

统一身份认证服务

# 快速入门

文档版本 15  
发布日期 2025-01-14



版权所有 © 华为技术有限公司 2025。保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

## 商标声明



HUAWEI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。

# 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 创建用户组并授权.....	1
2 创建 IAM 用户并登录.....	7

# 1 创建用户组并授权

## 操作场景

如果企业中不需要每个人都注册账号，则可以由企业的管理员注册一个账号，在这个账号下创建用户组并分配权限，然后将创建的IAM用户根据不同的职能加入到不同的用户组中，分发给企业的人员使用。关于账号和IAM用户的概念，详情请参见：[IAM基本概念](#)。

本章节以A公司Company-A使用IAM创建用户组并授权为例，帮助您快速了解，企业如何使用IAM完成服务权限的配置。

## 操作流程

操作步骤	说明
<a href="#">准备工作</a>	注册华为账号并完成实名认证。
<a href="#">步骤一：创建用户组</a>	完成创建一个用户组，授权的最小单位是用户组。
<a href="#">步骤二：给用户组授权</a>	给用户组授予策略或角色，后续加入用户组的用户可以获得相应的权限。

## 准备工作

如果您已有一个华为账号，请跳到[步骤一](#)。如果您还没有华为账号，请参考以下步骤创建。

1. 打开<https://www.huaweicloud.com/>，单击“注册”。
2. 根据提示信息完成注册，详细操作请参见“[注册华为账号并开通华为云](#)”。注册成功后，系统会自动跳转至您的个人信息界面。
3. 参考“[企业实名认证](#)”完成企业账号实名认证。

### 说明

因为统一身份认证服务为免费服务，因此无需为账号充值。

## 步骤一：创建用户组

**步骤1** A公司管理员，使用注册的华为账号登录华为云。

图 1-1 登录华为云



**步骤2** A公司管理员进入华为云“控制台”。

图 1-2 进入控制台



**步骤3** 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”。

图 1-3 进入统一身份认证



步骤4 在统一身份认证服务，左侧导航窗格中，单击“用户组”>“创建用户组”。

图 1-4 创建用户组



步骤5 在“创建用户组”界面，输入“用户组名称”为“开发人员组”。  
用户组名称只能包含中文、大小写字母、数字、空格或特殊字符(-\_)。

图 1-5 输入用户组信息



步骤6 单击“确定”，完成用户组创建。

返回用户组列表，创建成功的用户组“开发人员组”将会展示在用户组列表中。

----结束

## 步骤二：给用户组授权

A公司的开发人员需要使用的云服务为ECS和OBS，需要为“开发人员组”授予这两个服务的管理员权限。如需查看所有云服务的系统权限，请参见：[系统权限](#)。

**步骤1** 管理员确定该用户组中的用户所需的权限。

通过查看[系统权限](#)，需要设置的权限如表1所示。其中“权限作用范围”由该服务的物理部署位置决定。

- 区域项目级服务：如果在某个区域的项目中设置权限，则权限只在该项目中生效。例如：选择权限仅在区域的项目“华北-北京四”生效，则IAM用户将无权访问其他区域项目中的资源。
- 全局服务：全局服务部署时不区分区域，访问全局服务不需要切换区域。例如：授予对象存储服务（OBS）的权限后，IAM用户可以访问所有区域项目中的OBS资源。

表 1-1 所需权限

使用的服务	权限作用范围	设置权限
ECS	区域项目	ECS FullAccess
OBS	全局区域	OBS OperateAccess

**步骤2** 在用户组列表中，单击新建用户组“开发人员组”右侧的“授权”。

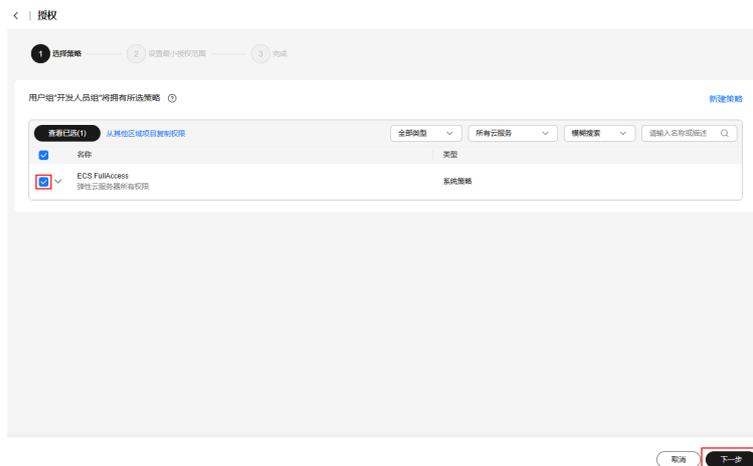
图 1-6 授权



**步骤3** 设置区域项目级服务的权限。

1. 由表1可知，ECS服务为区域项目级服务。勾选需要授予用户组的项目级服务权限，单击“下一步”。

图 1-7 勾选所需权限



2. 选择授权范围方案为“指定区域项目资源”，并选择“华北-北京四”，单击“确定”。

设置完成后，开发人员组仅在“华北-北京四”有访问权限，访问其它区域将提示没有权限。

图 1-8 指定权限生效的区域



**步骤4** 在用户组列表中，单击“开发人员组”右侧的“授权”。

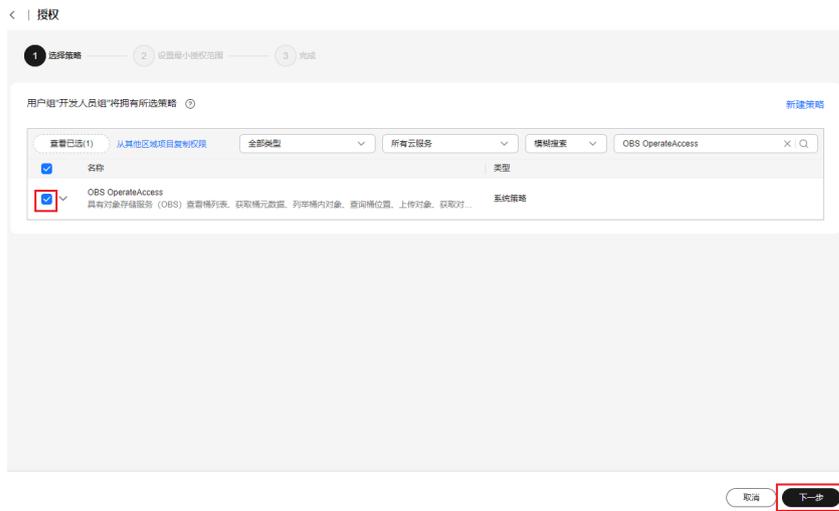
图 1-9 授权



**步骤5** 设置全局服务的权限。

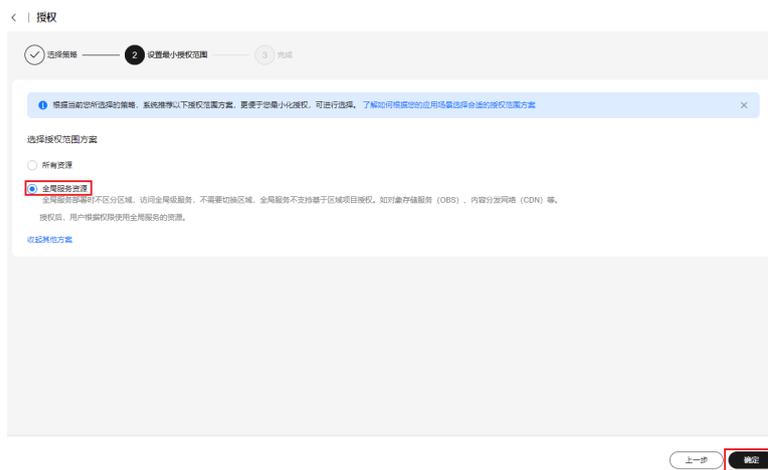
1. 勾选需要授予用户组的全局服务权限“OBS OperateAccess”，单击“下一步”。

图 1-10 勾选 OBS OperateAccess



2. 选择授权范围方案为“全局服务资源”，单击“确定”。

图 1-11 指定权限生效的区域



设置权限完成后，单击用户组“开发人员组”的名称，在授权记录页签下可以查看到已授予的权限。

### 📖 说明

授予OBS相关的权限后，大概需要等待15~30分钟策略才能生效。

---结束

# 2 创建 IAM 用户并登录

## 操作场景

上一个章节已完成用户组的创建，本章节将描述A公司使用已注册的账号Company-A，给公司成员创建IAM用户“Alice”并加入用户组“开发人员组”的操作，使得它拥有独立的用户和密码，IAM用户Alice可以独立登录华为云并使用权限范围内的资源。

## 操作流程

操作步骤	说明
<b>步骤一：创建IAM用户</b>	完成创建一个IAM用户，并将其加入用户组中获得相应的权限。
<b>步骤二：IAM用户登录控制台</b>	IAM用户登录控制台，使用权限范围内的资源。

## 步骤一：创建 IAM 用户

**步骤1** 在统一身份认证服务，左侧导航窗格中，单击“用户” > “创建用户”。

按照如下表格说明完成IAM必要参数设置，其他参数均可保持默认配置。

**步骤2** 配置基本信息。在“创建用户”界面填写“用户信息”和“访问方式”。

1. 输入用户名“Alice”。

图 2-1 配置用户信息

The screenshot shows the 'Create User' interface in the IAM console. It is divided into three steps: 1. Configure user basic information (selected), 2. Add user group (optional), and 3. Complete. Under step 1, there is a section for 'User Information' with a note: 'Username, email address, and mobile number can be used as login credentials for IAM users. We recommend that you fill in all of them.' Below this are several input fields: 'Username' (filled with 'Alice'), 'Email Address (optional)', 'Mobile Number (optional)' (with a dropdown for '+86 (China Mainland)'), 'Description (optional)', and 'External ID (optional)'. There is also a 'Delete' button. At the bottom, there is a note: 'Add user. You can still create 9 users this time.'

### 说明

您可以使用此处设置的用户名、邮件地址或手机号任意一种方式登录华为云。

表 2-1 用户信息

参数	示例	说明
用户名	Alice	必填。IAM用户登录华为云的用户名。 只能包含如下字符：大小写字母、空格、数字或特殊字符(-_)且不能以数字或空格开头。
邮件地址	暂不配置	“凭证类型”选择“首次登录时设置”时必填，选择其他时选填。IAM用户绑定的邮件地址，可作为登录凭证，也可由IAM用户自己绑定。
手机号	暂不配置	选填。IAM用户绑定的手机号，可作为IAM用户的登录凭证，也可由IAM用户自己绑定。

2. 配置“访问方式”。

图 2-2 配置访问方式



表 2-2 访问方式

访问方式	示例	说明
编程访问	勾选	为IAM用户启用访问密钥或密码，支持用户通过API、CLI、SDK等开发工具访问云服务。
管理控制台访问	勾选	为IAM用户启用密码，支持用户登录管理控制台访问云服务。此时凭证类型“密码”为必选项。

3. 配置“凭证类型”和“登录保护”。

图 2-3 配置凭证类型和登录保护

凭证类型  访问密钥  
创建用户成功后下载访问密钥。

密码

自定义

自动生成  
系统自动生成密码，创建用户完成后可下载。

首次登录时设置  
系统通过邮件发一次性登录链接给用户，用户使用该链接登录管理控制台并设置密码。

USB KEY  
绑定USB KEY，有效提升您的账号安全

\* 登录保护  开启登录保护（推荐）  
 不开启

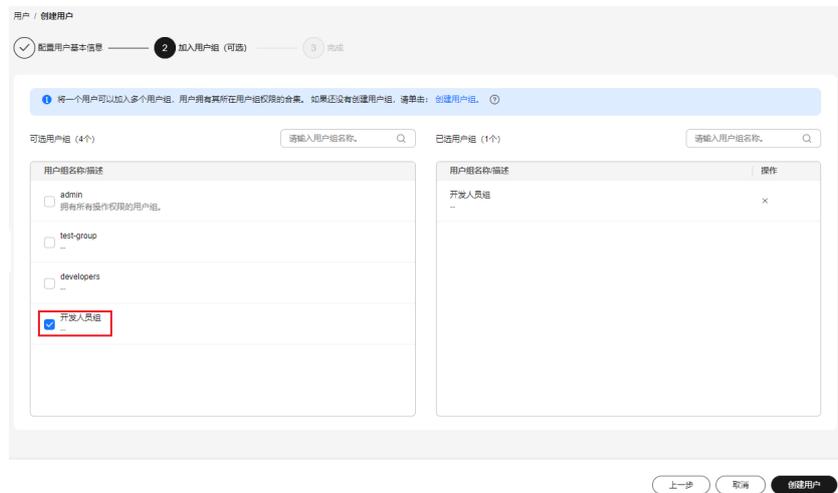
表 2-3 配置凭证类型和登录保护

凭证类型与登录保护	示例	说明
访问密钥	不勾选	访问密钥（AK/SK，Access Key ID/Secret Access Key）包含访问密钥ID（AK）和秘密访问密钥（SK）两部分，是您在华为云的长期身份凭证，您可以通过访问密钥对华为云API的请求进行签名。 创建用户完成后即可下载本次创建的所有用户的访问密钥（AK/SK）。
密码	自定义	- 自定义用户密码，并选择用户首次登录时是否需要重置密码。 如果您是用户的使用主体，建议您选择该方式，设置自己的登录密码，且无需勾选首次登录时重置密码。
	自动生成	选择 系统自动生成IAM用户的登录密码，创建完用户即可下载Excel形式的密码文件。将密码文件提供给用户，用户使用该密码登录。 密码文件需在创建完用户后及时下载，如取消下载将无法再次获取该密码文件。可以通过修改IAM用户密码重新设置用户密码。 仅在创建单个用户时适用。

凭证类型与登录保护		示例	说明
	首次登录时设置	-	系统通过邮件发一次性登录链接给用户，用户登录控制台并设置密码。 如果您不是用户的使用主体，建议选择该方式，同时输入用户的邮件地址和手机，用户通过邮件中的一次性链接登录华为云，自行设置密码。该链接7天内有效。
登录保护	开启登录保护	-	开启登录保护后，IAM用户登录时，除了在登录页面输入用户名和密码外（第一次身份验证），还需要在登录验证页面输入验证码（第二次身份验证）。 该功能是一种安全实践，您可以选择通过手机、邮件地址、虚拟MFA进行登录验证。
	不开启	<b>选择</b>	不开启登录保护。创建完成后，如需开启登录保护，请参见： <a href="#">登录保护</a> 。

**步骤3** 单击“下一步”，将Alice加入到上一步创建的用户组“开发人员组”中。

图 2-4 加入用户组



**步骤4** 单击“创建用户”，IAM用户创建完成。创建成功的IAM用户Alice将显示在新建用户列表中。

**步骤5** 单击“下载密码”。下载后，将账号名、IAM用户名Alice及下载的初始密码告知对应的员工。

图 2-5 下载密码



----结束

## 步骤二：IAM 用户登录控制台

A公司管理员完成IAM用户创建后，IAM用户Alice就可以使用账号名Company-A、用户名Alice及密码访问华为云。如果登录失败，可以联系[管理员重置密码](#)。

**步骤1** 在登录页面，单击登录下方的“IAM用户”，在“IAM用户登录”页面，输入“租户名/原华为云账号名”、“IAM用户名/邮件地址”和“IAM用户密码”。

图 2-6 IAM 用户登录

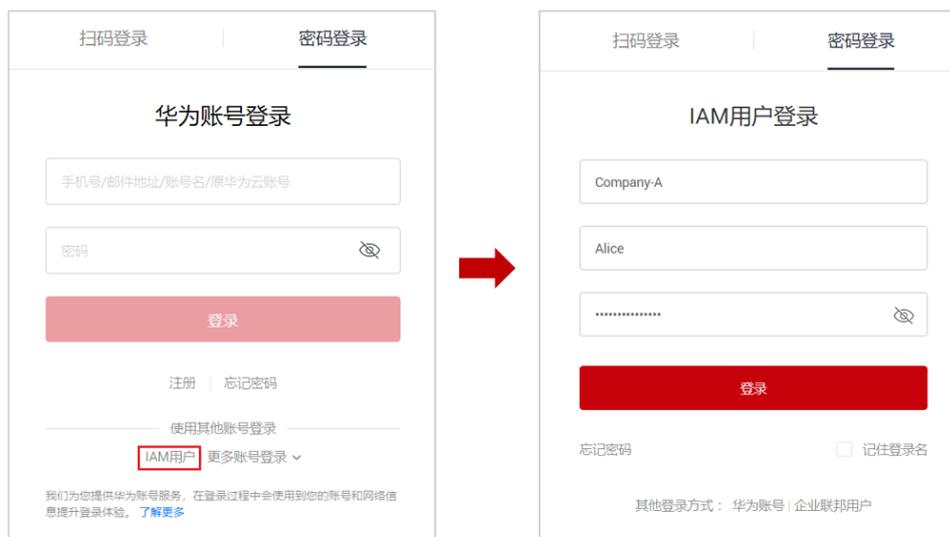


表 2-4 登录信息

参数	示例	说明
租户名/原华为云账号名	Company-A	IAM用户所属的账号。此处假设A公司的账号名为“Company-A”。
IAM用户名/邮件地址	Alice	在IAM创建用户时，输入的IAM用户名/邮件地址。如果不知道IAM用户名及初始密码，请向管理员获取。

参数	示例	说明
IAM用户密码	*****	IAM用户的密码，非账号密码。此处需要输入上一步中下载的Alice用户的密码。

**步骤2** 单击“登录”，IAM用户Alice登录华为云。

**步骤3** IAM用户Alice验证权限。

1. IAM用户Alice登录成功后，请先切换至“华北-北京四”。



2. IAM用户Alice在“服务列表”中选择弹性云服务器ECS，可以进入ECS的主页面并进行创建ECS、管理ECS等所有操作，表示ECS FullAccess权限配置成功。
3. IAM用户Alice在“服务列表”中选择对象存储服务OBS，可以进入OBS的主页面并进行查看桶列表、查询桶位置的操作，但不能执行创建OBS桶的操作，表示OBS OperateAccess权限配置成功。
4. IAM用户Alice在“服务列表”中选择除ECS和OBS服务外的任一服务，系统提示权限不足，表示ECS和OBS服务的权限配置成功。
5. IAM用户Alice切换区域至除“华北-北京四”的任一区域，无法进入除对象存储服务OBS以外服务的主页面，包括弹性云服务器ECS，表示权限中区域项目的授权范围配置成功。

----结束