式拒绝 |
| 策略鉴权结果 | 显式拒绝 | 身份策略 | 策略 | 策略 |
| | 允许 | 身份策略 | 不涉及 | 不涉及 |
| | 隐式拒绝 | 身份策略 | 不涉及 | 身份策略 |

因此，如果您仅使用策略授权且进行了授权范围之外的操作，那么策略和身份策略的鉴权结果都将是隐式拒绝，所以提示信息中的授权项将来源于身份策略。此时，如果您不想使用身份策略授权，但是您又在策略中找不到该授权项，则说明提示信息中的身份策略授权项有一个策略授权项别名，且该身份策略授权项与其别名不一致，可以通过在策略中授予这个身份策略授权项别名来进行解决，身份策略授权项与其别名的对应关系请详见**身份策略授权参考**。

# 1.6 身份策略与策略如何兼容

对于IAM目前支持的角色与策略权限模型和身份策略权限模型来说，他们既相互隔离但又用法类似。

推荐新注册的华为云账号仅使用身份策略进行授权管理，可以实现更加安全和精细化的权限控制。但是，存量的账号可能会同时使用角色与策略权限模型和身份策略权限

模型进行授权管理。也就是说一个IAM身份可能会被同时授予多个IAM权限，包含系统角色、系统策略、自定义策略、系统身份策略和自定义身份策略等，这些权限可以同时生效。其中，系统角色是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，不具有可配置性，用户根据自己的业务需求实际选择即可。而系统策略、自定义策略、系统身份策略和自定义身份策略在使用上则更加细粒度，它们的混合使用较为复杂。

对于策略和身份策略来说，最主要的是选择业务所需要的授权项。以IAM为例，与IAM服务相关的全部的授权项请参见**权限和授权项**，其中在“策略授权参考”中包含了策略授权项与支持的API的对应关系，在身份策略授权参考中包含了身份策略授权项与支持的API的对应关系。为了在身份策略中兼容使用原本仅支持策略授权项的API，IAM在身份策略中增加了能够对这些API进行操作的部分身份策略授权项。在这些身份策略授权项中，因为命名规范原因，一部分沿用了原来符合规范的策略授权项，另外一部分则是对原来不符合规范的策略授权项进行了重命名。因为进行了重命名，所以称原来的策略授权项为现在身份策略授权项的别名。

对于IAM服务来说，直接使用原有策略授权项作为身份策略授权项的列表见**表1-1**，对策略授权项进行重命名作为身份策略授权项的列表见**表1-2**。

**表 1-1** IAM 直接使用策略授权项作为身份策略授权项的列表

| 身份策略授权项 | 访问级别 | 策略授权项 |
| --- | --- | --- |
| iam:identityProviders:listMappings | 列表 | iam:identityProviders:listMappings |
| iam:identityProviders:getMapping | 读 | iam:identityProviders:getMapping |
| iam:identityProviders:createMapping | 写 | iam:identityProviders:createMapping |
| iam:identityProviders:deleteMapping | 写 | iam:identityProviders:deleteMapping |
| iam:identityProviders:updateMapping | 写 | iam:identityProviders:updateMapping |
| iam:identityProviders:listProtocols | 列表 | iam:identityProviders:listProtocols |
| iam:identityProviders:getProtocol | 读 | iam:identityProviders:getProtocol |
| iam:identityProviders:createProtocol | 写 | iam:identityProviders:createProtocol |
| iam:identityProviders:deleteProtocol | 写 | iam:identityProviders:deleteProtocol |
| iam:identityProviders:updateProtocol | 写 | iam:identityProviders:updateProtocol |
| iam:securityPolicies:getProtectPolicy | 读 | iam:securityPolicies:getProtectPolicy |

| 身份策略授权项 | 访问级别 | 策略授权项 |
| --- | --- | --- |
| iam:securityPolicies:updateProtectPolicy | 写 | iam:securityPolicies:updateProtectPolicy |
| iam:securityPolicies:getPasswordPolicy | 读 | iam:securityPolicies:getPasswordPolicy |
| iam:securityPolicies:updatePasswordPolicy | 写 | iam:securityPolicies:updatePasswordPolicy |
| iam:securityPolicies:getLoginPolicy | 读 | iam:securityPolicies:getLoginPolicy |
| iam:securityPolicies:updateLoginPolicy | 写 | iam:securityPolicies:updateLoginPolicy |
| iam:securityPolicies:getConsoleAclPolicy | 读 | iam:securityPolicies:getConsoleAclPolicy |
| iam:securityPolicies:updateConsoleAclPolicy | 写 | iam:securityPolicies:updateConsoleAclPolicy |
| iam:securityPolicies:getApiAclPolicy | 读 | iam:securityPolicies:getApiAclPolicy |
| iam:securityPolicies:updateApiAclPolicy | 写 | iam:securityPolicies:updateApiAclPolicy |

**表 1-2** 身份策略授权项与策略授权项对应关系的列表

| 身份策略授权项 | 访问级别 | 策略授权项（身份策略授权项的别名） |
| --- | --- | --- |
| iam::listAccessKeys | 列表 | iam:credentials:listCredentials |
| iam::createAccessKey | 写 | iam:credentials:createCredential |
| iam::getAccessKey | 读 | iam:credentials:getCredential |
| iam::updateAccessKey | 写 | iam:credentials:updateCredential |
| iam::deleteAccessKey | 写 | iam:credentials:deleteCredential |
| iam:projects:list | 列表 | iam:projects:listProjects |
| iam:projects:create | 写 | iam:projects:createProject |
| iam:projects:listForUser | 列表 | iam:projects:listProjectsForUser |
| iam:projects:update | 写 | iam:projects:updateProject |
| iam:groups:list | 列表 | iam:groups:listGroups |
| iam:groups:create | 写 | iam:groups:createGroup |
| iam:groups:get | 读 | iam:groups:getGroup |

| 身份策略授权项 | 访问级别 | 策略授权项（身份策略授权项的别名） |
| --- | --- | --- |
| iam:groups:delete | 写 | iam:groups:deleteGroup |
| iam:groups:update | 写 | iam:groups:updateGroup |
| iam:groups:removeUser | 写 | iam:permissions:removeUserFromGroup |
| iam:groups:listUsers | 列表 | iam:users:listUsersForGroup |
| iam:groups:checkUser | 读 | iam:permissions:checkUserInGroup |
| iam:groups:addUser | 写 | iam:permissions:addUserToGroup |
| iam:users:create | 写 | iam:users:createUser |
| iam:users:get | 读 | iam:users:getUser |
| iam:users:update | 写 | iam:users:updateUser |
| iam:users:list | 列表 | iam:users:listUsers |
| iam:users:delete | 写 | iam:users:deleteUser |
| iam:users:listGroups | 列表 | iam:groups:listGroupsForUser |
| iam:users:listVirtualMFADevices | 列表 | iam:mfa:listVirtualMFADevices |
| iam:users:createVirtualMFADevice | 写 | iam:mfa:createVirtualMFADevice |
| iam:users:deleteVirtualMFADevice | 写 | iam:mfa:deleteVirtualMFADevice |
| iam:users:getVirtualMFADevice | 读 | iam:mfa:getVirtualMFADevice |
| iam:users:bindVirtualMFADevice | 写 | iam:mfa:bindMFADevice |
| iam:users:unbindVirtualMFADevice | 写 | iam:mfa:unbindMFADevice |
| iam:identityProviders:list | 列表 | iam:identityProviders:listIdentityProviders |
| iam:identityProviders:get | 读 | iam:identityProviders:getIdentityProvider |
| iam:identityProviders:create | 写 | iam:identityProviders:createIdentityProvider |
| iam:identityProviders:delete | 写 | iam:identityProviders:deleteIdentityProvider |

| 身份策略授权项 | 访问级别 | 策略授权项（身份策略授权项的别名） |
| --- | --- | --- |
| iam:identityProviders:update | 写 | iam:identityProviders:updateIdentityProvider |
| iam:identityProviders:getSAMLMetadata | 读 | iam:identityProviders:getIDPMetadata |
| iam:identityProviders:createSAMLMetadata | 写 | iam:identityProviders:createIDPMetadata |
| iam:identityProviders:getOIDCConfig | 读 | iam:identityProviders:getOpenIDConnectConfig |
| iam:identityProviders:createOIDCConfig | 写 | iam:identityProviders:createOpenIDConnectConfig |
| iam:identityProviders:updateOIDCConfig | 写 | iam:identityProviders:updateOpenIDConnectConfig |
| iam:users:listLoginProtectSettings | 列表 | iam:users:listUserLoginProtects |
| iam:users:getLoginProtectSetting | 读 | iam:users:getUserLoginProtect |
| iam:users:updateLoginProtectSetting | 写 | iam:users:setUserLoginProtect |
| iam:quotas:list | 列表 | iam:quotas:listQuotas |
| iam:quotas:listForProject | 列表 | iam:quotas:listQuotasForProject |

在**表1-2**中策略授权项也就是身份策略授权参考中的别名。这两种方式都可以实现利用身份策略授权项对原本仅支持策略授权项的API进行控制，例如使用**表1-1**中的iam:identityProviders:listMappings授权项时，在IAM新版控制台中创建授予iam:identityProviders:listMappings身份策略授权项的身份策略，可以实现对原本仅支持策略授权项的**GET /v3/OS-FEDERATION/mappings**接口进行控制，来查询身份提供商的映射列表，操作步骤请参阅**创建自定义身份策略**。

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

这与在IAM旧版控制台中创建授予iam:identityProviders:listMappings策略授权项的策略效果一致，操作步骤请参阅**创建自定义策略**。

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

```
        "Effect": "Allow",
        "Action": [
            "iam:identityProviders:listMappings"
        ]
    }]
}
```

而在使用**表1-2**中的iam::listAccessKeys授权项时，在IAM新版控制台中创建授予iam::listAccessKeys身份策略授权项的身份策略，可以实现原本仅支持策略授权项的GET /v3.0/OS-CREDENTIAL/credentials接口进行控制，来查询所有永久访问密钥：

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

这与在IAM旧版控制台中创建授予iam:credentials:listCredentials策略授权项的策略效果一致：

```
{
    "Version": "1.1",
    "Statement": [{
        "Effect": "Allow",
        "Action": [
            "iam:credentials:listCredentials"
        ]
    }]
}
```

# 1.7 仅使用企业项目授权但无法找到错误提示信息中的授权项

## 问题描述

用户在仅使用企业项目授权的场景下进行某项操作时提示无权限，在策略中无法找到该错误提示信息中的授权项。

## 可能原因

支持查询所有企业项目绑定的资源列表的接口如果是由身份策略或强制访问控制策略（如服务控制策略等）显式拒绝，则提示身份策略授权项被拒绝的信息，否则会按照策略授权项错误信息返回。示例如下：

IAM用户在IAM新版控制台未授权ces:siteMonitorRule:list权限，在调用对应接口时返回ces:remoteChecks:list无权限，例如报错信息为："Policy doesn't allow ces:remoteChecks:list to be performed"。其中，ces:siteMonitorRule:list是身份策略授权项，ces:remoteChecks:list是策略授权项。

## 解决方法

如用户需使用企业项目授权，则使用IAM旧版控制台中企业项目视图授权，对目标企业项目下的资源授予对应所需的权限；如不希望使用企业项目授权，则可在IAM新版控制台直接使用身份策略，或在IAM旧版控制台的IAM项目视图下使用策略进行授权。

# 1.8 拥有仅查看某企业项目资源权限的用户可以查看到账号下所有的资源

## 问题描述

某公司中存在企业项目A、B和C，管理员使用企业项目授权为某用户授予仅能查看企业项目A的权限，而后管理员在为该用户授予查看资源的身份策略后，用户可以查看到账号下企业项目A、B和C中的所有资源。

## 可能原因

该用户被授予允许查看资源的身份策略后，实际效果为可以查看账号下的所有资源。

## 解决方法

如希望该用户仅能查看企业项目授权中允许查看的资源，需要解绑身份策略，仅使用企业项目视图授权即可。

# 1.9 在身份策略中使用 NotAction 时权限不符合预期怎么办

## 问题描述

管理员在IAM新版控制台创建Deny语句的身份策略时，使用NotAction排除A云服务授权项之后，发现B云服务的授权项并没有被Deny限制。例如组织中成员账号拥有所有云服务权限时，管理员在创建Deny语句身份策略时使用NotAction排除VPC服务授权项后，发现EIP服务授权项没有被Deny限制。对应的身份策略示例如下：

```
{
    "Version": "5.0",
    "Statement": [{
        "Effect": "Deny",
        "NotAction": [
            "VPC:*:*"
        ]
    }]
}
```

## 可能原因

A云服务的某些授权项是B云服务某些授权项的别名。例如，EIP服务为兼容旧版控制台权限，会将VPC服务某些授权项作为EIP服务某些授权项的别名。在身份策略鉴权时，存在别名关系的授权项代表的含义是相同的，因此VPC授权项也会被当做EIP授权项，在配置NotAction排除VPC授权项后，实际上EIP授权项也被排除了，因此EIP授权项最终未被Deny限制。

## 解决方法

针对如上场景，如果用户需要Allow A云服务且同时Deny B云服务的授权项，那么在使用NotAction排除A云服务授权项时，还需要单独添加一条明确的Deny语句来拒绝B云服务的授权项。例如用户通常需要允许VPC且拒绝EIP的授权项，那么可以在Deny时通过NotAction来排除VPC授权项，然后再单独添加一条明确的Deny语句来拒绝EIP授权项。对应的身份策略示例如下：

```
{
   "Version": "5.0",
   "Statement": [{
         "Effect": "Deny",
         "NotAction": [
            "VPC:*:*"
         ]
      },
      {
         "Effect": "Deny",
         "Action": [
            "EIP:*:*"
         ]
      }
   ]
}
```

# 1.10 支持使用全局条件键 g:CalledVia 的云服务有哪些

以下服务支持使用全局条件键g:CalledVia：

**表 1-3** 支持 g:CalledVia 的云服务列表

| 云服务名称 | 云服务主体 |
| --- | --- |
| DDoS防护（AAD） | service.AAD |
| 访问分析（Access Analyzer） | service.AccessAnalyzer |
| 应用运维管理（AOM） | service.AOM |
| API网关（APIG） | service.APIG |
| 弹性伸缩（AS） | service.AS |
| 费用中心（Billing） | service.BILLING |
| 云堡垒机（CBH） | service.CBH |
| 云备份（CBR） | service.CBR |
| 云连接（CC） | service.CC |
| 云容器引擎（CCE） | service.CCE |
| 内容分发网络（CDN） | service.CDN |
| 云监控服务（CES） | service.CES |
| 云防火墙（CFW） | service.CFW |
| DDoS原生高级防护（CNAD） | service.CNAD |
| 云运维中心（COC） | service.COC |
| 软件开发生产线（CodeArts） | service.CODEARTS |
| 流水线（CodeArts Pipeline） | service.CodeArtsPipeline |
| 微服务引擎（CSE） | service.CSE |

| 云服务名称 | 云服务主体 |
| --- | --- |
| 凭据管理服务（CSMS） | service.CSMS |
| 云搜索服务（CSS） | service.CSS |
| 云审计服务（CTS） | service.CTS |
| 数据治理中心（DataArts Studio） | service.DataArtsStudio |
| 数据库安全服务（DBSS） | service.DBSS |
| 云专线（DC） | service.DCAAS |
| 分布式缓存服务（DCS） | service.DCS |
| 文档数据库服务（DDS） | service.DDS |
| 专属加密服务（DHSM） | service.DHSM |
| 数据湖探索（DLI） | service.DLI |
| 云解析服务（DNS） | service.DNS |
| 数据复制服务（DRS） | service.DRS |
| 数据安全中心（DSC） | service.DSC |
| 数据仓库服务GaussDB（DWS） | service.DWS |
| 弹性公网IP（EIP） | service.EIP |
| 弹性负载均衡（ELB） | service.ELB |
| 企业管理（EPS） | service.EPS |
| 企业路由器（ER） | service.ER |
| 云硬盘（EVS） | service.EVS |
| 全球加速（GA） | service.GA |
| 云数据库（GaussDB） | service.GaussDB |
| 云数据库（TaurusDB） | service.GaussDBforMySQL |
| 企业主机安全（HSS） | service.HSS |
| 统一身份认证（IAM） | service.IAM |
| IAM身份中心（IdentityCenter） | service.IdentityCenter |
| 镜像服务（IMS） | service.IMS |
| 设备接入（IoTDA） | service.IoTDA |
| 密钥管理服务（KMS） | service.KMS |
| 密钥对管理服务（KPS） | service.KPS |
| 云日志服务（LTS） | service.LTS |

| 云服务名称 | 云服务主体 |
| --- | --- |
| MapReduce服务（MRS） | service.MRS |
| NAT网关（NAT） | service.NAT |
| 对象存储迁移服务（OMS） | service.OMS |
| 组织（Organizations） | service.Organizations |
| 私有证书管理服务（PCA） | service.PCA |
| 资源访问管理（RAM） | service.RAM |
| 云数据库（RDS） | service.RDS |
| 资源编排服务（RFS） | service.RF |
| | service.RFStackSets |
| | service.RFStackSetsOrgMember |
| 资源治理中心（RGC） | service.RGC |
| 配置审计（Config） | service.RMSMultiAccountSetup |
| | service.RMSConforms |
| | service.RMSRemediation |
| SSL证书管理服务（SCM） | service.SCM |
| 安全云脑（SecMaster） | service.SecMaster |
| 应用管理与运维平台（ServiceStage） | service.ServiceStage |
| 消息通知服务（SMN） | service.SMN |
| 主机迁移服务（SMS） | service.SMS |
| 容器镜像服务（SWR） | service.swr |
| 标签管理服务（TMS） | service.TMS |
| 虚拟私有云（VPC） | service.VPC |
| VPC终端节点（VPCEP） | service.VPCEP |
| Web应用防火墙（WAF） | service.WAF |
| 云桌面（Workspace） | service.Workspace |

其中，资源编排服务（RFS）和配置审计服务（Config）有多个服务主体。

在资源编排服务（RFS）中：

- service.RF用于跨服务转发访问时以及代入云服务委托后通过用户模板中定义的云服务创建、更新或删除相应云服务资源。

- service.RFStackSets用于代入云服务委托后通过Organizations查询组织单元、成员信息或组织管理员通过IAM获取成员账号的信任委托临时凭据。
- service.RFStackSetsOrgMember用于代入云服务委托后通过IAM创建用于在资源栈集服务管理场景下各组织成员账号的信任委托以及为信任委托添加策略。

在配置审计服务（Config）中：

- service.RMSMultiAccountSetup用于跨服务转发访问时通过IAM创建用于组织合规规则和组织合规规则包创建或更新场景的服务关联委托，以及代入云服务委托后通过SMN发送资源变更通知或通过OBS转储资源快照。
- service.RMSConforms用于跨服务转发访问时通过IAM创建用于合规规则包创建或更新场景的服务关联委托。
- service.RMSRemediation用于跨服务转发访问时通过IAM创建用于合规修正配置创建或更新场景的服务关联委托。

# 1.11 身份策略拒绝访问错误信息

当用户为通过身份策略授权某些权限或通过身份策略等显式禁止某些权限时，一般会收到IAM提供的鉴权错误提示；用户可基于鉴权错误提示明确此次访问被拒绝的原因，从而排除故障。

## 隐式拒绝与显式拒绝

由于鉴权导致访问被拒绝可分为两种情况：隐式拒绝和显式拒绝。

隐式拒绝表明此次访问未得到管理员的明确授权。错误提示通常包含以下信息：

```
User: ${principal} is not authorized to perform: ${action} on resource: ${resource} because no ${policy_type} policy allows the ${action} action.
```

显式拒绝表明此次访问受管理员的明确限制。错误提示通常包含以下信息：

```
User: ${principal} is not authorized to perform: ${action} on resource: ${resource} with an explicit deny in the ${policy_type} policy.
```

| | |
|---|---|
| ${principal} | 主体 |
| ${action} | 访问执行操作 |
| ${resource} | 被访问资源 |
| ${policy_type} | 策略类型 |

## 错误信息示例

- **策略或身份策略隐式拒绝**

  此次访问未得到明确授权，没有附加到该主体上明确授权此次访问的策略或身份策略。

  检查附加到该主体上的策略或身份策略是否缺失对应访问执行操作的“Allow”语句，通过IAM管理员配置对应的权限。

  ```
  User: ${principal} is not authorized to perform: ${action} on resource: ${resource} because no identity-based policy allows the ${action} action.
  ```

- **策略或身份策略显式拒绝**

此次访问受到明确限制，有附加到该主体上明确禁止此次访问的策略或身份策略。

检查附加到该主体上的策略或身份策略是否有对应访问执行操作的“Deny”语句，通过IAM管理员去除对应的限制。

```
User: ${principal} is not authorized to perform: ${action} on resource: ${resource} with an explicit deny in an identity-based policy.
```

- **资源策略隐式拒绝**

  此次访问未得到明确授权，没有基于资源明确授权此次访问的资源策略。

  检查基于资源的策略是否缺失对应访问执行操作的“Allow”语句，配置对应的权限。

  ```
  User: ${principal} is not authorized to perform: ${action} on resource: ${resource} because no resource-based policy allows the ${action} action.
  ```

- **资源策略显式拒绝**

  此次访问受到明确限制，有基于资源明确禁止此次访问的资源策略。

  检查基于资源的策略是否有对应访问执行操作的“Deny”语句，去除对应的限制。

  ```
  User: ${principal} is not authorized to perform: ${action} on resource: ${resource} with an explicit deny in a resource-based policy.
  ```

- **信任策略隐式拒绝**

  此次访问未得到明确授权，委托中没有明确授权此次访问的信任策略。

  检查信任委托中的信任策略是否缺失对应访问执行操作的“Allow”语句，配置对应的权限；或检查委托中的委托对象。

  ```
  User: ${principal} is not authorized to perform: ${action} on resource: ${resource} because no agency trust policy allows the ${action} action.
  ```

- **信任策略显式拒绝**

  此次访问受到明确限制，委托中有明确禁止此次访问的信任策略。

  检查委托中的信任策略是否有对应访问执行操作的“Deny”语句，去除对应的限制。

  ```
  User: ${principal} is not authorized to perform: ${action} on resource: ${resource} with an explicit deny in the agency trust policy.
  ```

- **会话策略隐式拒绝**

  此次访问未得到明确授权，委托会话中没有明确授权此次访问的会话策略。

  检查委托会话中的会话策略是否缺失对应访问执行操作的“Allow”语句，配置对应的权限。

  ```
  User: ${principal} is not authorized to perform: ${action} on resource: ${resource} because no session policy allows the ${action} action.
  ```

- **会话策略显式拒绝**

  此次访问受到明确限制，委托会话中有明确禁止此次访问的会话策略。

  检查委托会话中的会话策略是否有对应访问执行操作的“Deny”语句，去除对应的限制。

  ```
  User: ${principal} is not authorized to perform: ${action} on resource: ${resource} with an explicit deny in a session policy.
  ```

- **服务控制策略隐式拒绝**

  此次访问未得到明确授权，没有附加到该主体所属租户或所属组织根目录或组织单元的明确授权此次访问的服务控制策略。

  检查附加到该主体所属租户或所属组织根目录或组织单元的服务控制策略是否缺失对应访问执行操作的“Allow”语句，通过组织管理员配置对应的权限。

  ```
  User: ${principal} is not authorized to perform: ${action} on resource: ${resource} because no service control policy allows the ${action} action.
  ```

- **服务控制策略显式拒绝**

  此次访问受到明确限制，有附加到该主体所属租户或所属组织根目录或组织单元的明确禁止此次访问的服务控制策略。

  检查附加到该主体所属租户或所属组织根目录或组织单元的服务控制策略是否有对应访问执行操作的“Deny”语句，通过组织管理员去除对应的限制。

  ```
  User: ${principal} is not authorized to perform: ${action} on resource: ${resource} with an explicit deny in a service control policy.
  ```

# 2 IAM 用户管理类

## 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”，切换登录入口。


  b. 可能原因：手机号/邮箱地址/账号名/原华为云账号和IAM用户名输入错误。

  解决方法：输入正确的手机号/邮箱地址/账号名/原华为云账号和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”**

  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地址或网段访问华为云。

  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华为云或由管理员修改访问控制规则。详情请参考：**访问控制**。

# 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“登录验证策略”页签。

**说明**

仅对账号下的IAM用户生效，对账号本身不生效。

**步骤3** 在“登录验证策略”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。
- “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**

# 3 安全设置类

## 3.1 如何设置登录验证

为了确保您信息的安全，您可以通过绑定的MFA设备设置登录验证。

绑定MFA设备后，账号或IAM用户登录控制台时，需要在“登录验证”页面进行MFA设备验证。

解绑MFA设备后，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

**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IAM用户名称，进入用户详情界面。

**步骤3** 选择“安全设置”页签，找到“多因素认证设备”。

**步骤4** 单击“添加MFA设备”。

**步骤5** 指定MFA设备名称。仅支持大小写字母、数字或特殊字符(-_)。

**步骤6** 根据**如何绑定虚拟MFA**进行虚拟MFA绑定或根据**如何绑定硬件MFA**进行硬件MFA绑定。

**----结束**

## 3.2 如何关闭登录验证

为了确保您信息的安全，您可以通过绑定虚拟MFA设备设置登录验证。

绑定MFA设备后，账号或IAM用户登录控制台时，需要在“登录验证”页面进行MFA设备验证。

解绑MFA设备后，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

**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IAM用户名称，进入用户详情界面。

**步骤3** 选择“安全设置”页签，找到“多因素认证设备”。

**步骤4** 单击MFA设备“操作”列的“解绑”。

**步骤5** 在弹出的对话框中，输入“YES”。以下以解绑虚拟MFA为例。

**图 3-1** 确认解绑


**步骤6** 单击“确定”，验证成功后，完成解绑MFA设备操作。

**----结束**

# 3.3 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号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，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：华为云App、 Google Authenticator等），才能绑定虚拟MFA设备。

## 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。

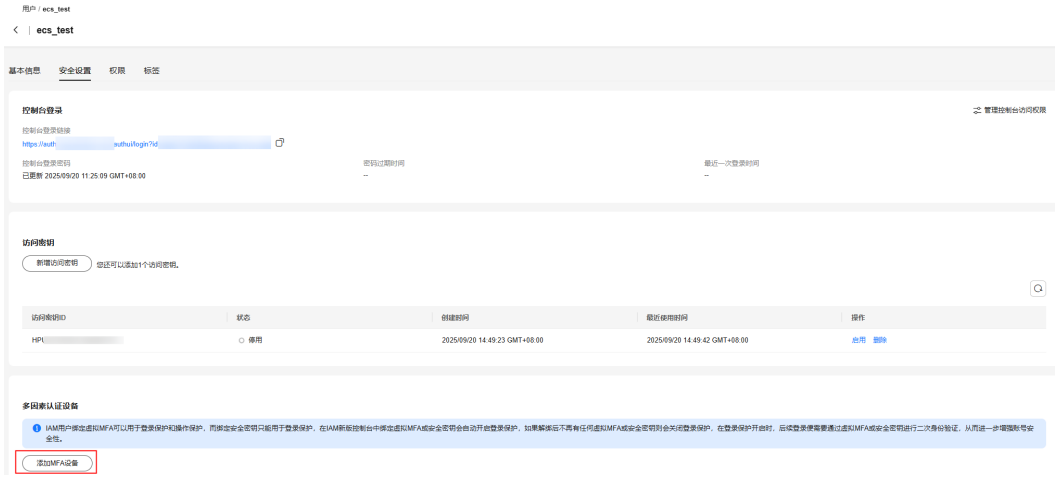
**步骤2** 单击IAM用户名称，进入用户详情界面。

**步骤3** 选择“安全设置”页签，找到“多因素认证设备”。

**步骤4** 单击“添加MFA设备”。

**图 3-2** 添加 MFA 设备




**步骤5** 指定MFA设备名称。仅支持大小写字母、数字或特殊字符(-_)。

**步骤6** 选择MFA设备。

**步骤7** 根据绑定虚拟MFA的页面，在您的MFA应用程序中添加用户。

**步骤8** 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9** 在“设置设备”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。

**步骤10** 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。

**----结束**

## 相关 FAQ

**3.4 如何获取虚拟MFA验证码**

**3.5 如何解绑虚拟MFA**

**3.7 虚拟MFA验证码校验不通过怎么办**

# 3.4 如何获取虚拟 MFA 验证码

绑定虚拟MFA后，用户在进行登录操作时，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，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。

**说明**

如果虚拟MFA验证码校验不通过，请参考：**3.7 虚拟MFA验证码校验不通过怎么办**。

# 3.5 如何解绑虚拟 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，请参考本章节。

解绑后，如需再次绑定虚拟MFA，请IAM用户在“账号安全设置”中自行重新绑定，详细操作请参见：**3.3 如何绑定虚拟MFA设备**。

## 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IAM用户名称，进入用户详情界面。

**步骤3** 选择“安全设置”页签，找到“多因素认证设备”。

**步骤4** 单击虚拟MFA设备“操作”列的“解绑”。

**步骤5** 在弹出的对话框中，输入“YES”。

**图 3-3** 确认解绑


**步骤6** 单击“确定”，验证成功后，完成解绑MFA操作。

**----结束**

# 3.6 MFA 设备丢失了怎么办

- 手机丢失、已删除虚拟MFA应用程序或丢失安全密钥的华为云账号或华为账号，请拨打免费客服电话4000-955-988反馈，客服人员会尽快为您重置MFA设备。
- 手机丢失、已删除虚拟MFA应用程序或丢失安全密钥的**IAM用户**，请联系管理员解绑MFA设备，管理员的操作步骤如下所示。

## 如何解绑虚拟 MFA

**步骤1** 进入**统一身份认证服务新版控制台**，在左侧导航栏选择“用户”页签。

**步骤2** 单击IAM用户名称，进入用户详情界面。

**步骤3** 选择“安全设置”页签，找到“多因素认证设备”。

**步骤4** 单击虚拟MFA设备“操作”列的“解绑”。

**步骤5** 在弹出的对话框中，输入“YES”。

**图 3-4** 确认解绑


**步骤6** 单击“确定”，完成解绑MFA操作。

**----结束**

## 如何解绑安全密钥

**步骤1** 进入**统一身份认证服务新版控制台**，在左侧导航栏选择“用户”页签。

**步骤2** 单击IAM用户名称，进入用户详情界面。

**步骤3** 选择“安全设置”页签，找到“多因素认证设备”。

**步骤4** 单击安全密钥设备“操作”列的“解绑”。

**步骤5** 在弹出的对话框中，输入“YES”。

**图 3-5** 确认解绑


**步骤6** 单击“确定”，完成解绑安全密钥。

**----结束**

# 3.7 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。）

# 3.8 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。
- 请确认短信验证码是否被视作垃圾短信而被拦截，您可以解除应用软件的短信拦截。

  **说明**

  请在手机短信中的“拦截短信”或“垃圾短信”中查找是否有华为云验证码相关短信。
- 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。

如果您的手机和邮箱均无法接收验证码，请您联系客服人员获取帮助。

### 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。
- 设置邮箱白名单：noreplyhk01@mail01.huawei.com；noreplydl01@mail01.huawei.com。
- 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。

如果您的手机和邮箱均无法接收验证码，请您联系客服人员获取帮助。

## 3.9 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”。

### 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**4.1 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**4.2 如何修改密码**。

# 3.10 添加 MFA 设备时提示该 MFA 设备已存在怎么办

## 问题描述

管理员在IAM新版控制台从“用户”列表进入需要添加MFA设备用户的“安全设置”中，在多因素认证设备处单击“添加MFA设备”，输入“设备名称”后单击“下一步”之后报错“该MFA设备已存在”。

## 可能原因

- 该用户已经绑定了一个IAM的MFA设备，同一个用户只允许绑定一个IAM的MFA设备。
- 在账号中有其他用户使用了相同的MFA设备名称，MFA设备名称需要在整个账号内是唯一的。

## 解决方法

在IAM新版控制台的“用户 > 安全设置 > 多因素认证设备”中查看该用户是否绑定MFA设备或者其他用户是否绑定了相同设备名称的MFA设备。

# 4 密码凭证类

## 4.1 忘记密码怎么办

如果您忘记了IAM用户的密码，请参考**忘记IAM用户密码**自行重置登录密码。

如果您忘记了账号的密码，请参考**忘记账号密码**自行重置登录密码。

**说明**

本节只介绍IAM用户、华为云账号、华为账号的找回密码方式。

如果找回密码的过程中，报错“此账号无效或不受支持”，说明该账号不是IAM用户、华为云账号或华为账号。请再次检查输入的账号是否正确。如果您暂未注册华为账号，建议您先注册华为账号并开通华为云，请参考**注册华为账号并开通华为云**。

### 忘记 IAM 用户密码

如果您是IAM用户且未绑定邮件地址或手机，将无法自行修改密码，请联系管理员修改密码，详情请参考：**修改IAM用户密码**。

**步骤1** 在华为账号登录页面，单击“IAM用户 > 忘记密码”。

**图 4-1** 忘记 IAM 用户密码


**步骤2** 输入需要重置密码的IAM用户的管理员账号、IAM用户名/邮件地址和验证码。

**图 4-2** 输入 IAM 用户信息


**说明**

- 账号：注册华为云时创建的账号，账号是资源的归属以及使用计费的主体，对其所拥有的资源具有完全控制权限，可以访问华为云所有云服务。使用账号登录后，在IAM的“用户”中可以看到账号对应的根用户，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用户名和密码登录华为云，并根据权限使用所属账号中的资源。IAM不拥有资源，不进行独立的计费，IAM用户的权限和资源由所属账号统一控制和付费。
- 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：**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**3.8 无法接收验证码怎么办**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”或倒计时结束返回登录页，使用新设置的密码登录华为云。

**----结束**

## 忘记账号密码

**步骤1** 在华为账号登录页面，单击“忘记密码”。

**图 4-3** 忘记华为账号密码


**步骤2** 输入账号名或注册账号的手机号/邮件地址，单击“下一步”。

**图 4-4** 输入信息


**步骤3** 如果您在2输入了注册账号的账号名/手机号/邮件地址，选择获取验证码。

**说明**

- 如果无法接收验证码，请参考**3.8 无法接收验证码怎么办**进行处理。
- 找回密码的账号手机号/邮件地址不可用时，请联系人工客服获取帮助：中国香港 +852800931122。

**步骤4** 按照界面提示填写验证信息，单击“下一步”。

**步骤5** 按照页面提示，输入新密码并确认密码，单击“确定”。

由于华为账号涉及多项业务领域，如华为账号无法按照以上步骤找回时，建议您参考以下链接进行找回：

**https://consumer.huawei.com/cn/support/content/zh-cn15774338/**

**步骤6** 单击“立即返回”，使用新设置的密码**登录华为云**。

**----结束**

# 4.2 如何修改密码

- 主动修改密码
  - 如果您的**华为云账号暂未升级成华为账号**，需要主动修改密码，可以在“基本信息”中修改自己的密码。
  - 如果您的**华为云账号已升级成华为账号**，需要主动修改密码，可以在“基本信息”中单击“华为账号信息”右侧的“前往管理”，前往**华为账号网站>账号与安全>安全中心**，重置账号密码。
  - 如果您是**IAM用户**，可以在控制台页面，鼠标移动至右上方的用户名，在下拉列表中选择“我的凭证”，在右上角选择“体验新版控制台”，在“登录密码”处修改您的用户密码。
- 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：**4.1 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，详情请参考：**修改IAM用户密码**。

# 4.3 如何获取访问密钥 AK/SK

- 如果您有登录密码，可以登录控制台，在“控制台”页面，鼠标移动至右上方的用户名，在下拉列表中选择“我的凭证”，单击右上角的“体验新版控制台”，接下来便可以在访问密钥列表中查看访问密钥ID（AK），在下载的.csv文件中查看秘密访问密钥（SK）。具体方法请参见：**管理访问密钥**。
- 如果您没有登录密码，不能登录控制台，在访问密钥异常丢失或者需要重置时，可以请管理员在IAM中生成您的访问密钥，并发送给您。方法请参见：**管理IAM用户的访问密钥**。

# 4.4 丢失访问密钥 AK/SK 怎么办

如果您的访问密钥AK/SK已丢失，可以删除该访问密钥AK/SK后，创建新的访问密钥AK/SK。具体方法请参见：**新增访问密钥**。

**说明**

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：**管理IAM用户的访问密钥**。
- 请管理员为您配置权限。如需配置权限请参见：**给IAM用户授权**。

# 4.5 为什么我无法添加安全密钥设备

## 问题描述

IAM用户在添加安全密钥设备时报错，导致无法绑定安全密钥进行登录保护。

## 可能原因

- 您没有添加安全密钥的权限。
- 您的设备不支持使用安全密钥。
- 您的浏览器版本过低。

## 解决方法

- 请检查您的IAM用户是否拥有安全密钥相关权限。例如，添加安全密钥需要iam:mfa:enableV5授权项，删除安全密钥需要iam:mfa:disableV5授权项，列举安全密钥需要iam:mfa:listMFADevicesV5授权项。
- 请检查是否有在Windows设置中开启Windows Hello，可以使用面部识别、指纹识别或PIN码来进行验证。如果不使用Windows Hello，您还可以使用支持FIDO2的硬件设备来进行验证。
- 请检查您的浏览器是否是最新版本，推荐使用最新的谷歌浏览器。请确保您的浏览器中不含有与WebAuthn不兼容的插件，请禁用任何可能不兼容的浏览器插件后重试。

# 4.6 如何获取“欧洲-都柏林”区域的访问密钥 AK/SK

## 问题描述

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

由于“欧洲-都柏林”区域用户属于联邦认证授权访问“欧洲-都柏林”云服务系统的虚拟用户，不是“欧洲-都柏林”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-都柏林”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-都柏林”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-都柏林”区域。
2. 在“欧洲-都柏林”区域控制台，选择“管理与部署>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-都柏林”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“安全设置”。
3. 在IAM用户详情“安全设置”页面，单击“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-都柏林”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**

# 4.7 如何通过禁用 Token 以达到只使用身份策略鉴权的目的

## 禁用 Token 的原因

Token类型凭证请求认证方式自带一些劣势：

- 使用Token认证时，身份策略授权将不会生效。
- Token相对临时访问密钥安全性更低。
- 用户身份权限信息静态固化在Token中，权限更新后需要重新获取Token。

## 禁用 Token 的相关接口

**表 4-1** 禁用 Token 的相关接口

| 方法 | 接口 | 身份策略授权项 | 接口说明 |
| --- | --- | --- | --- |
| POST | /v3/auth/tokens | iamToken::generatePkiToken | 获取Token |
| GET | /v3/auth/tokens | iamToken::validatePkiToken | 校验Token合法性 |

## 约束与限制

- 在禁用Token前，需要确认没有任何依赖Token的业务场景。否则禁用后会造成获取Token失败，从而导致业务功能受到影响。
- 不建议在身份策略中使用通配方式来达到禁用效果。

  以下身份策略示例对iamToken::*的通配形式进行了Deny。如果后续系统新增iamToken::xxx格式的授权项，也将会被这个身份策略预期外地禁用，存在潜在的风险。

  ```
  {
     "Version": "5.0",
     "Statement": [{
        "Effect": "Deny",
        "Action": [
           "iamToken::*"#不推荐使用通配形式进行Deny
        ]
     }]
  }
  ```

  建议策略只对具体的授权项进行Deny。例如您希望禁用获取Token的操作，建议您只对iamToken::generatePkiToken这个授权项进行Deny。

## 操作方式

- **身份策略方式**

  您可以在IAM新版控制台配置身份策略进行禁用获取Token。

  请参考**创建自定义身份策略**以及以下示例完成自定义身份策略的创建，并将**身份策略附加至授权主体**。

以下身份策略示例结合了g:DomainId条件键（可选），表示禁止该用户获取Token：

```
{
    "Version": "5.0",
    "Statement": [{
        "Effect": "Deny",
        "Action": [
            "iamToken::generatePkiToken"
        ],
        "Condition": {
            "StringEquals": {
                "g:DomainId": [
                    "xxxxxxxxxxxxxxxxxxxx"
                ]
            }
        }
    }]
}
```

- **SCP方式**

  您可以在组织服务控制台配置SCP进行禁用获取Token。

  请参考**创建SCP**以及以下示例完成SCP的创建，并**将SCP绑定至组织单元或成员账号**上。

  以下SCP示例结合了g:UserId条件键（可选），表示禁止该用户获取Token：

```
{
    "Version": "5.0",
    "Statement": [{
        "Effect": "Deny",
        "Action": [
            "iamToken::generatePkiToken"
        ],
        "Condition": {
            "StringEquals": {
                "g:UserId": [
                    "xxxxxxxxxxxxxxxxxxxx"
                ]
            }
        }
    }]
}
```

# 5 委托管理类

## 5.1 创建信任委托时提示权限不足怎么办

### 问题描述

IAM用户尝试进入IAM控制台创建信任委托时，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：

- 账号根用户：账号根用户可以使用所有服务，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“IAMFullAccessPolicy”系统身份策略的用户：具备该权限的用户为IAM管理员，可以使用IAM。

### 解决方法

- 请管理员创建信任委托，方法请参见：**创建信任委托**。
- 请管理员授予使用IAM服务的权限，方法请参见：**给IAM用户授权**。

## 5.2 切换信任委托后无法访问某些云服务的控制台和 API 怎么办

### 问题描述

账号A给账号B创建信了任委托，账号B切换信任委托后访问某些云服务的控制台和API报错。

## 可能原因

- 如果访问的云服务不支持信任委托，则切换后无法通过控制台或API访问该云服务，详情请参见：**支持身份策略与信任委托的云服务列表**。
- 如果访问的云服务支持信任委托，则可能是没有给该信任委托授予相应的云服务访问权限。
- 如果访问的云服务支持信任委托且授予了相应的云服务访问权限，则可能是该云服务的控制台或API间接访问了不支持信任委托的云服务。

## 解决方法

- 如果访问的云服务不支持信任委托，您可以选择创建委托并授予相应权限来访问该云服务，关于信任委托和委托的区别见**信任策略**。
- 如果访问的云服务支持信任委托，您需要检查是否给该信任委托授予了合适权限的身份策略。
- 如果访问的云服务时间接访问了不支持信任委托的云服务，您也可以选择创建委托并授予相应权限来访问该云服务。

# 6 账号管理类

## 6.1 账号登录失败怎么办

### 问题描述

账号登录华为云时，提示“账号或密码错误”。

### 可能原因

- 登录入口有误。
- 账号名输入有误。
- 密码输入有误。

### 解决方法

- 请选择正确的登录入口。请确认您输入的账号为华为账号或华为云账号，如果您已升级华为账号，请进入“华为账号登录”入口，如**图1**。如果您暂未升级华为账号，请进入“华为云账号登录”入口，如**图2**。
- 如果您是IAM用户，请进入“IAM用户登录”入口。如果您登录失败，请参考：**2.1 IAM用户登录失败怎么办**。

**图 6-1** 华为账号登录


**图 6-2** 华为云账号

- “华为账号登录”方式登录华为云时，支持使用**手机号、邮件地址、华为账号名、华为云账号名**登录。“华为云账号登录”方式登录时，支持使用**华为云账号名、邮件地址**登录。
  - 如果您已注册华为账号，请输入华为账号绑定的手机号/邮件地址/华为账号名登录华为云，详情请参考：**华为账号登录华为云**。
  - 如果您未注册华为账号、已注册华为云账号，且华为云账号暂未升级华为账号，请输入原华为云账号名登录。
- 如您通过华为账号登录，请输入华为账号的密码。如您通过华为云账号登录，请输入华为云账号的密码。

# 6.2 华为云账号、华为账号、IAM 用户、企业联邦用户的关系

本文为您介绍华为云常见账号的基本概念、各账号之间的关系和区别。

## 华为云有哪些账号

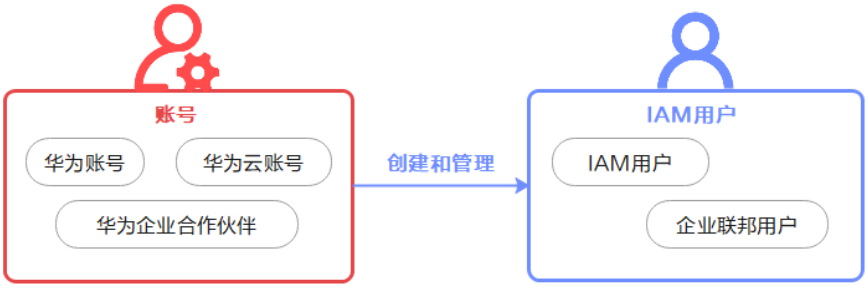
华为云账号体系主要分为两类：

- **账号**：在华为云注册或创建的账号。拥有华为云最高权限，可以访问拥有的所有资源并为资源付费。账号包括华为账号、华为云账号。
- **IAM用户**：由账号在统一身份认证服务（IAM）中创建，由账号管理，权限由账号分配，使用资源产生的费用由账号支付，按照账号授予的权限使用资源。

账号与IAM用户可以类比为父子关系。

您可以通过华为账号、华为云账号、华为网站账号、华为企业合作伙伴账号登录华为云，以账号的身份使用拥有的资源和云服务。

如果您是账号创建的IAM用户，可以分别通过IAM用户入口登录华为云，根据账号授予的权限使用资源和云服务。




## 华为账号

注册一个华为账号，即可访问华为云、华为商城等所有华为服务。

**注册**：在任意华为服务网站注册华为账号，如**华为账号网站**。

**登录华为云**：“华为账号”登录入口。初次使用华为账号登录华为云，请按照指引开通华为云业务或绑定已有华为云账号，后续可以直接登录。


## 华为云账号

华为云专属账号，仅能登录华为云，无法登录其他华为服务。

**注册**：2021年10月30日之前在华为云注册的账号。为了统一账号，提升登录体验，当前在华为云只能注册华为账号。

**登录华为云**：“华为账号”、“华为云账号”登录入口。


## IAM 用户

华为云资源的使用者，根据账号授予的权限使用账号中的资源。

**创建**：账号在IAM中创建IAM用户，详情请参考：**创建IAM用户**。

**登录华为云**：“IAM用户”登录入口。


### 其他

如果您已有**华为企业合作伙伴**账号，可以使用该账号登录华为云，登录成功后以账号的身份访问华为云。

## 6.3 升级华为账号失败怎么办

### 问题描述

将您的华为云账号升级成为华为账号时，系统提示升级失败。

### 可能原因

1. 可能原因：您已使用相同手机号码或邮件地址分别注册了华为云账号和华为账号，且未使用华为账号登录开通过华为云。

   解决方法：请退出当前的华为云账号登录，重新使用华为账号登录，然后选择关联已有的华为云账号。
2. 可能原因：您已注册**多个**华为云账号和**一个**华为账号，已使用华为账号关联或开通了华为云，此时暂不支持将其他华为云账号升级为华为账号。

   解决方法：请登录时忽略升级提示，选择暂不升级，并通过华为云账号登录。
3. 可能原因：您已使用相同手机号码或邮件地址分别注册了华为云账号和华为账号，但注册国家或地区不同，暂不支持将该华为账号和华为云账号关联。

   解决方法：请登录时忽略升级提示，选择暂不升级，并通过华为云账号登录。
4. 可能原因：您已注册的华为账号已冻结。

   解决方法：请在“**华为账号网站>安全中心>解冻账号**”解冻账号后，重新升级。
5. 可能原因：您从电信运营商购买了回收后再次售卖的手机号码，之前曾有人用该号码注册了华为账号。

   解决方法：请在**华为账号网站**重新注册华为账号后，使用新华为账号登录关联您的华为云账号。

# 6.4 升级华为账号后，还可以用原华为云账号登录吗

- **您已经注册过华为账号**

  如果华为账号与华为云账号信息（手机号码、邮件地址、账号名）一致，可继续使用原华为云账号登录；如果华为账号与华为云账号的部分信息不一致，就不能用原华为云不一致的信息登录（例如：手机号码相同，邮件地址不同时，不能用原华为云账号中的邮件地址登录）。

- **您从未注册过华为账号**

  升级后账号登录信息不变，您可继续用原手机号码、邮件地址、账号名登录。

# 6.5 账号根用户没有权限怎么办

## 问题描述

使用账号根用户访问华为云时，接口或页面显示没有权限。

## 可能原因

您的账号可能是Organizations组织中的成员，组织管理员设置了服务控制策略（SCP）来限制您账号的权限，SCP会同时影响根用户的访问权限。

## 解决方法

进入Organizations控制台查看您账号所绑定的SCP策略是否有影响您使用，并联系您的组织管理员评估解绑对应的SCP策略。